

Prof. Dr. Đorđe Krivokapić
Jelena Adamović
Dunja Tasić Krivokapić
Andrea Nikolić

HANDBOOK: PERSONAL DATA PROTECTION IN BUSINESS

HANDBOOK: PERSONAL DATA PROTECTION IN BUSINESS

Prof. Dr. Đorđe Krivokapić
Jelena Adamović
Dunja Tasić Krivokapić
Andrea Nikolić

Reviews

Milan Marinović
Prof. Dr. Hrvoje Lisičar
Dr. Nasir Muftić

Art direction

Kristina Pavlak

Translation

Milica Jovanović

Layout

Miodrag Panić

Design

Goran Ratković

Printed by Službeni Glasnik

Number of copies: 150

Published by the Faculty of Organizational Sciences, Belgrade, 2023.

Prof. Dr. Đorđe Krivokapić
Jelena Adamović
Dunja Tasić Krivokapić
Andrea Nikolić

HANDBOOK:
Personal data protection
in business



Publication “HANDBOOK: PERSONAL DATA PROTECTION IN BUSINESS” was created as a result of the Author’s activities within the project “Greater Internet Freedom” realized by the Author with the support of Internews and the United States Agency for International Development USAID. The views expressed in this publication/book do not reflect necessarily the views of Internews and the United States Agency for International Development USAID or the Government of the United States of America.

CONTENT

1. FOREWORD	11
1.1. Commissioner's foreword	11
1.2. Greater Internet Freedom Serbia Project foreword	13
2. GLOSSARY AND ABBREVIATIONS	15
2.1. Legal glossary	15
2.2. Technical glossary	18
2.3. Abbreviations	19
3. PREFACE	21
4. LEGAL FRAMEWORK	25
4.1. International system	25
4.2. European Union	26
4.2.1. GDPR	26
4.2.2. Police directive	27
4.2.3. National legislation	27
4.2.4. European Data Protection Board opinions	28
4.2.5. Opinions and decisions of independent supervisors	29
4.2.6. Decisions of the Court of Justice of the European Union	34
4.2.7. National court practice	34
4.2.8. Additional support	35
4.3. Serbia	37
4.3.1. Personal Data Protection Law	37
4.3.2. Secondary legislation	38
4.3.3. Practice	39
4.3.3.1 Court decisions	41
4.3.3.2. Decisions of the Commissioner	41

4.3.3.3. Opinions of the Commissioner	42
4.4. Commissioner for Information of Public Importance and Personal Data Protection	43
4.4.1. History and status	43
4.4.2. Commissioner's powers	45
4.5. Broader regulatory framework	45
4.5.1. Information security	45
4.5.2. E-commerce, advertising law, and intermediary liability	47
4.5.3. Law of obligations	49
4.5.4. Cybercrime	49
4.5.5. Free access to information of public importance and open data	50
4.5.6. Sectoral legislation	51
4.5.7. Self-regulation	51
4.5.7.1. Code of conduct	52
4.5.7.2. Certification	53
4.5.7.3. Binding corporate rules	55
4.5.7.4. Ethical guidelines for the development a nd application of reliable and responsible artificial intelligence	56
5. SCOPE OF APPLICATION	57
5.1. Material application	57
5.1.1. Automated processing and data collections	57
5.1.2. Personal or household exemption	58
5.2. Territorial application	60
6. BASIC CONCEPTS	67
6.1. Personal data	67
6.2. Data subject	72
6.3. Special categories of personal data	73
6.4. Data processing	77
6.4.1. Automated decision-making and profiling	80
7. KEY ROLES	87
7.1. Data controller	90

7.2. Joint controllers	95
7.3. Data processor	98
7.4. Data recipient	100
7.5. Third party	101
8. PRINCIPLES OF DATA PROCESSING	103
8.1. Importance of principles	103
8.2. Lawfulness, fairness, and transparency	104
8.3. Purpose limitation	110
8.4. Data minimisation	115
8.5. Accuracy	119
8.6. Storage limitation	122
8.7. Integrity and confidentiality	125
8.8. Accountability	127
9. LAWFULNESS	131
9.1. When is processing lawful?	131
9.2. Conclusion and execution of contracts	134
9.3. Compliance with legal obligations	138
9.4. Legitimate interests	140
9.5. Consent	147
9.5.1. Consent of minors	151
9.6. Protection of vital interests	153
9.7. Execution of public authority	154
9.8. Lawfulness of processing special categories of data	157
10. RESPONSIBILITY AND COMPLIANCE	161
10.1. Key obligations	161
10.1.1. Joint controller agreement	163
10.1.2. Controller and processor relationship	166
10.2. Documentation	169
10.2.1. Mapping processing activities	170
10.2.2. Records of processing activities	171
10.2.2.1. Controller's records	172
10.2.2.2. Processor's records	173
10.2.3. Policies and templates	173

10.3. Data Protection Impact Assessment	174
10.4. Privacy by Design and by Default	182
10.5. Data processing security	187
10.5.1. Risk Assessment	188
10.5.2. Security measures	190
10.5.2.1. Access control	191
10.5.2.2. Encryption	192
10.5.2.3. Pseudonymisation, tokenisation, and anonymisation	193
10.5.2.4. Data loss prevention	195
10.6. Incident Response	196
10.6.1. Incident management	196
10.6.2. Incident management policy.....	201
10.6.3. Notifying the Commissioner	202
10.6.4. Notifying data subjects	204
10.7. Data transfers	204
10.7.1. General rule for transfers	206
10.7.2. Transfers based on an adequate level of protection	206
10.7.3. Transfer with appropriate safeguards	210
10.7.4. Transfers in special situations	213
10.7.5. Data import into Serbia from the EU	214
10.8. Representative	216
10.8.1. Representative of a foreign controller or processor in Serbia	216
10.8.2. Representative of a Serbian controller or processor in the EU	218
10.8.3. Representative of a Serbian controller or processor in third countries	220
10.9. Allocation of roles in the organization	221
10.9.1. Managing the protection of personal data in the organization	222
10.9.2. Management	224
10.9.3. Data Protection Officer	226
10.9.3.1. When is there an obligation to appoint a Data Protection Officer?	226
10.9.3.2. Data Protection Officer status	229
10.9.3.3. Data Protection Officer duties	231

10.10. Employees	231
10.11. Organizational and personnel measures	234
10.12. Continuous internal education	236
10.13. Service providers	237
10.13.1. Software Services	237
10.13.2. Storage and maintenance services	238
10.13.3. E-commerce services	239
10.13.4. Professional management and consulting services	239
10.14. Cooperation with the Commissioner	241
11. CITIZENS' RIGHTS	245
11.1. Exercising rights and Transparency	245
11.2. The right to information	247
11.3. Right of access	252
11.4. Right to rectification and completion	255
11.5. Right to erasure	256
11.6. Right to restriction of processing	260
11.7. Right to data portability	262
11.8. Right to object	264
11.9. Right to legal remedy	265
11.10. Rights regarding automated decisions and profiling	266
11.11. Restriction of rights	269
11.12. Citizen requests	269
12. TYPICAL SITUATIONS	271
12.1. Recruitment process	271
12.2. Required personnel records	276
12.3. Video surveillance of employees	280
12.4. Employee productivity monitoring	284
12.5. Direct marketing	289
12.6. Mobile application	294
12.7. Online market and loyalty program	298
12.8. Big data	302
13. SPECIAL CASES OF PROCESSING	307
13.1. Freedom of expression and information	307

13.2. Free access to information of public importance	310
13.3. Processing of the national identification number	310
13.4. Processing in the field of labour and employment.....	311
13.5. Processing for archiving, research, and statistics	311
13.6. Processing by churches and religious communities	312
13.7. Processing for humanitarian purposes by authorities	312
14. SANCTIONS	313
14.1. Misdemeanour penalties	313
14.2. Nonmonetary liabilities	316
14.3. Compensatory damages	317
14.4. Reputational risk	318
14.5. Criminal liability	319
AUTHORS' BIOGRAPHIES	323

1. Foreword

1.1. COMMISSIONER'S FOREWORD

Those of you lucky enough to hold this publication must be familiar with the feeling of waking up on a beautiful spring or summer morning and deciding to go to a nearby mountain and climb its highest peak, the one you have never climbed before. And so you go. And while you are slowly progressing towards your goal, when the fatigue starts to set in, you ask yourself a little bit in the loss of morale: “Will I be able to do this? Is it worth this much effort?” Well, that's exactly how I felt when I saw how much work was in front of me and how many pages of text I had to read in order to be able to write a valid foreword. And as I slowly progressed in reading, just like our hiker up the mountain, the facts and data flooded me like a real summer burst of clouds. And when, finally, I finished reading the last words of the last line on the last page of the publication, like our hero climbing to the highest mountain peak, I got the answer to the question: “It was worth it!” And how worth was it! And just as he was presented with a wonderful scene of fields, hills, forests, and settlements of various colours, the whole “world” of personal data protection in Serbia and in Europe was presented to me. It has everything: a normative framework, expert opinions, court decisions, and great examples from the practice of the Commissioner, as well as authorities from EU member states. There's something for everyone interested.

Exceptional, well-conceived, and even better executed publication that undoubtedly possesses both quality and capacity to be an indispensable reading material for every data controller in Serbia and beyond. Although the authors' intention was probably to target primarily business participants such as manufacturing companies, corporations, trade, hospitality, and other enterprises, banks, insurance companies, and entrepreneurs, it can be freely said that authorities handling citizens' data will also derive no less benefit from this publication. Despite being quite extensive, which is entirely justified considering the breadth of its coverage and the multitude of topics it addresses, it is still easy to navigate through and find what specifically interests you.

As someone who has been dealing with the protection of personal data for a long time, I have to single out many examples from the practice of European and national authorities that protect personal data, as well as the practice of courts throughout Europe. A particular value in use of this publication is represented by various hypothetical examples outlined under the title “Typical situations”

which in a concise and simple and quite sufficient way teach how to behave and what to pay attention to in specific situations of planning and beginning with the processing of personal data. However, I must emphasize that this publication, with all its virtues, does not represent too much of a surprise for me, because I did not expect anything less from the author of the publication, who is a proven expert in the field of personal data protection and is well aware of the needs of all layers of society, especially participants in business to familiarize themselves in the right way and to the greatest extent possible with all aspects of personal data protection, above all in Serbia. In addition, I must emphasize the educational function of this publication, which will greatly help the Commissioner's efforts to spread awareness of the importance and ways of protecting personal data everywhere, and especially among those who handle our data and process it, in order to do it as safely as possible, to the general satisfaction. In any case, one thing is certain: I and the employees of the Commissioner's office will be happy to use this publication as an extremely useful aid in performing our basic task – protection of personal data. And to everyone else, especially those who deal with the processing of personal data in their daily life and work, I recommend this publication with pleasure.

The Commissioner
Milan Marinović

1.2. GREATER INTERNET FREEDOM SERBIA PROJECT FOREWORD

Dear readers,

With great enthusiasm, I express my gratitude for the opportunity to write these lines. Furthermore, I feel excited to be honoured and privileged to participate in this exceptional project that will ultimately be the result of the collective efforts of outstanding talents, experts, as well as the leading author, a foremost regional expert in this field.

Digitalization, with its abundance of benefits, paves the way for incredible progress in many spheres of our lives. However, at the same time, we are facing new challenges. Useful new technologies in everyday use generate unprecedented amounts of data and require us to have answers to numerous questions about privacy and data security.

In the era of global connectivity and continuous flow of information, it is increasingly important to have clear and precise laws that protect human rights and freedoms in the digital ecosystem, as well as data integrity, transparency, and accountability in their processing. With the further expansion of the digital economy and industry, regulations must constantly adapt to encompass the interests of a broader range of individuals and organizations. Just like the devices we use, the rules of the digital age are becoming increasingly complex.

As someone who has spent most of the professional career in the private sector, I am well aware of how much those who manage processes and organize business operations need support to better understand their rights and obligations – towards partners, employees, clients, and the wider public. I trust that in this regard, assistance is most needed by entrepreneurs, managers, owners of small and medium-sized enterprises, as well as by many organizations within the public sector.

It is exactly the kind of support that is now before you: a reliable guide to interpreting complex legislative solutions in personal data protection, as well as their practical implementation in day-to-day business operations. The rules are illustrated with examples of best practices and data protection solutions that are applied across Europe and are also applicable in Serbia and most of our region.

I hope that the Handbook will serve you as a valuable tool to better understand the key challenges of personal data protection and to encourage discussions about further enhancing regulatory solutions at both local and European level.

Only through collective effort can we build a sustainable and secure digital environment for present and future generations.

Thank you for dedicating your time to this handbook and for joining us in our endeavour to improve personal data protection.

Sincerely,

Danilo Barjaktarević,
Project Director at GIF
(Greater Internet Freedom Serbia)

2. Glossary and abbreviations

2.1. LEGAL GLOSSARY

Personal data

Any information relating to an individual human being, regardless of whether that person has already been identified or can be identified based on that information.

For example: name and surname, address, bank account, fingerprint, health record, physical or psychological characteristics, accounts and passwords for online services (messages, email, social networks), activities on the internet (shares, likes, clicks, search, metadata), IP address, IMEI number, etc. If the device or browser is personalized, even cookies downloaded from websites are considered personal data.

Special categories of personal data

Information that is closely related to the fundamental personal rights and freedoms. That is why we also call it sensitive information.

These are data on racial or ethnic origin, political opinion, religious or philosophical beliefs, membership in a trade union, genetic and biometric data, as well as data concerning health, sex life or sexual orientation.

Their processing is prohibited in principle, except in strictly prescribed cases, where the obligations of their protection are greater and the penalties are more drastic.

Data subject

An individual (natural person, person, citizen) whose personal data is processed.

In many European languages, including Serbian, the law often uses a phrase “the person to whom the data relates” when talking about the rights of citizens in relation to the processing of their personal data, to highlight the direct connection between the person who has the rights and specific data.

Processing of personal data

Any contact with personal data or sets of personal data. These actions can be both active and passive: collecting, alignment or combination, grouping, storing, adaptation or alteration, retrieval, disclosure by transmission, duplicating, publishing,

comparing, erasure or destruction, etc. Personal phone book, photo album and similar examples of processing for personal and family purposes are not subject to the law.

Data controller

The role that an individual or organization has in relation to the processing of personal data.

This status means that a natural or legal person in the role of controller has full control over data processing, i.e. determines why and how data is collected and stored. The data controller manages the processing of data in all stages: determines the type, purpose and method of processing, method and duration of storage, defines the rights of the data subjects, as well as their own and the processor's obligations.

Joint controllers

When the purpose and method of one processing operation is jointly determined by two or more controllers, they have an additional obligation to mutually agree on their responsibilities to ensure that the operation is in compliance with the law, as well as for exercising the rights of the citizens whose data they process. Their arrangement must be governed by an agreement and presented to the data subjects.

Processor

Another important role that an individual or organization can have in relation to the personal data processing. That natural or legal person has no control over the processing: the data processor does not make important decisions about why, how and for how long the data is processed, but acts exclusively according to the instructions given by the controller.

When the processor entrusts certain processing actions to another entity on behalf of the controller, that other processor is called a sub-processor.

Data recipient

An individual or organization is a recipient when they indirectly receive someone's personal data. As of that moment, the recipient must switch to the role of either controller or processor, which means that they assume the appropriate obligations in relation to the processing of the data they have received.

Data Protection Impact Assessment

There are situations in which the scope, purpose or method of personal data processing are particularly risky for the rights and interests of the citizens whose data is being processed. The controllers are then required by law to assess possible risks in certain stages of processing in advance and to define technical and organizational measures that would mitigate or eliminate those risks. Such document is the basis for the development of internal procedures, but also proof of compliance with prescribed protection measures. As the processing circumstances change, for example, with the use of more advanced technology, new analyses and impact assessments are needed.

Records of processing activities

Almost all controllers and processors are obliged to keep internal records of personal data processing operations. The law prescribes the minimum information that these records must contain.

Privacy policy

A statement or legal document that contains information about the method and purpose of collecting and processing personal data, the obligations of the controller and the rights of citizens.

Data Protection Officer

Controllers who process massive amounts of personal data, as well as those who process sensitive personal data on a large scale, are obliged by law to appoint a person who will ensure compliance in all stages of processing. That person can be one of the employees of the controller, or an outside expert.

It is a good practice for controllers and processors who do not have this legal obligation, to voluntarily appoint a Data Protection Officer (DPO).

Commissioner

An independent and autonomous public authority, whose full name in Serbia is Commissioner for Information of Public Importance and Protection of Personal Data. It is an agency equipped with professional staff and resources to monitor compliance with the law, authorized to carry out inspections. The Commissioner receives complaints from citizens whose rights to the protection of personal data have been violated and initiates the appropriate procedure.

Data breach notification

In the event of a violation of the security of the personal data, the processor is obliged to inform the controller as soon as they become aware of the violation. The controller shall notify the Commissioner of the violation within 72 hours at the latest. The law obliges the controller to inform the citizens whose data they process about the violation, if the violation has resulted in increased risks for citizens.

Trusted resources

Explanations of the most important terms and basic legal institutes of the regulations governing the protection of personal data in the Serbian language can be found in the “Personal Data Protection Glossary”, published by the SHARE Foundation and freely available for download.¹

¹ Personal Data Protection Glossary (J. Adamović, SHARE Foundation, 2021)
[In Serbian]



2.2. TECHNICAL GLOSSARY

Privacy by default – a sales or distribution approach that implies that the default settings of the product or service are such as to protect privacy.

Privacy by design – approach to building, programming, designing, developing, etc. hardware or software, which implies that user privacy protection is an integral part of the device, program or system.

Cookies – pieces of data that websites exchange with the user's device for short-term memory of the user's activities on the site

Tracker cookies – special type of cookies used for long-term memory of user activities, their profiling based on behaviour, especially through third-party trackers. They belong to the types of cookies that are not necessary for the use of online services and as such are subject to provisions on consent given freely and unconditionally.

Opt-in – a predefined model of relationship with users, which implies the activation of the service only after the users express their explicit consent

Opt-out – a predefined model of relationship with users, which implies that the automatically activated service ends only after the users explicitly request it

Hashing – mathematical transformation of data of different lengths into a fixed length value, especially suitable for safe storage. Cryptographic hash functions are used as an additional element of security.

2.3. ABBREVIATIONS

CJEU – Court of Justice of the European Union

EDPB – European Data Protection Board

EDPS – European Data Protection Supervisor

EU – European Union

ePrivacy directive – Privacy and Electronic Communications Directive

GDPR – General Data Protection Regulation

ICO – Information Commissioner’s Office

IMEI – International Mobile Equipment Identity

IP – Internet Protocol, set of technical standards and rules for online data exchange

UMCN – Unique Master Citizen Number (identification number assigned at birth in Serbia)

PDPL – Personal Data Protection Law in force in Serbia

3. Preface

The General Data Protection Regulation (GDPR), which is in force in the EU, represents a radical advancement in personal data protection on a global level. Many countries outside the European Union, including those on other continents, have adopted their own national regulations following the new EU standards. Among them is Serbia, which passed its new law in 2018.

Although the legal framework for personal data protection has been in place for five years, time flies quickly, and it may seem logical to keep referring to it as new. However, contemporaries of the lightning-fast development of new technologies and tumultuous events worldwide – including the influence this development has on politics and law itself – bear witness to how five years is indeed a substantial period. For instance, the United Kingdom is no longer a member of the European Union nor the European Economic Area, while new forms of artificial intelligence, such as chatbots, are used for presenting fictitious submissions in court, providing medical advice from hell, and plagiarizing school assignments. Without vast amounts of data, including personal data, the accelerated digital transformation of businesses and the rapid development and application of artificial intelligence technologies would not have been possible. Regardless of the changes that have occurred, it appears that the legal framework for personal data protection is becoming increasingly relevant and significant for modern business.

The goal of the Personal Data Protection in Business Handbook is to raise awareness about this specific field and provide practical information to the members of the business sector on compliance with both the Serbian Law on Personal Data Protection and GDPR in an accessible and easily understandable format. The business, academic, and professional communities, the Commissioner, various state bodies, and the civil sector all agree that complying with the legal framework for personal data protection poses a challenge for corporations, small and medium-sized enterprises, and other business entities, as well as for legal, organizational, and technical consultants who provide services in this area. The Handbook was created to assist the businesses in establishing a responsible personal data processing system that upholds high standards of human rights protection without compromising their competitive advantage.

The Handbook will be useful to all stakeholders involved in modern business: data protection officers and other professionals who have chosen this field of work, as well as business leaders, entrepreneurs who are starting or expanding

their operations, and other legal, organizational, and technical consultants providing services in the field of digital transformation. The Handbook will be of particular significance for knowledge innovation programs in the areas of information and communication technology law and the digital economy, as well as for academic study programs that aim to prepare students for entrepreneurship and the business environment, such as management, economics, information systems, creative industries, and others.

Concise and practical, the Handbook guides the reader through critical areas, the understanding of which is essential for anyone intending to process personal data within a business. The Handbook contains:

- Introductory chapters that comprise an index of terms and abbreviations (II) and present the international, European, and national legal framework for personal data protection (IV).
- Chapters providing an overview of key aspects of personal data protection, such as the scope of the law's application (V), fundamental concepts (VI) and roles (VII), principles (VIII) and lawfulness (IX) of personal data processing, as well as individual rights (XI) and sanctions (XIV).
- Chapters that provide guidelines for implementing the legal framework through assuming responsibility and the compliance process (X).
- Chapters that guide readers through typical business situations (XII) and specific cases of personal data processing (XIII).

Alongside an overview of the legal framework, application advice, the Commissioner's opinions and guidelines, the practice of various data protection authorities across the European Union are also presented, accompanied by recommendations from bodies responsible for interpreting the rules. The Handbook also contains practical advice, reliable resources, and tools that will aid the process of complying with the personal data protection legal framework, as well as concrete examples gathered over the five years of applying new rules in the field. Furthermore, the Handbook provides an overview of practical guidance for small and medium-sized enterprises developed by the Commissioner, supervisory authorities, civil society, and professional organizations.

In preparing this Handbook, the authors aimed to empower business stakeholders when encountering rules of personal data protection, enabling them to discern pertinent issues and take appropriate steps in the planning stage of their business activities. Special attention is given to contextualizing the application of legal mechanisms within business relationships, enhancing the capacity of business stakeholders to identify and manage legal, organizational, and technical risks. The goal of the Handbook is not only to familiarize readers with the legal framework but also to ensure an accurate interpretation of regulations in the field of personal data protection.

In the course of their work, the team of authors enjoyed generous support of a broad spectrum of stakeholders, ranging from the Commissioner's expert services, business associations, and specialized law firms to representatives of academia

and leading civil society organizations. All of them made specific contributions to this Handbook, providing feedback on the initial draft and suggesting improvements to the text, current examples, guidelines, and reliable resources, allowing it to reach its final form. The authors would like to extend special thanks to Milan Marinović, the Commissioner for Information of Public Importance and Personal Data Protection, Gordana Mohorović, Assistant General Secretary of the Commissioner, Prof. Dr. Stevan Gostojić from the Faculty of Technical Sciences at the University of Novi Sad, as well as Ninoslava Bogdanović and Danilo Krivokapić from the SHARE Foundation, who, with their expert and precise comments and contributions, greatly contributed to the quality of the Handbook.

Unless otherwise clearly stated, the term Personal Data Protection Law or its abbreviation PDPL, or simply the Law, refer to the specific piece of legislation in the Republic of Serbia.

The pronouns they/them are used when referring to a natural person of unspecified gender.

The guide is currently available in Serbian and English languages.

In Belgrade,
July 1, 2023

Authors:
Prof. Dr. Đorđe Krivokapić
Jelena Adamović
Dunja Tasić Krivokapić
Andrea Nikolić

4. Legal framework

4.1. International system

In order to better understand the domestic and European legal frameworks of personal data protection, it is of particular practical importance to know the basic international instruments, as well as the earlier European framework that was applied through the Data Protection Directive (Directive 95/46/EC).¹ Certain elements of the existing regulation, such as the principles of data processing, are entirely based on these documents. Therefore, the interpretations of these acts, as well as the practice based on them, can be applied analogously when interpreting the Serbian data protection law and the EU General Data Protection Regulation.

Also of importance are United Nations treaties and agreements, including the Universal Declaration of Human Rights (1948)² and the International Covenant on Civil and Political Rights (1966).³ The Universal Declaration stipulates that no one can interfere in someone else's private life, family, home or correspondence, nor attack someone's honour and reputation.

The Council of Europe also has a number of fundamental documents relevant to the field of personal data protection, starting from the European Convention for the Protection of Human Rights and Fundamental Freedoms,⁴ down to specific bylaws securing better and consistent application of various documents. The European Convention stipulates that everyone has the right to respect for their private and family life, home and correspondence. The concept of the right to privacy is further shaped by regulations on the protection of personal data. The Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108+), as well as its additional protocols are in force,⁵ and in 2021, the Advisory Committee of the Convention on the Protection of Persons with regard to Automatic Processing of Personal Data adopted the Guidelines for facial recognition⁶

1 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A31995L0046>

2 Universal Declaration of Human Rights <https://www.un.org/en/about-us/universal-declaration-of-human-rights>

3 International Covenant on Civil and Political Rights <https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights>

4 European Convention on Human Rights https://www.echr.coe.int/documents/d/echr/convention_ENg

5 Convention 108 and Protocols <https://www.coe.int/en/web/data-protection/convention108-and-protocol>

6 Guidelines on facial recognition <https://edoc.coe.int/en/artificial-intelligence/9753-guidelines-on-facial-recognition.html>

and the Guidelines of the Council of Europe on the protection of data about children in the educational environment.⁷ Recommendations of the Committee of Ministers to member states on the processing of personal data in the context of employment, health data protection and others were also adopted.⁸

Trusted resources

An overview of the key privacy and personal data protection laws in over 100 different jurisdictions around the world is freely available in a handbook published by the DLA Piper law firm. This exceptionally informative tool can also be useful for comparing legal solutions in the field of personal data protection in different countries.¹



¹ DLA Piper's Data Protection Laws of the World Handbook - 2023 edition.

4.2. European Union

4.2.1. GDPR

With the adoption of the General Data Protection Regulation, Directive 95/46 EC was repealed, with the stipulated obligation to review and harmonize other EU acts according to the newly established rules. The GDPR applies to all 27 member states of the European Union. It also applies to all countries in the European Economic Area (EEA), which, in addition to EU members, includes Iceland, Liechtenstein, and Norway. As of January 1, 2021, the United Kingdom is no longer a member of the EU and is no longer subject to the EEA, but since the same year the country adopted the law referred to as UK GDPR and fully compliant with the standards prescribed in the GDPR. Switzerland, which is also not a member of the EU, has adopted a privacy protection law modelled after the GDPR.

The text of the General Regulation consists of two components, the Articles and the Recitals. Normative text is presented in 99 articles, i.e. legal norms, standards and obligations that organizations must comply with. The 173 recitals constitute the Preamble, an integral introduction to the General Regulation, in which explanations and accompanying context are given for a better understanding of the legal provisions. In the first recital, the protection of personal data is defined as a fundamental human right.

7 Children's data protection in an education setting – Guidelines <https://edoc.coe.int/en/children-and-the-internet/9620-childrens-data-protection-in-an-education-setting-guidelines.html>

8 Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data <https://rm.coe.int/16806ebe7a>; Recommendation CM/Rec(2015)5 of the Committee of Ministers to member States on the processing of personal data in the context of employment https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805c3f7a; Recommendation CM/Rec(2019)2 of the Committee of Ministers on the protection of health-related data <https://edoc.coe.int/en/international-law/7969-protection-of-health-related-date-recommendation-cmrec20192.html>

When deciding on the meaning and application of certain provisions competent institutions take recitals into consideration. With the help of recitals, it is clearer to organizations in which cases and in what way they should comply with the prescribed standards. For example, recital 32 lists examples of clear affirmative consent to data processing, clarifying that consent is considered to be ticking a box when visiting an internet website, choosing technical settings for information society services or another statement or conduct which clearly indicates the data subject's acceptance of the personal data processing. It also states what does not constitute consent, such as silence, pre-ticked boxes or other forms of inactivity. The preamble is therefore not only useful, but also represents a necessary starting point for the interpretation of regulations. The Domestic Law did not take over the Preamble of the GDPR, which somewhat complicates its interpretation.

4.2.2. Police directive

At the European Union level, the protection of personal data in the security sector is regulated by the so-called Police directive.⁹ This regulation takes into account that sectoral bodies are entrusted with delicate tasks routinely using personal data of citizens such as protecting state borders, protecting the safety of citizens and institutions, prosecuting criminals. In the case where the processing is carried out by the sector that protects public safety and security of the state and citizens, the data protection system has a special legal regime. Although the Police Directive relies on the standards prescribed by the GDPR, it provides for exceptions to the application of the general regime. Namely, the rights of data subjects can be significantly limited, and the principles of minimization and transparency are relaxed.

Bearing in mind the obligation of Serbia to harmonize its legislation with that of the European Union, assumed by Article 72 of the Stabilization and Association Agreement, the Law on Personal Data Protection was modelled after both the GDPR and the Police Directive, encompassing provisions that regulate processing under the general regime and in the security sector, i.e. processing for special purposes.

4.2.3. National legislation

Although the old EU Directive 95/46/EC laid significant foundations for the personal data protection, it did not achieve the uniformity of the rights of persons whose personal data are processed, nor did it foresee legal protection against inadequate processing of personal data outside the EU. Although it takes over most of the provisions from the old Directive, the GDPR removes these shortcomings by expanding the scope of application. The general regulation tightens the existing requirements and introduces several new ones, while additionally standardizing the protection system and

⁹ Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016L0680>

thereby narrowing the space for different rules within the EU common digital market. While directives only determine the objectives that EU member states should achieve by independently regulating details within national legislation, regulations represent a binding legislative act that is directly and fully applicable in all member states.

However, although the GDPR is directly applicable in all 27 EU member states, each country has retained the right to enact national laws, which would regulate the protection of personal data, within the limits of the powers provided by the GDPR. Thus, the General Regulation contains about 60 “open clauses” that allow member states to specifically regulate certain issues within the national framework, i.e. to strengthen the application of some provisions of the GDPR. The areas for which this type of flexibility applies concern, among other things, the processing of personal data in the context of employment (Article 88), the appointment of persons for the protection of personal data (Article 37), legal bases (Article 6, paragraph 1, points c and e), automated decision-making and profiling (Article 22), and joint controllers (Article 26).

The fact that an issue is not expressly regulated by the General Regulation is not, in principle, an obstacle for a member state to regulate it by national law. With such a regulation, states can define certain standards in more detail or prescribe special provisions for typical cases of processing such as, for example, specifying the age at which a minor can independently give consent for data processing and the like. For example, the German personal data protection law contains provisions on video surveillance in public spaces, which are not prescribed by the GDPR. Austria, Croatia, Hungary and Slovenia are some of the other EU countries that have supplemented the implementation of the General Regulation with a national law on the protection of personal data.¹⁰

Therefore, it is important to determine whether, in addition to the GDPR, compliance with the law in one of the EU countries includes a national regulation that additionally regulates specific issues.

4.2.4. European Data Protection Board opinions

At the time the old Directive 95/46 was adopted, it was already clear that harmonizing its interpretation was crucial for its implementation. Its Article 29 provided for the establishment of the Working Party on the Protection of Individuals with regard to the Processing of Personal Data, commonly known as the “Article 29 Working Party” (Art. 29 WP). The party consisted of representatives from data protection authorities of EU member states, and it has produced and adopted numerous opinions and guidelines over the years that extensively address a wide range of complex issues, from the concept of personal data itself, to the roles of data controllers and processors, rules for valid consent, and more. All opinions and guidelines issued by the Article 29 Working Party remain relevant as long as they are not in conflict with the new rules prescribed by the GDPR.

With the General Data Protection Regulation’s entry into force, the Article 29 Working Party was replaced by the European Data Protection Board (EDPB), whose

¹⁰ Data Guidance, Global Privacy Laws <https://www.dataguidance.com/advisories/global-privacy-laws>

main task is to contribute to the consistent application of rules across the EU, having essentially the same mandate as the Article 29 Working Party.¹¹ The EDPB has issued a series of opinions and guidelines that are crucial for understanding the GDPR and the rules on personal data protection. These documents are valuable for interpreting domestic law as well. They cover topics such as citizens' rights, the concepts of data controllers and processors, conditions for valid consent, territorial scope of the GDPR, criteria for calculating fines for GDPR violations, and more.¹² In addition, the EDPB has accepted a number of guidelines and opinions previously issued by the Article 29 Working Party as relevant for interpreting the General Data Protection Regulation.¹³

4.2.5. *Opinions and decisions of independent supervisors*

As the preceding Directive, the GDPR establishes the obligation for each European Union member state to provide for an independent supervisory authority for the protection of personal data, known as an independent supervisor. These supervisors autonomously monitor the application of personal data protection rules and have the power to issue opinions, conduct investigations, initiate proceedings, issue warnings and penalties, and more. In Serbia such an independent authority with special powers of state authority is called the Commissioner for Information of Public Importance and Personal Data Protection (Commissioner). Supervisory authorities must not be subject to any direct or indirect external influence and must not seek or receive instructions from anyone. Each member state provides the supervisory authority with appropriate resources, including human, technical, physical, and financial resources necessary for its successful operation.

The practice of independent supervisors is of paramount importance as they generally represent the most operational part of the national administration responsible for data protection. Since the enforcement of the General Data Protection Regulation, each national supervisor has developed extensive practice in interpreting and implementing the rules. These authorities are often highly proactive, with the Spanish, Italian, Danish, Belgian, and Romanian supervisors being the most active, issuing over a hundred different decisions each.¹⁴

Despite the United Kingdom's exit from the EU, the GDPR and the European legal framework for personal data protection remain relevant in this country. The Information Commissioner's Office (ICO), the British supervisory authority, continues to be one of the most productive supervisors in terms of developing practical opinions and guidelines.¹⁵

11 European Data Protection Board edpb.europa.eu

12 EDPB, Guidelines, Recommendations, Best Practices https://edpb.europa.eu/our-work-tools/general-guidance/guidelines-recommendations-best-practices_en

13 EDPB, Endorsed WP29 Guidelines https://edpb.europa.eu/our-work-tools/general-guidance/endorsed-wp29-guidelines_en






14 NOYB – European Center for Digital Rights, GDPR Hub, database of decisions of European independent authorities for the protection of personal data https://gdprhub.eu/index.php?title=Category:DPA_Decisions

15 Information Commissioner's Office ico.org.uk

**List of independent supervisors (commissioners)
in the European Union**

Austria	Austrian Data Protection Authority (Österreichische Datenschutzbehörde)	
Belgium	Commission for the protection of privacy (Commissie voor de bescherming van de persoonlijke levenssfeer, CBPL / Commission de la protection de la vie privée, CPVP)	
Bulgaria	Bulgarian data protection authority (Комисия за защита на личните данни)	
Czech Republic	The Office for Personal Data Protection (Úřad pro ochranu osobních údajů, ÚOOÚ)	
Denmark	Danish Data Protection Agency (Datatilsynet)	
Estonia	Estonian Data Protection Inspectorate (Andmekaitse Inspektsioon)	
Finland	Office of the Data Protection Ombudsman (Tietosuojavaltuutetun toimisto)	
France	National Commission on Informatics and Liberty (Commission nationale de l'informatique et des libertés, CNIL)	
Greece	Hellenic Data Protection Authority (Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, ΗΔΠΑ)	
Netherlands	Dutch Data Protection Authority (Autoriteit Persoonsgegevens, AP)	
Croatia	Croatian Personal Data Protection Agency (Agencija za zaštitu osobnih podataka, AZOP)	

Ireland	Data Protection Commissioner (An Coimisinéir Cosanta Sonraí, DPC)	
Italy	Italian Data Protection Authority (Garante per la Protezione dei Dati Personali)	
Cyprus	Commissioner for Personal Data Protection (Γραφείο Επιτρόπου Προστασίας Δεδομένων Προσωπικού Χαρακτήρα)	
Latvia	Data State Inspectorate (Datu valsts inspekcija/ Государственная инспекция данных)	
Lithuania	State Data Protection Inspectorate (Valstybinė duomenų apsaugos inspekcija, VDAI)	
Luxembourg	National Commission for Data Protection (Nationale Kommission für den Datenschutz / Commission nationale pour la protection des données, CNPD)	
Hungary	Data Protection Commissioner of Hungary (Nemzeti Adatvédelmi és Információszabadság Hatóság, NAIH)	
Malta	Office of the Information and Data Protection Commissioner – IDPC	
Germany	Federal Commissioner for Data Protection and Freedom of Information (Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, BfDI)	
Poland	The Bureau of the Inspector General for the Protection of Personal Data (Generalny Inspektor Ochrony Danych Osobowych, GIODO)	
Portugal	National Commission for Data Protection (Comissão Nacional de Protecção de Dados, CNPD / NCDP)	

Romania	The National Supervisory Authority for Personal Data Processing (Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal, ANSPDCP)	
Slovakia	Office for Personal Data Protection of the Slovak Republic (Úrad na ochranu osobných údajov Slovenskej republiky)	
Slovenia	Information Commissioner of the Republic of Slovenia (Republika Slovenija Informacijski pooblaščenec)	
Spain	Spanish Agency of data protection (Agencia Española de Protección de Datos, AEPD)	
Sweden	Swedish Data Protection Authority (Datainspektionen)	

**List of independent supervisors (commissioners)
outside the European Union**

Australia	The Office of the Australian Information Commissioner	
Montenegro	Agency for Protection of Personal Data (Агенција за заштиту личних података и слободан приступ информацијама)	
Guernsey	Office of the Data Protection Commissioner	
Hong Kong	Privacy Commissioner for Personal Data	
Iceland	Icelandic Data Protection Authority (Persónuvernd)	

Israel	Privacy Protection Authority (PPA)	
Canada	Privacy Commissioner of Canada (Commissariat à la protection de la vie privée du Canada)	
Liechtenstein	Data Protection Office (Datenschutzstelle)	
Norway	Norwegian Data Protection Authority (Datatilsynet)	
New Zealand	Privacy Commissioner	
Isle of Man	Information Commissioner	
North Macedonia	Directorate for Personal Data Protection (Дирекција за заштита на лични податоци)	
United States of America	Federal Trade Commission	
Serbia	Commissioner for Information of Public Importance and Personal Data Protection (Повереник за информације од јавног значаја и заштиту података о личности)	
Switzerland	Federal Data Protection and Information Commissioner (Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter, EDÖB / Préposé fédéral à la protection des données et à la transparence, PFPDT / Incaricato federale della protezione dei dati e della trasparenza, IFPDT; FDPIC)	
United Kingdom	Information Commissioner's Office – ICO	

4.2.6. Decisions of the Court of Justice of the European Union

The Court of Justice of the European Union (CJEU) interprets EU law, ensuring uniform application of the law across all member states. In line with its mandate, the Court has issued a series of decisions over the years that have played a significant role in interpreting and implementing the norms of the European framework for personal data protection. One of the most well-known CJEU decisions in the digital sphere is the *Google Spain v. AEPD and Mario Costeja González* case, which in 2014 expanded the right to be forgotten or the right to erasure.¹⁶ Following that Court decision, the GDPR specifically regulated the right to erasure with special attention.

4.2.7. National court practice

Judicial decisions of national courts in EU member states are significant sources for the interpretation of the General Regulation and the European framework for personal data protection. After five years of GDPR implementation, the number of relevant court decisions reaches the hundreds, with German courts being particularly active with nearly 150 decisions, followed by Dutch and Austrian courts with a double-digit number of published decisions.

Through the practice of national courts, criteria have been established to assess the intention of data controllers or processors to offer goods or services to individuals in the European Union, which is a condition for the application of the GDPR. Factors such as the currency for payment, the language used to offer goods or services, the internet domain, and others have been identified as relevant indicators confirming the intention to offer goods or services to individuals in the EU.

Practice

In the case of *Pammer v Schlüter* the CJEU established that it is necessary to determine whether a data controller intended to establish a relationship with consumers in one or more EU member states.¹ The Court prescribed significant indicators that a company based outside the EU offers goods or services to individuals in the EU, including the use of the language of a member state (if different from the language of the company's home state), the use of the currency of a member state (if different from the currency of the company's home state), the use of a domain associated with a member state (e.g., .fr or .eu), mentioning customers located in a member state, as well as targeted advertising directed at consumers in EU countries.

¹ Judgment of the Court (Grand Chamber) of 7 December 2010. *Pammer v Reederei Karl Schlüter GmbH & Co. KG (C-585/08)* and *Hotel Alpenhof GesmbH v Oliver Heller (C-144/09)*



16 Electronic Privacy Information Center, *The Right to Be Forgotten (Google v. Spain)* <https://archive.epic.org/privacy/right-to-be-forgotten/>

In a separate case, the Court determined that a data controller's activity is targeted at EU citizens when the controller operates a website for property sales located within the EU and conducts advertising in languages spoken within the European Union. On the other hand, the citizenship of the individuals whose personal data is processed is not relevant in this context.²



² GDPRHub, CJEU - C-230/14 – Weltimmo

Practice

In a case concerning the principles of data minimization and storage limitation, the CJEU issued a landmark decision that invalidated the EU directive on data retention.¹ The Directive aimed to harmonize national rules of EU member states on the retention of personal data collected in connection with the provision of publicly available electronic communication services. The CJEU ruled that the provisions of the Directive, which allowed for the processing of all types of data of all citizens through all means of electronic communication without any selection, limitation, or exception, were unacceptable. Additionally, the rule of the Directive that required all collected data to be stored for a period of six to 24 months was also deemed unacceptable. The timeframes were not linked to the precise types of data necessary to achieve the proclaimed purposes, nor were criteria established to determine a clear retention period within the given 18-month range that would genuinely be necessary to achieve those purposes.



¹ Judgment of the Court (Grand Chamber), 8 April 2014, C-293/12 & C-594/12, Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others

4.2.8. Additional support

In addition to international conventions, laws, and other legal documents, there are other sources available that are useful for interpreting the GDPR.

Documents from European institutions such as the European Commission, Council, and Parliament can be significant for interpreting the European legal framework for personal data protection. Furthermore, opinions and decisions from the European Data Protection Supervisor (EDPS) can provide valuable insights and guidance in understanding the GDPR.¹⁷

¹⁷ European Data Protection Supervisor https://edps.europa.eu/_en

Trusted resources

A comprehensive overview of relevant case law from European courts regarding breaches of key principles of personal data processing can be found in the Handbook on European Data Protection Law published by the European Union Agency for Fundamental Rights (FRA).¹



¹ FRA, Handbook on European data protection law - 2018 edition

Additionally, there are numerous useful platforms that provide detailed insights into best practices and experiences in GDPR implementation.

Trusted resources

One particularly useful tool is the GDPR Hub database, which allows for detailed searches based on specific articles of the GDPR and provides an overview of relevant decisions from competent authorities, ranging from national data protection supervisors to courts and other relevant institutions.¹ There is also a dedicated platform for monitoring GDPR implementation, providing an overview of fines and other sanctions imposed in proceedings before EU competent authorities.²



¹ NOYB – European Center for Digital Rights, GDPR Hub



² GDPR Enforcement Tracker

Privacy and data protection are the focus of various civil society organizations, such as NOYB (None Of Your Business), a non-profit organization for digital rights founded in 2017 and based in Vienna, Austria. Useful practices and guidelines for better GDPR compliance are published on their platform.¹⁸

The EDRI (European Digital Rights) association brings together nearly fifty organizations dedicated to protecting civil and human rights in the digital environment from across Europe.¹⁹ The association's website is rich in content related to digital rights, including opinions and positions on the interpretation of the legal framework for personal data protection from a public interest perspective.

¹⁸ Noyb - None of Your Business <https://noyb.eu/en>

¹⁹ EDRI <https://edri.org/>

Locally, the Belgrade-based SHARE Foundation is actively involved in shaping policies in the field of personal data protection at the European and global levels.²⁰ Established in 2012 as a non-profit organization aiming to advance human rights and freedoms in the online sphere, the SHARE Foundation promotes positive values of an open and decentralized internet, as well as free access to information, knowledge, and technology. Among other activities, this organization regularly publishes handbooks, analyses, and similar publications such as the Personal Data Protection Glossary,²¹ Guide to the Law on Personal Data Protection and GDPR,²² Guide to GDPR and Personal Data Protection – My Data, My Rights²³ and others. The SHARE Foundation has also launched several websites serving as educational resources for citizens, human rights defenders, and online media, with a focus on freedom of expression on the internet, data privacy, digital security, and open access to knowledge.²⁴ One notable initiative is the “My Data” platform, which specifically focuses on personal data protection.²⁵ In January 2017, the Commissioner for Information of Public Importance and Personal Data Protection presented the SHARE Foundation with a letter of appreciation for its outstanding contribution to promoting the right to personal data protection.

4.3. Serbia

4.3.1. Personal Data Protection Law

Establishing the normative framework for personal data protection in the Republic of Serbia began in the 1990s, more precisely with the inclusion of a guarantee for the protection of personal data in the Constitution in 1990. The first law that regulated this field in Serbia was enacted in 1998, but despite being in force for ten years, it was not effectively implemented. The current Constitution of the Republic of Serbia, adopted in 2006, guarantees the protection of personal data within the section on human and minority rights and freedoms. Subsequently, in 2008, the Law on Personal Data Protection was enacted, and its implementation began in 2009. Due to its deficiencies and the rapid and unstoppable technological advancements, this law needed to be replaced with a new, more modern one. This was done in November 2018 when the current law was adopted and came into force

20 SHARE Foundation <https://www.sharefoundation.info/en/>

21 SHARE Foundation, Personal Data Protection Glossary, 2021. <https://resursi.sharefoundation.info/wp-content/uploads/2021/07/Recnik-pojmova-zastita-podataka-final.pdf> [in Serbian]

22 SHARE Foundation, A guide to the Personal Data Protection Law and the GDPR - interpreting the new legal framework, 2019. www.sharefoundation.info/Documents/vodic_zzpl_gdpr_share_2019.pdf [in Serbian]

23 SHARE Foundation, Guide to GDPR and Personal Data Protection – My data, my rights, 2018. <https://resursi.sharefoundation.info/wp-content/uploads/2018/07/Podaci-u-doba-interneta-Final.pdf> [in Serbian]

24 SHARE Foundation, Initiatives, www.sharefoundation.info/en/initiatives/

25 SHARE Foundation, Portal My data <https://mojipodaci.rs/> [in Serbian]

in August of the following year.²⁶ The delayed implementation was conditioned by the introduction of new high standards for personal data processing. One of the most important novelties was the requirement for certain data controllers to appoint a Data Protection Officer overseeing data processing within the organization and communicates with the Commissioner for Information of Public Importance and Personal Data Protection, as well as other interested parties.

The Law on Personal Data Protection is a specific piece of legislation that horizontally regulates the protection of fundamental rights and freedoms of individuals, as prescribed by the Constitution and other laws, with a focus on the right to personal data protection. It primarily governs the rights of individuals regarding the processing of personal data and the free flow of such data. It also establishes standards for data processing, obligations of data controllers and processors, codes of conduct for specific situations, as well as oversight of enforcement of the law.

The text of the law is largely an adapted translation of the GDPR and the so-called Police Directive, which regulates the circumstances under which competent authorities process personal data related to criminal proceedings and threats to national security. Therefore, it can be said that the principles of the GDPR have been introduced into the domestic context. However, although the Law on Personal Data Protection is a compilation of translations of the GDPR and the Police Directive, the preambles of these two documents are omitted.

Of importance for the implementation of the Law on Personal Data Protection are also the Law on General Administrative Procedure,²⁷ the Law on Administrative Disputes,²⁸ and the Law on Inspection Oversight,²⁹ which primarily apply to the procedure for data protection before the Commissioner and other competent bodies.

However, the regulatory framework in this area does not end here, considering need for harmonizing other laws with the Law on Personal Data Protection. This requires a systematic approach by all state bodies. In this regard, significant efforts are being made to develop a Personal Data Protection Strategy and an Action Plan for its implementation.

4.3.2. Secondary legislation









Improvements to the legal framework are facilitated by a series of bylaws provided for by the Law on Personal Data Protection.

26 Personal Data Protection Law (Official Gazette of RS, No. 87/2018) www.paragraf.rs/propisi/zakon_o_zastiti_podataka_o_licnosti.html [in Serbian]

27 Law on General Administrative Procedure (Official Gazette of the RS, No. 18/2016, 95/2018 – authentic interpretation and 2/2023 – decision of the CC) www.paragraf.rs/propisi/zakon-o-opstem-upravnom-postupku.html [in Serbian]









28 Law on Administrative Disputes (Official Gazette of RS, No. 111/2009) www.paragraf.rs/propisi/zakon_o_upravnim_sporovima.html [in Serbian]

29 Law on Inspection Supervision (Official Gazette of RS, No. 36/2015, 44/2018 - other laws and 95/2018) www.paragraf.rs/propisi/zakon_o_inspekcijskom_nadzoru.html [in Serbian]

Relevant secondary legislation [available in Serbian language only]		
Standard contractual clauses	Decision on establishing standard contractual clauses	
Impact assessment	Decision on the list of types of personal data processing activities for which an assessment of the impact on the protection of personal data must be carried out and the opinion of the Commissioner must be sought	
Register of the Data Protection Officer	Rulebook on the form and method of keeping Data Protection Officers registry	
	Decision on the List of countries, parts of their territories or one or more sectors of certain activities in those countries and international organizations in which it is considered that an adequate level of protection of personal data is ensured	
Inspection oversight	Rulebook on the form of identification of an authorized person for inspection supervision under the Law on the Protection of Personal Data with forms of identification	
Data protection rights breach	Rulebook on the complaint form	
	Rulebook on the form of notification of a personal data breach and the manner of notifying the Commissioner for Information of Public Importance and Personal Data Protection of a personal data breach	
	Rulebook on the form and method of keeping internal records of violations of the Personal Data Protection Act and measures taken during inspection supervision	

4.3.3. Practice

Decisions of the Commissioner and court practice do not represent formal sources of law in Serbia but serve as auxiliary tools for better understanding of regulations. The starting point for interpretation is the text of the Law and subsidiary regulations, followed by the interpretation of court and practice of the Commissioner as the competent authority. However, the existing court practice in the Republic of Serbia in this field is very limited, making the practice of the Commissioner, available on their website and in a series of annual publications, the most significant source for interpretation.

Publication year	Title of the publication of the Commissioner for Information of Public Importance and Personal Data Protection [available in Serbian language only]	
2016.	Data Protection - Controller's Manual	
2017.	Personal data protection - Positions and opinions of the Commissioner	
2018.	Protection of personal data in the field of labor relations - Positions and opinions of the Commissioner	
2019.	Personal data protection - Positions and opinions of the Commissioner	
2020.	Protection of personal data - regulations	
2021.	Personal data protection - Positions and opinions of the Commissioner	
2022.	Personal data protection - Positions and opinions of the Commissioner	
2023.	Personal data protection – Positions, opinions, and practice of the Commissioner	

Since numerous concepts in the Law were adopted from European regulations, which were previously unfamiliar to the domestic legal system, it is advisable to interpret them in the same way as the provisions of the GDPR, for which there are already various instruments available.

Practice

Shortly after the implementation of the domestic Law, the Commissioner published an unofficial translation of the European General Data Protection Regulation in their annual publication.¹ This will undoubtedly provide a valuable insight into the comprehensive text of the GDPR in the native language, as it represents a complex legal framework that has raised the standards for personal data protection not only in EU member states, where it is directly applicable, but has also set a model standard worldwide. The current law in Serbia also incorporates a range of provisions from the material part of the GDPR, while omitting the introductory segment of the General Data Protection Regulation. As the preamble contains important explanations for better understanding the new norms and their application, it would be beneficial for every data processing in Serbia to be informed by the recitals of the preamble.

¹ Commissioner for Public Information and Personal Data Protection, Personal Data Protection - Regulations (Publication No. 5)



4.3.3.1 Court decisions

Although not a source of law in Serbia, court practice can serve as a source for better understanding of regulations and practices in the field of personal data protection. Relevant parts of court decisions from domestic courts are available on the website of the Commissioner,³⁰ as well as in other electronic legal databases.

4.3.3.2. Decisions of the Commissioner

The practice of independent supervisory authorities is highly significant for the adequate and uniform application of regulations in the field of personal data protection.

The Commissioner for Information of Public Importance and Personal Data Protection, acting *ex officio* or upon complaint from individuals, can conduct inspection proceedings regarding the implementation and enforcement of the Law. In relation to the conducted inspection, the Commissioner can issue various decisions. Filing a complaint with the Commissioner does not affect the right of individuals to initiate other administrative or judicial protection procedures.

If the Commissioner determines irregularities in the processing of personal data that are contrary to the Law, the Commissioner notifies the data controller and requests the rectification of the identified irregularities. The Commissioner may also order the implementation of adequate technical, personnel, and organizational measures for data protection in accordance with established standards and procedures. Following the inspection, the Commissioner can issue a decision on rectifying irregularities, a decision on the temporary prohibition of data processing, and/or a decision on the erasure of certain data if deemed necessary.

³⁰ Poverenik.rs, Decisions of domestic courts <https://shorturl.at/aqAC4> [in Serbian]

The data subject, data controller, data processor, or any other interested party has the right to initiate administrative proceedings against the Commissioner's decision within 30 days from the receipt of the decision. Filing an administrative lawsuit does not affect the right to initiate other administrative or judicial protection procedures. Additionally, if the Commissioner fails to act upon the complaint within 60 days from the date of its submission, the data subject has the right to initiate administrative proceedings.

When irregularities in data processing or misuse of personal data are identified, the Commissioner can submit a proposal to initiate misdemeanor proceedings. Additionally, based on the findings obtained during the inspection proceedings, the Commissioner can file a criminal complaint. Furthermore, the Commissioner has the authority to initiate proceedings to assess the constitutionality and legality of regulations and other general acts.

4.3.3.3. Opinions of the Commissioner

The Commissioner has the authority, and in some cases the duty, to issue various opinions and actively participate in the process of adopting regulations within their jurisdiction. As a general rule, the Commissioner provides an opinion on draft laws or proposed strategies and action plans related to the protection of personal data.

Practice

At the time the new law was being prepared, the Commissioner has provided an opinion to the Ministry of Justice on the need for the regulation of video surveillance. Among other things, the Commissioner proposed provisions regarding general obligations and records in relation to video surveillance, video surveillance in business premises, residential buildings, private apartments and houses, as well as video surveillance of public areas. However, the opinion was not approved.

The Data Protection Strategy in Serbia was adopted in 2010 but without a corresponding Action Plan. Considering the increasing scope of personal data processing and significant changes in terms of new technologies, the Commissioner initiated the development of a new Data Protection Strategy in 2021.¹ The first public consultations for its development were held in March 2023.²

¹ Ministarstvo pravde RS, Strategija zaštite podataka o ličnosti za period od 2023. do 2030. godine [in Serbian]

² Predlog strategije zaštite podataka o ličnosti za period 2023. do 2030. godine: Izveštaj o sprovedenoj javnoj raspravi [in Serbian]



The Commissioner is also authorized to issue opinions clarifying problematic situations within its competence. Any interested party can request an opinion from the Commissioner regarding specific questions related to the protection of personal data.

Practice

In 2013, an opinion was requested from the Commissioner regarding the age limit for valid consent to the processing of personal data.¹ Since the Law on Personal Data Protection does not regulate this issue, a uniform age limit has not been established. The Commissioner assessed that in each situation, the specific circumstances of the processing of personal data of minors should be taken into account, particularly the purpose of the processing and the type of data being processed, as well as relevant laws. The Commissioner analyzed the age limit for certain legal transactions and actions that minors can undertake, as prescribed by various laws in Serbia, and concluded that the answer to the age limit question should be sought in the function or purpose of the processing itself



¹ Poverenik.rs, Mišljenje – Uzrast maloletnog lica za obradu podataka o ličnosti [in Serbian]

Periodic publication issued by the Commissioner containing views, opinions, and practices is also significant. Additionally, on its website and in the appendix of publications, the Commissioner publishes a list of foreign companies that have appointed their representatives in accordance with the Law on Personal Data Protection. This information is important for citizens who are unsure of whom to contact in case of rights violations involving a foreign company.

4.4. Commissioner for Information of Public Importance and Personal Data Protection

Relevant provisions: *GDPR* – Articles 37-39, Recitals 117-145; *PDPL* – Articles 4, 73-81

4.4.1. History and status

The Commissioner protects two human rights, the right to access information of public importance and the right to personal data protection. Both rights are explicitly protected by the Constitution of the Republic of Serbia.³¹ The right to access information is enshrined in Article 51, which guarantees that everyone has the right to be accurately, fully and timely informed about matters of public importance, as well as to access information kept by state authorities. The right to personal data protection is guaranteed by Article 42 of the Constitution, which states: “Protection of personal data shall be guaranteed. Collecting, keeping, processing and using of personal data shall be regulated by the law. Use of personal data for any the purpose other the one were collected for shall be prohibited and punishable in accordance with the law, unless this is necessary to conduct criminal proceedings or protect safety of the Republic of Serbia, in a manner stipulated by the law. Everyone shall have the right to be informed about personal data collected about him, in accordance with the law, and the right to court protection in case of their abuse.”

³¹ Constitution of The Republic of Serbia <http://www.ustavni.sud.rs/page/view/en-GB/235-100028/constitution>

First in 2004 the institution of the Commissioner for Information of Public Importance was established through the Law on Free Access to Information of Public Importance.³² As a fundamental mechanism for increasing the transparency of government authorities, this legislation enabled citizens to actively seek information of public interest, rather than passively receiving it depending on the benevolence of government authorities and public officials. Journalists, especially those involved in investigative journalism and topics of high societal interest such as corruption and organized crime, have benefited the most from this law. It is difficult to imagine any serious journalistic investigation today without frequent reference to the Law on Free Access to Information of Public Importance. Over time, requests for exercising this right have also been actively submitted by other citizens. The right to access information of public importance is one of the most effective tools available to citizens for controlling the work of public authorities. For example, every citizen has the right to know how public funds are being spent, and the salary of a government official represents information of public importance.

This law established the Commissioner as an independent state body with autonomous authority. The Commissioner is appointed by the National Assembly, upon the proposal of the parliamentary committee responsible for information, for a period of eight years, without the possibility of reappointment to this position. The Commissioner must hold a law degree, have at least ten years of work experience, and a recognized reputation and expertise in the field of human rights protection and promotion.

With the enactment of the Law on Personal Data Protection in 2008, the Commissioner's jurisdiction expanded to include this area as well. Clear conditions are stipulated regarding who can process personal data and under what conditions, as well as the rights of individuals whose personal data is being processed. It is the Commissioner's task to oversee the implementation of the law. Thus, the Commissioner's authority is divided into two levels: one pertains to the protection of the right to free access to information and supervision of the implementation of the Law on Free Access to Information of Public Importance, while the other level pertains to the protection of the right to privacy, i.e., the protection of personal data and supervision of the implementation of the Law on Personal Data Protection. These two levels of authority are naturally opposing and represent two sides of the same coin – the relationship between the right of the public to know and the right to privacy. Therefore, in the exercise of optimal protection of these two rights, it is always necessary to seek an appropriate balance. This is one of the obligations of the Commissioner.

In 2004, the National Assembly appointed Rodoljub Šabić as the first Commissioner in Serbia, and he was reappointed in 2011, with his mandate ending in late 2018. The new Commissioner, Milan Marinović, was appointed in 2019.

As an independent authority responsible for enforcing two laws and other legally prescribed tasks, the Commissioner should be entirely independent from

32 Law on Free Access to Information of Public Importance (Official Gazette of RS, No. 120/2004, 54/2007, 104/2009, 36/2010 and 105/2021) https://www.paragraf.rs/propisi/zakon_o_slobodnom_pristupu_informacijama_od_javnog_znacaja.html [in Serbian]

any political or other influences in the exercise of their powers. Their role is supervisory in nature – to monitor the implementation of the laws.

The Commissioner is obliged to prepare an annual report on their activities, which is submitted to the National Assembly, provided to the Government, and made available to the public.

4.4.2. Commissioner's powers

Under the new Law on Personal Data Protection, the Commissioner has a broad range of powers. Firstly, they oversee and ensure the implementation of the Law on Personal Data Protection. They raise public awareness about the risks, protective measures, and rights related to the processing of personal data, as well as the legal obligations of data controllers and processors. They provide information on the legal rights for individuals whose data is being processed. The Commissioner handles complaints from individuals whose data is being processed and determines whether there has been a violation of the law. They collaborate with supervisory authorities in other countries regarding data protection, exchange information and provide mutual legal assistance. The Commissioner compiles and publicly publishes on their website a list of types of processing activities that require processing impact assessment. They also maintain a record of data protection officers provided by data controllers or processors.

The Commissioner also carries out inspection powers. They are authorized to, among other things, order data controllers, processors, or their representatives to provide all necessary information, grant access to all personal data and other information required for exercising their powers, as well as access to all premises, facilities, and equipment of data controllers and processors. They also inform data controllers and processors about possible violations of the law, and so on.

The Commissioner has the authority to take certain corrective measures, such as issuing a warning to a data controller or processor in case of a breach of the law, ordering them to comply with a request from the data subject regarding the exercise of their rights, instructing the data controller and processor to align their processing activities with the Law on Personal Data Protection in a specific manner and within a specified timeframe, ordering the data controller to inform the data subject about a breach of their personal data, imposing temporary or permanent restrictions on processing activities, imposing a monetary fine based on an offense notice if a violation is found during an inspection, etc.

In the exercise of their powers, the Commissioner may initiate legal proceedings, while the court oversees the acts of the Commissioner carried out in the exercise of their inspection powers.

4.5. Broader regulatory framework

4.5.1. Information security

Information security encompasses all types of information, regardless of their origin and form, whether they are personal data or not. Regulations in this field govern measures and responsibilities for protection against internal and external

risks in information and communication systems, where information can include both personal data and business data owned by companies or other legal entities.

The three fundamental principles of information security closely related to the protection of personal data are confidentiality, integrity, and availability of data. This means that data is processed in a way that ensures adequate protection of personal data, including protection against unauthorized or unlawful processing, as well as accidental loss, destruction, or damage.

Data security entails taking appropriate technical, organizational, and personnel measures. Necessary steps are prescribed to protect information systems and other digital assets from human and technical errors, cybercriminals, and other malicious individuals or organizations.

Therefore, while some protection standards overlap, the field of personal data protection primarily focuses on safeguarding data relating to individuals, while the field of information security guarantees protection of all data from unauthorized access, corruption, or theft. Specific information security standards are prescribed, including ISO 27001, an international standard for information security. It requires organizations to identify risks to information security and select appropriate control measures to enhance protection.

In January 2023, the Directive on measures for a high common level of cybersecurity within the EU, known as the NIS 2 Directive,³³ was adopted at the European Union level, replacing the previous Network and Information Security Directive (NIS Directive).³⁴ The NIS directives prescribe specific standards related to the development of additional rules and procedures to enhance the preparedness of critical sectors in responding to cyber risks. This involves primarily prevention, as well as adequate response to risks and threats, cooperation among all member states, and establishing a culture of security in sectors vital to the economy and society, which heavily rely on ICT, such as energy, transportation, water, banking, financial market infrastructure, healthcare, and digital infrastructure.

The Law on Information Security was modelled after the NIS Directive and applies to systems used by public authorities, systems processing particularly sensitive data, industries of special significance, and critical infrastructure.³⁵ Serbia has extended the scope of the law to include public authorities, thus raising the European standard that doesn't apply to state bodies. The Law on Information Security stipulates that, when exercising their powers and fulfilling legal obligations,

33 Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) <https://eur-lex.europa.eu/eli/dir/2022/2555>

34 Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC

35 Law on Information Security (Official Gazette of RS, No. 6/2016, 94/2017 and 77/2019) https://www.paragraf.rs/propisi/zakon_o_informacionoj_bezbednosti.html [in Serbian]

data processing involving personal data must comply with the Law on Personal Data Protection. The level of data protection within essential ICT systems must correspond to the sensitivity and importance of the data and the potential harm that may arise from unauthorized disclosure, alteration, deletion, or destruction of the data. It should also be in line with regulations governing data protection issues, such as trade secrets, classified information, and personal data.

Trusted resources

Explanations of basic legal institutes and regulations in the field of information security can be found in the publication “Guide for Critical ICT Systems: Information Security”, published by the SHARE Foundation and freely available for download.¹

¹ Guide for ICT systems of special importance: Information security (D. Krivokapić et al., SHARE Foundation, 2017) [in Serbian]



4.5.2. E-commerce, advertising law, and intermediary liability

Buying and selling products and services online have significantly evolved in recent years. E-commerce has become more convenient and easier for both customers and sellers, but it also brings new risks. Since it is practically impossible to conduct an online transaction without processing personal data, data security of users is one of the most significant challenges in e-commerce. Sellers are obligated, among other things, to establish and disclose their privacy policies on their website, inform users about the personal data collected, how it is used, stored, and so on.

The European Directive on Electronic Commerce is fully compliant with the fundamental principles of personal data protection, particularly regarding unsolicited electronic communications and intermediary liability.³⁶

The Directive on Privacy and Electronic Communications applies to the processing of personal data using publicly available electronic communication networks within the EU.³⁷ Providers of electronic communication services are obligated to implement appropriate technical and organizational measures to ensure secure communication. In accordance with the principle of transparency, users must be provided with a detailed breakdown of the charges for using

³⁶ Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce), <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32000L0031>.

³⁷ Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32002L0058>

communication services. The principle of lawfulness dictates that data regarding the GPS location of users can only be processed once it has been anonymised or with the user's consent, which they can withdraw at any time.

Direct marketing is one of the key reasons why organizations collect personal data. In accordance with the Privacy and Electronic Communications Directive, a service provider may process user data for the purpose of advertising or direct marketing, but only if there is consent from the data subjects. The practice of sending electronic mail for direct marketing purposes without disclosing the sender's identity or providing a means for the recipient to opt out of such communications is prohibited. However, communicating via email with existing customers for the promotion of new products and services is allowed. On the other hand, GDPR explicitly states in Recital 47 that processing personal data for direct marketing purposes may be considered a legitimate interest. Nevertheless, the data controller should ensure that all conditions for invoking legitimate interest are met, as failure to do so would render the processing of data for direct marketing purposes unlawful.

Dilemma

After the adoption of the Law on Personal Data Protection, the question arose regarding the legality of processing data for advertising purposes. Is it necessary to obtain prior consent from the individuals targeted by the advertising message for such processing, or can the advertiser rely on legitimate interest as the legal basis for processing if such consent is not obtained? Since the Law on Personal Data Protection does not contain contextual explanations similar to the GDPR preamble, there is no explicit statement that direct advertising can be carried out based on the legitimate interest of the data controller as a legal basis for processing personal data. This possibility is indirectly regulated by the Law on Personal Data Protection through rules on the use of the right to object. However, direct marketing in Serbia is regulated by the Law on Advertising, which defines it as the direct sending of advertising messages to individuals through various media such as telemarketing, mail, catalogues, leaflets, etc.¹ Obtaining prior consent from individuals is required for direct advertising to individuals. Therefore, when aligning business practices with the rules of the domestic legal framework, one should be particularly cautious since it is unclear whether the standards for valid consent in the Law on Personal Data Protection are applicable to consent under the Law on Advertising. A similar dilemma exists in relation to the Law on Consumer Protection and the Law on Electronic Commerce, which regulate direct advertising and sending commercial messages within their respective domains of application. In the absence of unified definitions, the best approach is to analyse each individual situation, taking into account the specific circumstances in which marketing or promotional messages are sent.

¹ Law on Advertising (Official Gazette of RS, No. 6/2016 and 52/2019 - other laws) [in Serbian]



The Serbian Commissioner

The legal basis for processing personal data for direct marketing purposes can only be the consent of the individuals whose data is being processed. This position is not in conflict with the General Regulation because while the GDPR allows legitimate interest to be a legal basis for processing personal data for direct marketing purposes, it leaves it up to the member states to regulate this issue differently in accordance with their legal systems.¹

¹ *Protection of personal data: Positions, opinions and practice of the Commissioner, Publication no. 7, Belgrade, 2022, pp. 148-149 [in Serbian]*



4.5.3. Law of obligations

The fundamental principles of contractual relationships are also reflected in the obligations prescribed by the Law on Personal Data Protection. Accordingly, in line with the principle of autonomy of will, contractual parties are free, within the limits of mandatory provisions, public order, and good customs, to regulate their relationships according to their own will. In addition, the parties are obliged to adhere to the principles of conscientiousness and fairness in establishing relationships and exercising rights and obligations arising from those relationships.

In some situations, there are certain gaps between contract and data protection laws. Analysis from the perspective of contract law is necessary for transactions in which personal data is provided in exchange for a service, as data protection standards do not include the basic principles of law of obligations, such as, for example, the equality of parties. When personal data is used as a means of exchange in contracts, one of the issues to consider is the autonomy of the parties. Persons who submit their personal data for processing often do not have adequate bargaining power, so it can be said that their freedom of contract is limited. On the other hand, the autonomy of the controller's will is also limited, bearing in mind that he cannot process data under any conditions and to an unlimited extent, nor can he ask the data subject to waive the right to withdraw consent.

4.5.4. Cybercrime

The rapid development of modern technology, an increasing number of users, and the abundance of personal data in circulation contribute to the growing importance of cybersecurity. Therefore, personal data not only enjoy administrative and civil protection but are also protected under criminal law.

Some violations of personal data protection can be classified as offenses regulated by the Criminal Code. Within the framework of crimes against human and citizens' rights and liberties, there is a criminal offense of unauthorized collection of personal data. This criminal offense punishes the collection, processing, and use of data that have been unlawfully obtained, disclosed to others, or used for purposes they were

not intended for. A more severe form of this criminal offense is prescribed when committed by a public official in the performance of their duties. Another criminal offense that can be committed in relation to the protection of personal data is the unauthorized publication and display of another person's file, portrait, or image. Criminal liability can be established in case there is no consent from the individual for the publication or display of personal data in another way.

Therefore, personal data must be used for the purpose for which they were collected and in the manner prescribed by the Law on Personal Data Protection. Any unjustified departure beyond the legal boundaries constitutes a violation that can lead to criminal liability for the data controller or processor, as well as third parties who have access to the relevant personal data. To constitute the essence of a criminal offense, it is sufficient to commit the prohibited actions of acquisition, disclosure, or use for other purposes. Due to the fact that these offenses are prosecuted upon private complaint rather than *ex officio*, there is not extensive court practice. Furthermore, many violations of personal data protection in the digital space are committed by anonymous individuals whose identities cannot be determined by citizens, thus preventing them from initiating criminal proceedings.

4.5.5. Free access to information of public importance and open data

The Universal Declaration of Human Rights (1948) provides for the right to seek, receive, and impart information, thereby establishing access to data as an essential element of citizens' rights regarding freedom of thought and expression. In Serbia, this is regulated by the Law on Free Access to Information of Public Importance, including the right of citizens to be informed whether a state body possesses certain information, the right to an availability of information of public importance, that is to be provided with access to documents containing such information, and the right to receive a copy of the document containing the requested information. In case the requested information is already available to the public, the state body has an obligation to direct the interested party to where and when such information was published. The right of access has limited effects on the private sector since it concerns information held by public authorities.

Unlike the right to access information of public importance, which is granted upon request, the concept of open data refers to data that are freely available to everyone from their creation, to be used in any way, for any purpose, without copyright restrictions and control mechanisms, with appropriate attribution. European legal regulations and the Law on Electronic Administration stipulate certain categories of entities that are obligated to open data.³⁸ Primarily, these are state administration bodies and organizations entrusted with exercising public powers. Although they are different concepts, the goal and principles of both access rights and open data are generally the same: transparency and efficiency in providing public services.

38 Law on Electronic Administration (Official Gazette of RS, No. 27/2018) www.paragraf.rs/pro-pisi/zakon-o-elektronskoj-upravi-republika-srbija.html [in Serbian]

The differences between free access to information of public importance and open data are mostly historical and increasingly fading. While the freedom of access to information is based on the idea of citizens' right to be informed and of reducing information asymmetry, as well as on the notion that the state collects and holds information for the benefit of citizens rather than its own, opening data for reuse emphasizes the technological usefulness of such data for further use in innovation and economic progress, and only then focuses on the government's accountability and transparency requirements.

In the context of personal data protection, the right of access is limited, meaning it is only granted to the data subject, regardless of whether the data is held by public authorities or private organizations. The individual has the right to know that their personal data is being processed lawfully, to be informed about the purpose, manner, and other elements of the processing, and to be granted access to the data concerning them. In certain situations, access may be denied, but only when necessary and as a proportionate measure in a democratic society, while respecting the fundamental rights and legitimate interests of the individuals whose data is being processed.

4.5.6. Sectoral legislation

Certain aspects of personal data protection may be regulated by laws that supplement the basic protection standards set out in the provisions of the Law on Personal Data Protection in various fields. Furthermore, the Law on Personal Data Protection imposes an obligation to align specific laws with the new personal data protection system.

For instance, the processing of personal data related to work or employment will be subject not only to the Law on Personal Data Protection but also to the provisions of the Labour Law, as the fundamental legislation governing labour rights. Additionally, financial data such as account numbers, information about funds in an account, creditworthiness, and similar information constitute personal data. In some situations, the data controller has an obligation to provide personal data to the competent state authority. Therefore, the Law on Prevention of Money Laundering and Terrorist Financing imposes an obligation on banks, brokerage firms, payment institutions, and others to provide information, data, and documentation to the Administration for the Prevention of Money Laundering for the purpose of preventing and detecting money laundering and terrorist financing.

Sector specific laws do not comprehensively regulate all issues related to personal data protection but assume the application of general principles, the application of criteria for protecting human dignity, legitimate interests, and fundamental rights of the individuals whose data is being processed, thus complementing the personal data protection system.

4.5.7. Self-regulation

Unlike the old, the new Personal Data Protection Law introduces several new institutions of self-regulation based on the GDPR, namely: the possibility of creating a code of conduct, the possibility of certification (issuance of a certificate on the protection of personal data), as well as the application of the so-called binding business rules.

4.5.7.1. Code of conduct

Relevant articles: *GDPR*, Articles 24, 28, 32, 40-41, 57-58, 64, 70 and 83, Recitals 77, 81, 98-99, 148 and 168; *PDPL*, Articles 59-60.

In order to more effectively implement regulations, associations and other entities representing groups of data controllers or processors have the option to develop a code of conduct. This institute takes into account the specificities of data processing in respective industry sectors and the specific needs of small and medium-sized companies. The codes of conduct should further regulate the principles of fair and transparent processing, provide more detailed explanations of the legitimate interests of the data controller as a legal basis for processing in specific cases, additionally regulate the collection and pseudonymisation of personal data, specify how the rights of individuals whose data is being processed are exercised, address the transfer of data to other countries and international organizations, describe the peaceful resolution of disputes between the data controller and the individuals concerned, outline the mutual obligations of data controllers and processors, and so on.

Given that a code of conduct is optional rather than mandatory, the Law on Personal Data Protection encourages and promotes it. Adopting a code of conduct is beneficial not only to better address the needs of specific data controllers and processors but also to facilitate the demonstration of their compliance with the law.

According to the Law, entities that can develop a code of conduct are associations and other representatives of groups of data controllers or processors, which suggests that a code can be created even by one association as a separate legal entity established in accordance with the Law on Associations. As this provision was transposed from the GDPR, it should be noted that the term “associations” used in the General Data Protection Regulation has a different meaning than the term denoting a legal entity used in Serbian legal system.

The intention of the GDPR is to encompass multiple different entities under the concept of an association, united by a common basis. Therefore, it could be inferred that the intention of the domestic legislator is the same – for the code to apply to self-regulating the behaviour of multiple entities connected by certain common circumstances, rather than just one association. It remains to be seen whether associations, as independent and separate legal entities, will autonomously adopt such codes of conduct to regulate themselves in practice.

The code of conduct must include provisions that enable an accredited legal entity to supervise the implementation of the code by data controllers and processors who have committed to its application.

To develop or amend a code of conduct, a proposal for the code or its amendments is submitted to the Commissioner for their opinion and approval. The Commissioner is authorized to encourage the development of such a code, and if they consider the code to be in compliance with the law and containing sufficient

guarantees for the protection of personal data, the code of conduct or its amendments will be registered and published on the Commissioner's website.

The Law on Personal Data Protection stipulates that the control of code implementation is carried out by “a legal entity accredited for control in accordance with the law regulating accreditation”. However, the control by such an accredited entity does not exclude the control and inspection powers held by the Commissioner regarding the code of conduct.

Conditions that a legal entity must meet to be accredited are prescribed, but it remains unclear which legal entities will be involved in controlling the implementation of the code if voluntary code development becomes established in practice. One of the conditions for a legal entity to be accredited is to “demonstrate to the Commissioner its independence and expertise regarding the content of the code”, but it is not specified in detail how such independence and expertise are demonstrated.

In the event that a data controller or processor violates the code of conduct, the accredited legal entity may, among other measures, temporarily or permanently exclude the data controller or processor from the application of the code. The accredited legal entity is obliged to inform the Commissioner about the measures taken. The measures taken by the accredited legal entity do not affect the powers of the Commissioner or the right of the data subject to file a complaint with the Commissioner or seek judicial protection.

Guidelines

The European Data Protection Board has clarified the procedure for approving codes of conduct at the national and European levels. The minimum criteria that the competent supervisory body requires before accepting the adoption of the code have been established.¹

¹ EDPB, Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679



4.5.7.2. Certification

Relevant provisions: *GDPR* – Articles 24-25, 28, 32, 42-43, Recitals 77, 81, 100, 166, and 168; *PDPL* – Articles 61-62.

For the purpose of demonstrating compliance with the law, especially regarding small and medium-sized companies, the Law on Personal Data Protection introduces the possibility of establishing a procedure for issuing certificates for personal data protection. The purpose of certification is to confirm that the data controller or processor has implemented the Law into their operations and adheres to it.

Similar to the code of conduct, the Commissioner has the authority to encourage the issuance of certificates for personal data protection, as it is a voluntary process. The Commissioner establishes certification criteria, verifies compliance with the certification requirements, and conducts periodic reviews of issued certificates. The Commissioner's criteria for certification are yet to be developed in practice.

Guidelines

The European Data Protection Board defines that certification criteria should reflect the requirements and principles for protecting individuals in relation to the processing of their personal data, and contribute to the consistent application of the GDPR.¹ When developing certification criteria, certain general principles apply: the criteria should be uniform and subject to verification and control, they should take into account the circumstances of the case and the parties involved (two collaborating companies or a company and its client), they should be flexible to be applicable to different types of organizations, including micro, small, and medium-sized enterprises, etc.

¹ EDPB, Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation 2016/679, 23. 1. 2019



Additionally, similar to the accredited legal entity for the code of conduct, the Law also provides for the existence of a certification body that, alongside the Commissioner, has the right to issue certificates. The Commissioner establishes and publishes accreditation criteria for certification bodies, but it remains to be seen how these bodies will operate in practice and whether data controllers and processors will choose to seek certification from certification bodies or from the Commissioner.

The criteria for issuing certificates have not yet been adopted, so the requirements that a data controller or processor must meet to obtain a certificate are not known. However, apart from obligations, the certification process should also offer motivation for legal entities to voluntarily opt for certification. Since certification can help a data controller or processor easily demonstrate compliance with the law during inspections, it can lead to a competitive advantage in the market by positively impacting the controller's reputation as a market participant. On the other hand, possessing a certificate does not affect the prescribed rights and obligations of data controllers regarding the processing of personal data, nor does it affect the inspection and other powers of the Commissioner. In other words, having a certificate does not automatically guarantee or ensure ongoing compliance with the law, but it can be utilized as evidence of compliance. A certificate that has been issued can expire or be revoked, so the certified entity must continue to ensure that it complies with the Law on Personal Data Protection when processing data.

Certificates are issued for a period of up to three years and can be renewed provided that the certificate holder continues to meet the criteria for its issuance. The Commissioner or the certification body may revoke a certificate if it is determined that

the certificate holder no longer meets the necessary criteria. The Commissioner maintains and publishes a list of certification bodies and issued certificates on their website.

4.5.7.3. Binding corporate rules

Relevant provisions: *GDPR* – Articles 4 and 47, Recital 110; *PDPL* – Articles 4 and 67.

Internal rules on personal data protection are considered binding corporate rules under the Law. They are adopted and implemented by a data controller or processor with residence or registered office within the territory of the Republic of Serbia for the purpose of regulating the transfer of personal data to a data controller or processor in one or more countries within a multinational company or group of economic entities.

Therefore, binding corporate rules relate to data transfers within multinational companies. This practically means that multiple companies belonging to the same group and having a common ultimate owner from different countries (corporate groups) can establish their internal rules on personal data protection to regulate the transfer of personal data to a data controller or processor outside the territory of Serbia but within the same corporate group. This allows them to regulate the transfer of personal data without applying the complex data transfer rules prescribed by the Law on Personal Data Protection.

The Commissioner approves binding corporate rules if they meet the following conditions: they have a legal binding effect, each member of the multinational company or group of economic entities applies and enforces them, including their employees; they explicitly ensure the exercise of the data subjects rights; they define the structure and contact details of the multinational company or a group of business entities; they specify the transfer of personal data, types of personal data, processing activities, purpose, data subjects, and the name of the country to which the data are transferred; they prescribe the obligation of their own implementation; they determine the application of general principles of personal data protection and the rights of individuals whose data are processed, as well as the means of exercising such rights; they define the acceptance of responsibility by the data controller or processor within the territory of the Republic of Serbia for any violation committed by another member of the corporate group with a registered office or residence outside Serbia unless the data controller or processor proves that the other member is not responsible for the event causing harm; they specify the powers of the data protection officer; the complaint procedure; the cooperation with the Commissioner, etc.

If binding corporate rules meet the legal requirements, the Commissioner approves them within 60 days from the date of the approval request submission. However, since this pertains to a multinational group of companies, it remains to be seen how the binding corporate rules approved by the Serbian Commissioner will be applied (and possibly further verified) by the competent authorities for personal data protection in countries where other related companies of the same corporate group are based. There is also the question of what happens if a Serbian company, which is part of a multinational corporate group, has not adopted binding corporate

rules, but they have been adopted in another country by another member of the corporate group. According to the Law, the Commissioner would need to approve such binding corporate rules, even if they have already been approved by the competent authority of another country.

4.5.7.4. Ethical guidelines for the development and application of reliable and responsible artificial intelligence

Artificial intelligence (AI) has become a hot topic in recent years, discussed in professional, academic, and other circles. There is a debate about the possibilities of AI, as well as the numerous challenges it brings. Alongside its many advantages, the increasing prevalence and rapid development and implementation of AI raise issues of unauthorized data usage, asymmetry of information in algorithmic decisions, disregard for basic human rights, lack of transparency, and the question of accountability for AI-driven decisions.

It is becoming crucial to establish rules at the industry level, leading states, international organizations, civil society, and other forums to develop legal and ethical standards for the application of AI systems. The ethical framework commonly encompasses topics such as privacy, accountability, security, transparency, equality, professional responsibility, and the promotion and enhanced protection of human rights. At the European Union level, the Ethics Guidelines for Trustworthy Artificial Intelligence were adopted in April 2019.³⁹ These guidelines represent a set of fundamental standards that governments, manufacturers, service providers, and users should follow to ensure that AI systems do not violate human dignity, rights, and fundamental freedoms, particularly regarding data protection. Following the European regulations, Serbia has adopted the Ethical Guidelines for the Development, Application, and Use of Reliable and Responsible Artificial Intelligence in 2023.⁴⁰

Data management is regulated to ensure accuracy, security, and accessibility of data for the preservation of their quality. Data controllers are obliged to provide lawful access to data while respecting individuals' privacy, all in accordance with personal data protection regulations. Furthermore, the Strategy for the Development of Artificial Intelligence for the period 2020-2025 envisages the establishment of certification for AI-based products to ensure personal data protection and compliance with international ethical standards.⁴¹ The certification program will primarily be developed for AI systems established by public administration bodies and the private sector, ensuring security and public trust that the developed solutions comply with regulations governing personal data protection.

39 European Commission, Futurium, Ethics Guidelines for Trustworthy AI <https://ec.europa.eu/futurium/en/ai-alliance-consultation.1.html>

40 National Platform for Artificial Intelligence, <https://www.ai.gov.rs/tekst/sr/189/nacionalna-ai-platforma.php> [in Serbian]

41 Strategy for the development of artificial intelligence in the Republic of Serbia for the period of 2020-2025, https://www.srbija.gov.rs/extfile/sr/437304/strategija_razvoja_vestacke_inteligencije261219_2_cyr.pdf [in Serbian]

5. Scope of application

5.1. Material application

Relevant provisions: <i>GDPR</i> – Article 2, Recitals 15-21; <i>PDPL</i> – Article 3.
--

The law applies to the processing of personal data, whether in whole or in part, carried out in an automated manner, as well as to non-automated processing of personal data that constitutes part of a data collection or is intended for a data collection. The scope of material application is quite broad, and the law excludes its application only in cases of non-automated processing of personal data that does not constitute a data collection, as well as processing of personal data carried out by an individual for their private or household purposes.

5.1.1. Automated processing and data collections

Automated processing refers to the use of technology that enables the automatic processing of data, such as computers and other electronic devices capable of collecting, storing, manipulating, and distributing data to process larger volumes of data quickly and efficiently with minimal human involvement. Processing activities are considered partially automated when they are performed partly manually and partly automatically. For example, manually entering personal data into a digital database, or if several data processing operations, some performed manually and others automatically, are closely interconnected in a logical process. The law does not apply to non-automated processing of personal data that does not constitute a data collection or part of a collection of personal data.

A data collection is any structured set of personal data that can be accessed or searched based on certain criteria, regardless of whether the collection is centralized, decentralized, or categorized on a functional or geographic basis. Therefore, for it to be considered a data collection under the law, the data must be organized and grouped in a structured manner that enables easy and quick retrieval of specific information, whether it's folders in a cabinet, Excel spreadsheets, databases, or similar systems.

If we have a box of various paper documents in a cabinet, some of which contain personal data, it would be considered non-automated processing of data that does not constitute a data collection because they are not organized and structured in a way that allows access or searching based on specific criteria but are randomly placed in the box. However, if we were to structure those papers so that they constitute a searchable collection of personal data based on certain criteria (e.g., the collection is structured in alphabetical order by last name), then the applicable law would govern their processing.

Practice

The concept of a data collection was considered by the CJEU in the “Jehovah's Witness” case.¹ Specifically, the community of Jehovah's Witnesses used a form to collect or process personal data in the course of door-to-door preaching, and the processing of personal data was not carried out by automated means. This raised the question of whether the processed data already constituted or should have been part of a data collection. The Court took the view that personal data collected during door-to-door preaching, assigned to preachers based on geographical sectors for the purpose of organizing follow-up visits, constituted a data collection. The Court concluded that a data collection exists when the “data are structured according to specific criteria that enable easy retrieval for later use. Such a set of data does not necessarily have to include data sheets, specific lists, or other search methods.”



¹ GDPR Hub, CJEU - C-25/17 – Jehovan todistajat

A complaint was filed with the Icelandic supervisory authority stating that *Íslandspostur*, the Icelandic postal service, maintains a separate register of stamp collectors.² Allegedly, all foreign mail addressed to the complainant had been subjected to customs control, whether it was general or traceable mail. In response, the postal service explained that it does not maintain a separate register but, according to the law, all mail in Iceland is subject to customs duties, and as a customs intermediary, the postal service is obliged to conduct customs inspections. The postal service also specified that the selection of mail, which may contain high-value goods, is carried out by employees who gain knowledge through experience for successful identification. As it was not proven that a separate register of stamp collectors exists, the supervisory authority dismissed the complaint. This case would likely have been resolved differently if it could be established that the postal service employees follow a process that requires them to verify every shipment addressed to a specific individual. However, as long as the decision-making regarding this matter is based on the employees' discretionary assessment and experience, it cannot be considered as the processing of personal data covered by the provisions of the GDPR since there is neither automated processing nor a data collection of personal data involved.



² GDPR Hub, Persónuvernd (Iceland) – 2022020332 and 2021112244

5.1.2. Personal or household exemption

Processing of personal data carried out by an individual for their private purposes or the purposes of their household falls outside the scope of the Law, and the

Law will not apply to personal address books, photo albums, personal correspondence, activities on social media and the internet directed towards a limited circle of contacts, and similar cases, if the owner uses them solely for personal, non-business purposes. Therefore, a person who has telephone numbers and names in their mobile phone that they use for personal needs is not considered a data controller, nor will they be required to comply with the legal obligations. However, if an individual initiates a business venture and uses their phone contact list to send business offers to individuals whose phone numbers they have, they become a data controller within the meaning of the law because they are no longer using it solely for personal, private purposes.

For this exception to apply, it is necessary for the processing to be carried out by an individual. Processing carried out by legal entities, regardless of their form (including associations, foundations, endowments, etc.), cannot be covered by this exemption, even if the processing is conducted without commercial interest.

Practice

The answer to the question of whether the purpose of the specific processing includes making personal data accessible to the public constitutes the key criterion distinguishing processing for private purposes from processing subject to the law. If the data being processed, in whole or in part, goes beyond the individual's private sphere, it cannot be considered processing for private purposes. In the case of *Bodil Lindqvist*, the CJEU held that publishing personal data on a publicly accessible blog does not constitute processing for private purposes.¹



¹ GDPR Hub, CJEU – C-101/01 – Bodil Lindqvist

In the *Ryneš* case, the CJEU determined that a camera system installed on a family home for the purpose of property protection cannot be exempted from legal obligations due to the fact that it also captures public space. This position was later confirmed by the Hungarian supervisory authority, which concluded that the use of motion-detection cameras covering large areas of public space in an apartment complex cannot be classified as an exception for processing for private purposes.³



² GDPR Hub, CJEU – C-212/13 – František Ryneš



³ GDPR Hub, NAIH (Hungary) – NAIH-4177-...../2021

To determine whether a particular processing of personal data falls under the exception for private purposes, it is important to first consider whether the processing takes place within a space considered private. If the processing activities occur in a freely accessible environment, such as a public website, it is certain that this exception cannot be applied. Then it is necessary to assess the nature of the relationship between the individual carrying out the processing, the data subjects, and the group of individuals who have access to this data. If these individuals are connected through personal and family relationships, there is a possibility that this exception can be applied. Finally, attention must be paid to the purpose of the processing being pursued in the specific case. If the purpose can be linked to professional or economic activities, the exception will not apply.

Practice

The exception for private purposes does not apply to data controllers or processors that provide the means for this type of processing; they are obligated to comply with the law. The Danish supervisory authority has determined that the use of an online platform through which non-custodial parents can contact authorities, institutions, schools, etc., to obtain information about their children in accordance with Danish regulations, qualifies for a personal exception processing.¹ The supervisory authority has also determined that the platform has a duty to implement technical measures to protect personal data.



¹ GDPR Hub, Datatilsynet – 2020-31-4131

5.2. Territorial application

Relevant provisions: *GDPR* – Articles 3 and 27, Recitals 22-25, 36 and 80; *PDPL* – Articles 3 and 44.

The Law applies to the processing of data carried out by a data controller or processor with a registered office, residence, or domicile in the territory of the Republic of Serbia, within activities conducted in the territory of the Republic of Serbia, regardless of whether the actual processing takes place within that territory. For example, in the case of a data controller with a registered office in Serbia but whose data server is located outside Serbia, the Law's jurisdiction is unquestionable, and the data controller is obliged to comply with the provisions of the Law on the data stored on the server outside the territory of Serbia. Therefore, regardless of where the processing takes place, if it is related to activities conducted by a domestic data controller in Serbia, the Law applies to such processing.

Guidelines

The registered office of a legal entity can be determined based on two different criteria: the criterion of establishment or registered office, and the criterion of actual seat or the place where the legal entity carries out its activities and is managed.

The Serbian Law on Business Organizations defines the registered office as the place of the actual seat within the territory of the Republic of Serbia. This means that the Law on Business Organizations does not address the issue of the international affiliation of business organizations but rather their seat within the Serbian borders.

As for determining the international affiliation of a legal entity, the Law on Conflict of Laws with the Regulations of Other Countries stipulates that the affiliation of a legal entity is determined by the law of the state under which it was established. If a legal entity has its actual seat in another country and not in the country where it was established, and if according to the law of that other country, it has its affiliation, it will be considered a legal entity of that country.¹



¹ Article 17 of the Law on the Resolution of Conflicts of Laws with the Regulations of Other Countries [in Serbian]

The Law on Personal Data Protection applies to the processing of personal data carried out by a data controller or processor with a registered office, residence, or domicile in Serbia within activities conducted in Serbia, regardless of whether the actual processing takes place within the territory of the Republic of Serbia (Article 3). When a foreign legal entity, within the activities carried out by its branch or representation in the Republic of Serbia, processes personal data in Serbia, the question arises whether such processing falls under the Personal Data Protection Law since none of the mentioned laws explicitly regulates this situation..

Regarding the GDPR, it applies to all cases of processing personal data within the business activities of data controllers and processors established within the EU, regardless of whether the processing takes place within the EU or outside of it. In the case of a company operating in multiple different states, the GDPR specifies which location will be considered the main establishment. Recital 22 states that the establishment is considered the place where the effective and real exercise of activity of the legal entity is carried out, regardless of whether it is the registered office or a branch of the legal entity. This understanding has been confirmed by the Guidelines on the Territorial Scope² and decisions of the Court of Justice of the European Union, especially the decision C-230/14 - Weltimmo,³ which extended the concept of establishment to any potential place of real and effective economic activity.



² EDPB, Guidelines 3/2018 on the territorial scope of the GDPR



³ Judgment of the Court (Third Chamber) of 1 October 2015, Weltimmo s.r.o. v Nemzeti Adatvédelmi és Információszabadság Hatóság.

If a data controller established outside the European Union carries out “real and effective activity” within the territory of the EU Member States, even if it is minimal, regardless of its legal form, it may be considered as having an establishment in that EU Member State.

The opinion of the Commissioner is that the concept of a “seat” in the Law on Personal Data Protection should be interpreted in the context of the GDPR, which served as a model for the domestic law to ensure the realization of the right to personal data protection. Therefore, a “seat” within the meaning of the Law on Personal Data Protection is considered to be any effective and actual conduct of activities through stable arrangements, and the legal form of such arrangements is not the decisive factor in this regard, which would include branches and subsidiaries.⁴

⁴ Protection of personal data: Positions, opinions and practice of the Commissioner, publication no. 6, Belgrade, 2021. Case number: 073-14-2211/2019-02, pp. 16-17 [in Serbian]



It should be noted that a domestic company that decides to expand its business beyond the European zone to territories where there are lower standards of personal data protection than those established by the Law on Personal Data Protection and the GDPR, would still need to ensure that it cannot operate in accordance with local standards. For example, if a domestic company decides to organize the data processing of clients in the United States or the United Arab Emirates, where explicit consent and opt-in access are not required according to local regulations, it will not be able to opt for this lower standard because the Law will still be applicable to such processing. Of course, if it decides to incorporate a subsidiary in another country for the purpose of entering these markets, the Law will not apply to its operations since it is a separate legal entity.

The Law also provides for extraterritorial application in cases where a data controller or processor, who does not have a registered office, residence, or domicile in Serbia, processes personal data of individuals with a residence or domicile in Serbia if the processing activities are related to:

- offering goods or services to the individuals on the territory of the Republic of Serbia, regardless of whether payment is required from those individuals for these goods or services; or
- monitoring the activities of the individuals if the activities are conducted on the territory of the Republic of Serbia.

Offering goods and services encompasses various transactions, regardless of whether they involve payment by the data subjects, in order to include those services that appear to be free but use personal data and/or user attention as an alternative currency. For example, the owner of a language learning mobile application operated by a company from South Korea would be required to comply with the Law if they generate advertising revenue through the app in the Republic of Serbia. Monitoring the activities of individuals is particularly relevant for processing activities that are part of business models based on user behaviour tracking, such as targeted marketing.

Dilemma

Does the Personal Data Protection Law apply to a company based outside of Serbia but processing the data of Serbian citizens? The answer to this question depends on several circumstances. Let's take a hotel in Hungary as an example, where our citizen arrives and leaves their personal data: the Law will apply to the data controller in Hungary only if that hotel targets Serbian citizens in some way - by having a Serbian version of its website, having a marketing strategy for people in Serbia, etc. However, if it is a Hungarian hotel that does not have a website in Serbian, does not advertise in the Serbian market and doesn't target Serbian citizens in that way, and if the Serbian citizen has randomly chosen that hotel, the Law does not apply to that Hungarian data controller. Therefore, for extraterritorial application, it is crucial that there is an element of business targeting Serbian citizens or monitoring their activities.

The Serbian Commissioner

The legal position of a branch is regulated by the Law on Companies, according to which a branch is a separate organizational part of the company located in the territory of the Republic of Serbia through which the company conducts its activities. The branch does not have the status of a legal entity and acts on behalf and in the interest of for the account of the company in legal transactions. Therefore, the branch of a foreign company represents its separate organizational part, which does not have the status of a legal entity and can perform certain activities in order to conclude legal transactions on behalf of that company and can only conclude legal transactions related to its current business operations, while the foreign company is liable for its obligations towards third parties. Considering the above, neither the branch nor the representative office have the status of a data controller or processor; instead, the legal entity whose separate organisational part is the branch or representative office has that status. However, in order to ensure the exercise of the right to personal data protection in Serbia, the term "registered office" used in the Law on Personal Data Protection needs to be interpreted in accordance with the GDPR, specifically Recital 22, which stipulates that the registered office/ establishment implies any effective and real conduct of activities through stable arrangements, whereby the legal form of such arrangements is not a decisive factor in this regard. This is also confirmed by the EDPB guidelines on the territorial application of the Regulation. Therefore, the Commissioner's decision is that when a foreign legal entity, within the activities carried out by its branch or representative office in Serbia, processes personal data, the Law on Personal Data Protection applies to that processing.¹

¹ Ibid

Therefore, the Personal Data Protection Law applies to foreign data controllers and processors who have their registered office, domicile, or residence abroad if they target residents of Serbia for the purpose of selling goods or offering services, or if they monitor their activities in the territory of Serbia. It should be emphasized that the application of the Law in these cases does not depend on the nationality of the individuals whose data is processed but takes into account whether the individuals have domicile or residence and whether they are present in the territory of the Republic of Serbia. Thus, the processing of personal data of an Egyptian citizen studying in Belgrade would be subject to the application of the Personal Data Protection Law if an Egyptian application tracks their activities in the Republic of Serbia. The GDPR provides similar provisions, but it applies to controllers and processors outside the EU who offer goods and services to EU residents or who monitor the activities of individuals if such activities are carried out in the territory of the EU.

Guidelines

In its Guidelines on the GDPR territorial scope, EDPB states that the mere fact of processing personal data of individuals in the EU by a data controller or processor outside the EU is not sufficient for the application of the GDPR.¹ It requires an element of targeting individuals in the EU by offering them goods or services or by monitoring their behaviour (for example, through the use of tracking cookies). If a Chinese website, for example, sells goods by using one of the languages spoken in the EU, allows payment in European currency, and enables delivery to a European address, the GDPR would be territorially applicable to the data controller collecting data through this website. However, if a Chinese bank has a Danish citizen with a residence in China as a customer, and the bank operates solely in China without any business activities targeting the EU market, the GDPR would not apply to the processing of personal data of the Danish citizen.

Recital 24 of the GDPR clarifies the concept of “monitoring of the behaviour” as a processing activity that involves tracking the behaviour of individuals on the internet, including the potential subsequent use of personal data processing techniques that consist of profiling the individual, particularly for making decisions concerning them or for analysing or predicting their personal preferences, behaviour, and attitudes. Additionally, the EDPB expanded the scope of this recital to include not only tracking individuals on the internet but also tracking through other types of networks or technologies involving the processing of personal data, such as tracking through wearable or smart devices..

This interpretation should also be relied upon in the case of the extraterritorial application of domestic legislation.

¹ EDPB, Guidelines 3/2018 on the territorial scope of the GDPR (Article 3) – Version for public consultation, 16. 11. 2018.



Practice

In the digital economy, it is common for a data controller to engage in cross-border offering of goods or services while simultaneously monitoring the activities of individuals to whom they provide services. For example, the Norwegian supervisory authority determined the applicability of the GDPR to the American company Grindr, which offered services and tracked user behaviour for the purpose of providing location-based social networking and dating services for members of the LGBTQ community.¹ In this case, multiple GDPR violations were identified, and Grindr was fined 6.4 million EUR.



¹ GDPR Hub, Territorial scope of the GDPR

The French supervisory authority CNIL determined the extraterritorial application of the GDPR to the American company Clearview AI, which developed a tool for face recognition using publicly available images and videos on the internet.² Although the company was established in the United States and did not have a presence in the European Union, it processed personal data of European citizens by collecting online content featuring faces of individuals, including minors. As the business model primarily targeted legal entities that could search the database to potentially identify individuals, without offering goods and services to European citizens, the supervisory authority could establish the extraterritorial application of the GDPR solely based on the concept of “monitoring of behaviour”. CNIL therefore determined that it was sufficient for the processing to be linked to monitoring, and it was not necessary for behavioural tracking to be the primary purpose of the processing. Multiple GDPR violations were identified, and CNIL imposed a fine of 20 million EUR on Clearview AI. Additionally, the same company was fined significant penalties by the Italian (20 million EUR) and British (7.5 million GDP) supervisory authorities on the same grounds of extraterritorial jurisdiction.



² GDPR Hub, CNIL (France) – Délibération SAN-2022-019

The High Court of England and Wales decided that the processing of personal data of an Israeli and British resident within the journalistic activity of an American media outlet does not fall within the territorial scope of the GDPR, even though the media outlet offers services and tracks the behaviour of EU citizens.³



³ “It should be noted that this case deals directly with the GDPR as the issues at hand arose prior to Brexit.” GDPR Hub, Soriano v Forensic News LLC

The court considered whether the media outlet had a presence in the EU, whether it offered goods and services to individuals in the EU, and whether it monitored the behaviour of individuals in the EU. Firstly, the court determined that the media outlet did not have any stable arrangements in the United Kingdom, citing the fact that the news website did not have employees or representatives in the UK, while the number of subscribers in the UK was small. Secondly, the court held that the media outlet did not directly target consumers in the UK with its products and services. The fact that the UK was listed as an option for delivering the offered goods was disregarded due to lack of actual purchases. Specifically, the court found that only one baseball cap was purchased from the website in the UK. Finally, the court considered that tracking customers did not warrant extraterritorial application of the GDPR. The news website used cookies for behavioural profiling or tracking in the context of targeted advertising. The court determined that this was not the type of “monitoring” envisioned by the GDPR. The argument used by the court was that the website did not use such tracking for news dissemination but engaged in an activity unrelated to the claimant's lawsuit.

As none of the three criteria examined were met, the court decided that the GDPR does not apply in this case.

6. Basic concepts

6.1. Personal data

Relevant provisions: <i>GDPR</i> – Articles 2, 4, 9-10, Recitals 1, 2, 15, 17-20, 26, 30, 51; <i>PDPL</i> – Article 4.
--

Personal data is any information relating to an identified or identifiable natural person, directly or indirectly. As stated in the text of the Law itself, personal data can include any data that identifies us, such as our name, address, ID number, phone number, bank account number, etc., or data that reveals something about us, such as hair colour, favourite TV series, political views, recreational habits, or the type of mobile phone we use.

The quality of the personal data, whether it represents a fact, falsehood, or opinion, is not relevant. Personal data can be any type of content, such as handwriting, a child's drawing, a blood sample, a scent, or metadata related to the time of accessing specific content. The form of information is also not important; personal data can be expressed in written or digital form, in a database, photo, video, or audio recording, or in any other type of record or storage that allows accessing the information again. Additionally, encrypted data, which is readable only to authorized recipients, can also qualify as personal data.

Finally, personal data must be connected to an element that identifies or can identify the data subject. Identifiers in practice can be data such as a natural person's name and ID number, which can directly establish the uniqueness and individuality of a specific person by distinguishing them from all others. Identification can also occur indirectly by combining information that is not means of identification (gender, age, place of residence, profession, etc.) but, due to their nature and interrelation, enables the identification of the individual.

We live in an age where seemingly no data is insignificant and unusable. Our activities that take place through digital, and increasingly physical spaces, generate large amounts of diverse data. These data are processed on the internet, such as IP addresses, IMEI numbers of the devices we use to access the network, passwords, our email and social media accounts, activity history on such accounts (shares, likes, clicks), internet search history, and so on. Although many digitally generated data may not appear as personal data at first glance, they may contain information that can describe the personality or behaviour

of a particular individual and often indirectly identify the person themselves. For example, data on the amount of internet content consumed by a specific mobile subscriber can reveal their daily routines and, with high precision, determine the periods of the day when they are not at home based on the analysis of the times when the mobile device is not using internet traffic due to being connected to a Wi-Fi network. On the other hand, an IP address will not only enable tracking of the behaviour of a specific individual but may also independently lead to their identification. Therefore, categorizing certain data as personal data sometimes requires considering the entire context of a specific case, and the legal definition of personal data is broad enough to be tested in various situations and unforeseen events that may affect fundamental rights and freedoms.

When determining personal data, we may encounter various uncertainties, so each situation needs to be addressed individually. The same data can be treated differently depending on the context. A certain piece of information may qualify as personal data for one controller because they are in a position to link the data to a specific individual, while for another controller who does not have the ability to make such a connection, the same data does not qualify as personal data. Prescription data containing no patient identification may not appear to be personal data because there is no way to identify the patient. However, the relationship between the most commonly prescribed medications and doctors is of interest to the pharmaceutical industry and their marketing departments, so in that context, this information would represent personal data about the doctors.

Dilemmas

Is a handwritten signature considered personal data? Yes, if it can be linked to a specific or identifiable individual.¹ Generally speaking, to categorize a piece of data as personal data, it is important to determine whether it can indirectly or directly identify an individual. If the answer is affirmative, then it qualifies as personal data.








Is health information that is not closely determining a natural person and used for statistical purposes considered personal data? If such information cannot be used to identify an individual, it does not qualify as personal data. Anonymous data is used for statistical purposes, data that can no longer be linked to specific individuals. For example, the information that a certain number of people were affected by COVID-19 in a specific territory in May 2021 represents a set of anonymised data from which it is not possible to determine the identities of people in question.

¹ *Protection of personal data: Positions and opinions of the Commissioner, Publication no. 2, p. 13 [in Serbian]*



Practice

In processes conducted before the Court of Justice of the European Union, a range of data has undergone a test of qualification as personal data, and for many of them, this question is no longer a dilemma.

Personal data	CJEU decision	
Name, date of birth, nationality, gender, ethnic origin, religion, and language	YS and Others ¹	
Place of birth, citizenship, marital status, gender, records of entry and exit from the country, residence and domicile, data on issued passports, previous residence statements, reference numbers issued by authorities	Huber ²	
Data on earned and unearned income and property of individuals in a municipality	Satakunnan Markkinapörssi and Satamedia ³	
Data on salaries of public sector employees	Österreichischer Rundfunk u.a. ⁴	
Person's name in connection with their telephone coordinates or data about working conditions or hobbies	Lindqvist ⁵	
Working hours and break schedules	Worten ⁶	
Dynamic IP address	Breyer ⁷	

¹ GDPRHub, CJEU – C-141/12 and C-372/12 – YS v. Minister voor Immigratie, Integratie en Asiel

² GDPRHub, CJEU – C-524/06 – Huber



³ GDPR Hub, CJEU – C-73/07 – Satamedia

⁴ GDPR Hub, CJEU – C-465/00 – Österreichischer Rundfunk

⁵ GDPR Hub, CJEU – C-582/14 – Patrick Breyer

⁶ GDPR Hub, CJEU – C-342/12 – Worten

⁷ GDPR Hub, CJEU – C-101/01 – Bodil Lindqvist

Personal data	CJEU decision	
Video surveillance footage	Ryneš ⁸	
Content of written exams	Nowak ⁹	

⁸ GDPR Hub, CJEU – C-212/13 – František Ryneš

⁹ GDPR Hub, CJEU – C-434/16 – Peter Nowak

Judgment C-582/14 supports the view that the IP address is personal information.¹⁰ According to the decision, a dynamic IP address can be considered personal data for a controller if there is a reasonable expectation that the specific controller has the means to determine to whom that address belongs, in other words, has the ability to identify the owner of the IP address. The same position was taken by our Commissioner in a case they considered in 2020.¹¹

¹⁰ Judgment of the Court (Second Chamber), 19 October 2016, C-582/14, Patrick Breyer v Bundesrepublik Deutschland

¹¹ *Protection of personal data: Positions, opinions and practice of the Commissioner, publication no. 6, Belgrade, 2021. Case number: 073-14-2369/2019-02, p. 48-49 [in Serbian]*

A case was brought before the Croatian supervisory authority (AZOP) in which a real estate agency published a photograph on its website showing a property, including a person wearing a jacket and a protective mask.¹² AZOP concluded that such a photograph does not constitute personal data due to the circumstances that the identity of that person cannot be determined by objective factors available to an average person who is not acquainted with the person in the photograph, simply by looking at the attached photograph. In the specific case, the photograph was unclear, and the person was not visible (mostly covered by a protective mask).

¹² GDPR Hub, AZOP (Croatia) - Decision of 16 November 2021 - Real Estate Agency

The Serbian Commissioner

After an individual requested a complete report on the assessment of damages and photographs of vehicle damage from an insurance company regarding a traffic accident, the insurance company took the position that these were data related to a movable property and were not covered by the rights individuals have under the Personal Data Protection Law. Considering the established facts, the Commissioner ordered the insurance company to provide the individual with a copy of the photographs of the passenger vehicle involved in the traffic accident, stating that vehicle data itself does not constitute personal data, but becomes personal data when it can be linked to an individual. As the requested photographs are part of the records held by the controller, formed in relation to the individual's claim for compensation, and considered a collection of personal data, it is undisputed that they are indeed personal data. According to the Commissioner's assessment, there are no obstacles for the controller to provide the individual with a copy of the photographs.¹

¹ *Protection of personal data: Positions, opinions and practice of the Commissioner, publication no. 6, Belgrade, 2021. Case number: 072-16-2201/2020-06, pp. 46-48 [in Serbian]*



Practice

The Norwegian supervisory authority fined a controller for live streaming camera footage on a YouTube channel.¹ The controller installed a rotating camera on the roof of their headquarters, recording a public road, parking area, entrance to several stores, a bank, city council, and several other buildings. The live stream was broadcasted on the company's YouTube channel with over a thousand followers. The recordings were stored on a server for 14 days before deletion and were shared multiple times with the police regarding events captured by the camera in the city centre.

The controller provided notice of the camera's presence on their Facebook page and claimed that the camera was installed as a service to the residents of the area. They also stated that due to distance and poor video quality, it was not possible to identify license plate numbers or individuals passing by, which the supervisory authority agreed with. However, the supervisory authority emphasized that it was possible to identify the type of cars being driven, the type of clothing people were wearing, hair colour, etc., and that prior knowledge of someone's movements, shopping habits, appearance, or the car they drive could potentially identify the person being recorded by the camera. Therefore, the supervisory authority concluded that the camera processed personal data.

¹ GDPR Hub, Datatilsynet (Norway) – 20/01627



6.2. Data subject

Relevant provisions: *GDPR* – Article 4, Recitals 14 and 27; *PDPL* – Article 4.

Personal data refers to data related to a natural person, specifically excluding legal persons, animals, or similar entities. However, if data about a legal entity also pertains to an individual person, such data is considered personal data.

Although the Personal Data Protection Law does not explicitly state that the data subject must be alive, the general stance is that the law does not apply to personal data of deceased individuals. Within the European legal framework, recital 27 of the General Data Protection Regulation specifies that it does not apply to deceased persons, while allowing EU member states to establish rules regarding the processing of personal data of deceased individuals through national legislation. Additionally, certain protection of personal data of deceased individuals may be provided through legislation that does not specifically regulate personal data protection. For example, the Serbian Law on Public Information and Media provides the possibility for family members of a deceased individual to give consent for the publication of information about the deceased's private life, as well as the right for family members to file a lawsuit on behalf of the deceased in case of publishing incomplete or inaccurate information about the deceased that may harm their rights or interests.⁴²

The Serbian Commissioner

After an individual submitted a request to a bank in Belgrade, seeking information and a copy of data processed by the bank related to deceased persons, the bank informed the requester that it was unable to fulfil the request due to the obligation to maintain bank secrecy. The bank took the position that it can provide data on deceased individuals upon request from authorised bodies involved in probate proceedings. In the complaint filed with the Commissioner, the requester stated that the bank did not allow them to exercise their right to access data about deceased individuals. Since the Law does not contain provisions specifically addressing deceased individuals, the Commissioner took the stance that there was no legal basis for its application in this particular case. Hence, the complaint regarding the denial of the right to access data about deceased individuals was not justified.¹

¹ *Protection of personal data: Positions, opinions and practice of the Commissioner, publication no. 6, Belgrade, 2021. Case number: 072-16-246/2020-06, p. 18 [in Serbian]*



⁴² Law on Public Information and Media (Official Gazette of RS, No. 83/2014, 58/2015 and 12/2016 – authentic interpretation)

6.3. Special categories of personal data

Relevant provisions: *GDPR* – Article 9, Recitals 34-35, 50-56; *PDPL* – Article 17.

Personal data relating to racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic and biometric data, as well as data concerning health, sexual life, or sexual orientation of a natural person, are treated as special categories of personal data. These are particularly sensitive data that require a higher level of attention in processing compared to other personal data. The legal framework generally prohibits the processing of special categories of personal data, with specific exceptions that are exhaustively listed.

The list of special categories of personal data is comprehensive and closed, as are the circumstances under which their processing is exceptionally allowed. While some categories are clearly understood as special, others may require additional explanation.⁴³

1. Racial or ethnic origin

“Racial origin” refers to biological ancestry and inherited characteristics,⁴⁴ while “ethnic origin” pertains to cultural aspects that characterize a group of people, such as language, history, tradition, shared values, and a sense of community.

2. Political opinions

In the absence of a clear definition, it is assumed that any kind of clear, unequivocal statement, support or rejection of a particular political party or ideological organization can be placed under this category, as well as data on subscription to a politically oriented magazine, participation in offline and online petitions, liking and sharing political content on social networks, attendance at meetings or demonstrations.

3. Religious or philosophical beliefs

This category includes not only information about “traditional” religious affiliation but also other value orientations (e.g., pacifism, socialism), membership in naturalistic religions or religious sects, atheism, anthropomorphism, or membership in ideological organizations, as well as other information about religious and philosophical beliefs.

4. Trade union membership

Membership or activities that reveal a close association with a trade union, such as the status of a union representative, documents proving membership in a specific union, involvement in establishing a union, participation in union affairs management, subscription to union publications, distribution of union documents (publications, promotional materials), or expressing interest in union activities.

43 GDPR Hub, Article 9 GDPR, https://gdprhub.eu/Article_9_GDPR

44 Although using this term, the lawmaker has explicitly distanced themselves from theories which attempt to determine the existence of separate human races (Recital 51 of the GDPR Preamble).

5. Genetic data

Personal data related to inherited or acquired genetic characteristics of a natural person that provide unique information about the physiology or health of that person, particularly data obtained through analysis from a biological sample.

6. Biometric data

Personal data obtained through specific technical processing related to the physical, physiological, or behavioural characteristics of an individual that allows or confirms their unique identification, such as facial images or fingerprints.

7. Data concerning health

Data related to the physical or mental health of a natural person, including the provision of healthcare services, disclosing information about the person's health status.

8. Data concerning sexual life or sexual orientation

Personal data relating to heterosexuality, bisexuality, homosexuality, and transsexuality, including information about intended or undergone gender reassignment, or about living in a registered civil partnership or same-sex marriage, information related to sexual practices, and other actions that may reveal sexual orientation.

Praksa

It seems that eight types of special data should be interpreted quite broadly, not only encompassing data that directly contains sensitive information (such as a membership application to a political party or a medical diagnosis report) but also data from which sensitive information can be inferred. Signing an online petition related to political demands or a photograph of a person with a prescribed medication box, reveal something sensitive about the individual (either their political views or health condition) and therefore should be treated as special categories of personal data. The conclusions of the CJEU express this clearly: “The expression 'data concerning health' must be interpreted broadly to include all information relating to the health of an individual, both physical and mental.”¹ The Austrian supervisory authority in its decision established that a negative COVID-19 test result constitutes data concerning health.²

¹ CJEU, 6. novembar 2003, Bodil Lindkvist, C-101/01, margin no. 50

² GDPR Hub, DSB (Austria) – 2021-0.101.211



The intention of the legislator is to establish, as a basic rule, a prohibition on processing special categories of personal data while simultaneously providing exceptions in which their processing is allowed. When processing special categories of personal data as particularly sensitive data, the principle of minimization should certainly be applied, meaning processing should be limited to the minimum necessary to achieve its purpose.

Dilemmas

In the context of a supervisory procedure in early 2022, the Spanish supervisory authority did not find a violation of processing special categories of personal data in the case of *Grindr*, a globally popular social networking app for gay, bisexual, transgender, and pansexual individuals.¹ The authority determined that the app does not directly collect data related to users' sexual orientation and that the platform does not even have a field for entering such information, although users can voluntarily share this data within their public profile or in private messages exchanged with other users. The supervisor found that this information is not accessible to third parties for advertising purposes. They avoided making a decision on whether the use of the app reveals sexual orientation, taking into account the platform's claim to be open to all sexual orientations and gender identities, and that the app is used by individuals of heterosexual orientation “out of curiosity or to better understand themselves through interaction with other users”. On the other hand, in a 2021 case the Norwegian supervisory authority disagreed with *Grindr's* assertion that user data does not reveal their sexual orientation.²

¹ GDPR Hub, AEPD (Spain) – E/03624/2021

² GDPR Hub, Datatilsynet (Norway) – 20/02136-18, Special categories of data under Article 9.



Dilemmas

Is a photograph considered biometric data and therefore a special category of personal data?

According to the legal definition, biometric data is personal data obtained through specific technical processing related to the physical, physiological, or behavioural characteristics of an individual that allows for or confirms their unique identification, such as a facial image or fingerprint data. Accordingly, the Law on Personal Data Protection categorizes a photograph as biometric data only if it is created through specific technical processing related to the physical characteristics of a specific individual. Apart from this definition of biometric data, the Law does not mention photographs specifically..

On the other hand, the General Data Protection Regulation clarifies in Recital 51 of the preamble that the processing of photographs generally does not constitute the processing of special categories of personal data, as a photograph is considered biometric data only if it is processed through specific technical means that enable unique identification or identification of individuals. This means that an ordinary photograph of a person would not be considered biometric data.

It is important to note that the legal framework prohibits the processing of biometric data solely for the purpose of unique identification, and the processing of biometric data for other purposes is generally not covered by the regime that applies to special categories of data but falls under the general regime.

Guidelines

The European Data Protection Board guidelines on the processing of health data for scientific research purposes in the context of the COVID-19 pandemic state that health data is personal data relating to the physical or mental health of an individual, including data about their health that can be disclosed through the provision of healthcare services.¹ According to these Guidelines, health data can be obtained from various sources:

1. Information collected by healthcare professionals in patient records (such as medical history, examination results, and treatment).
2. Information that becomes health data through cross-references with other data, revealing health status or health risks (for example, assuming a person has a higher risk of a heart attack based on high blood pressure measured over a certain period).
3. Information from self-assessment surveys, where individuals answer questions about their health (such as reporting symptoms).
4. Information that becomes health data due to its use in a specific context (for example, information about recent travel or presence in a COVID-19 affected region processed by a medical professional for diagnosis).

¹ EDPB, Guidelines 03/2020 on the processing of data concerning health for the purpose of scientific research in the context of the COVID-19 outbreak



Practice

The opinion of the Advocate General of the Court of Justice of the European Union is that if an online search engine is requested to remove search results related to a specific individual and special categories of personal data, the service must assess, in the specific case, whether the right to privacy and the protection of personal data outweigh the public's right to access that information and the right to freedom of expression of the person who published such data.¹



¹ CJEU, Advocate General's Opinion in Case C-136/17, G.C. and Others v CNIL, 10. 1. 2019

6.4. Data processing

Relevant provisions: *GDPR* – Article 4; *PDPL* – Article 4.

The processing of personal data includes any action (automated or non-automated) taken in relation to personal data, such as collection, recording, organization, retrieval, erasure, destruction, storage, and many others. Although the term “processing” implies active behaviour, passive actions such as keeping and storing data are generally considered as data processing.

The intention of the legislator is not to exhaustively list the actions that can be considered as processing of personal data, but rather to enumerate the most common and typical processing actions. Therefore, it is important to bear in mind that any interaction with personal data constitutes their processing, and it is difficult to imagine a situation where someone comes into contact with personal data without it being considered as processing. Hence, any use or handling, including access to personal data, regardless of the duration or nature of such processing, will be deemed as processing under the law.

Dilemmas

Does merely storing data on a server, without accessing the data, constitute processing of personal data?

Although keeping data is a passive action, even when the entity keeping the data does not access it, the Law considers it as processing of personal data.

If my company receives documents containing personal data and immediately forwards them to another recipient without making copies, does the act of receiving and briefly holding the documentation constitute processing?

The act of receiving and forwarding data, even without accessing or copying it, is also considered as processing under the Law. Depending on the nature of the processing activity, the data controller will determine the appropriate steps to take in compliance with the applicable data protection laws. Generally, if the processing is less invasive and of shorter duration, the data protection measures implemented will be simpler.

Processing of personal data is a frequent practice in regular business correspondence. Tables and databases are manipulated daily, their content is improved, merged, and forwarded via e-mail and other means of communication. Sometimes it is necessary for organizations to become aware that each of these procedures can represent a separate processing action, which requires specific treatment.

Practice

A real estate agent accidentally sent an e-mail to everyone registered for the project with an attached spreadsheet containing the personal information of everyone who registered for the project. The Dutch court determined that sending a table containing individuals' contact information via email constitutes processing of personal data.¹



¹ GDPR Hub, Rb. Rotterdam – 9436020 \ CV EXPL 21-30289

The rapid development and implementation of information technologies, artificial intelligence, robotics, and the Internet of Things raise numerous dilemmas regarding the processing of personal data. Particularly interesting are the many examples of digital business transformation that fundamentally involve innovative data processing operations. Establishing systems of smart biometric cameras or drone networks for monitoring public and publicly accessible areas will involve a variety of personal data processing operations. It is essential to individually identify each of operations through a comprehensive analysis of the legal, organizational, and technical aspects of the system. However, in practice, the data controller may often focus on the most obvious processing operations, while many less obvious ones may go unnoticed due to the technical complexity of the project and insufficient transparency.

Practice

A German court has determined that the mere installation of a water meter with a radio module can be considered as data processing.¹ Although the installation does not directly process data in terms of storage, the necessary preparation, which is undoubtedly aimed at enabling data processing, constitutes data processing.



¹ GDPR Hub, VG Cottbus – VG 4 K 1191/19

When the French police began using drones to monitor compliance with isolation and other restriction measures during the COVID-19 pandemic, a series of questions arose before the local supervisory authority. CNIL assessed that there was no doubt that it involved the processing of personal data, as the drones were equipped with high-resolution cameras capable of zooming, which undeniably can capture images that can identify individuals.¹



¹ GDPR Hub, CNIL – SAN-2021-003

Dilemmas

When the Commissioner initiated an inspection of the Faculty of Law at the University of Belgrade in 2016, they established that a video camera located in front of the service counter was recording and simultaneously broadcasting the footage on the faculty's website.¹ Considering that the live video feed could reveal the faces of students waiting in line, potentially leading to their identification, there was no dispute that it involved the processing of personal data. The purpose of this processing was to inform students about the length of the queue and enable more efficient time management, but it was determined that, in accordance with the principle of minimization, there was no justification for processing personal data since the purpose could be achieved without such processing. As a result, the camera's technical settings were adjusted to lower the resolution of the footage to a level that does not allow for the recognition of students' faces in the queue while still enabling the determination of queue length. In this way, the Faculty of Law changed its practice by implementing a technical measure that prevented the processing of personal data, effectively exempting it from the application of data protection regulations.



¹ Kuris, "Students under constant camera surveillance: Future lawyers as reality stars", 02.11.2016. [in Serbian]

Practice

An exception to the rule that even passive keeping of data constitutes data processing occurs when an individual is entirely passive regarding the personal data that is somehow accessible to them. In a case before the Higher Administrative Court in Germany, it was concluded that the mere existence of a file in the basement premises of the property owner did not fall within the concept of personal data processing.¹



¹ GDPR Hub, OVG Hamburg – 5 Bs 152/20

Considering that the concept of data processing refers to an operation or a series of operations related to personal data, the Court interpreted the term “operation” to indicate that processing does not describe a state but rather an action, and that data processing transforms a state (particularly knowledge and data structure) into another state. Therefore, the Court took the view that the lack of attributable, voluntary human activity directed towards the files continuously stored in the basement premises since the hospital, which had been the data controller, ceased to exist did not constitute data processing by the property owner..

Dilemmas

During the COVID-19 pandemic, the protection of public health has prompted the use of technology in many social situations involving the processing of personal data, particularly data concerning individuals' health status, which represents a special category of personal data.

The French court ruled that scanning facial temperature with thermal cameras constitutes the processing of personal data.¹ In the specific case, fixed and portable thermal cameras were installed at the entrances of schools to monitor individuals' facial body temperature. In cases where an elevated temperature was detected, the municipality would initiate a procedure to notify the individual of the need to immediately leave the school. Furthermore, the judge considered that body temperature is sufficiently accurate to identify an individual and must be regarded as a special category of personal data.



¹ GDPR Hub, CE – N° 441065

In another case, the Spanish supervisory authority AEPD concluded that the use of thermal cameras to check patients' temperature, in the context of the COVID-19 pandemic, does not fall under the processing of personal data when there is no further recording, storage, processing, or any other action taken on the data displayed by the camera, provided that individuals are not simultaneously required to identify themselves.²



² GDPR Hub, AEPD (Spain) – E/03884/2020

6.4.1. Automated decision-making and profiling

Relevant provisions: *GDPR* – Articles 4 and 22, Recitals 30, 60, 70-72; *PDPL* – Articles 4, 38-39.

A special type of personal data processing is automated making of individual decisions and profiling.

Guidelines

These issues have been extensively addressed in the Guidelines on Automated Decision-Making and Profiling by the Article 29 Working Party, subsequently endorsed by the European Data Protection Board.¹ The Information Commissioner's Office in the UK has also published specific guidelines on automated processing of personal data and profiling.²

¹ Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 (wp251rev.01)



² ICO, Rights related to automated decision making including profiling



The EU Agency for Fundamental Rights has published a guide on preventing unlawful profiling today and in the future.³ These guidelines provide a broader view of profiling, describe the legal frameworks governing profiling, and explain why lawful profiling is not only necessary to respect fundamental rights but also essential for the effective operation of the police and border management. The guide also provides practical guidance on how to avoid unlawful profiling in police operations and border management operations. The principles and practices outlined in the guide are supported by examples, case studies, and case law from the EU and beyond.

³ FRA, Preventing unlawful profiling today and in the future: a guide



Automated decision-making refers to any decision-making process that is entirely carried out without human involvement. It can involve various types of decisions, such as determining the amount of tax or tax refund based on data provided by an individual, automated approval of loans, issuing fines for improper parking within a traffic enforcement camera system, evaluating a student within an information system that autonomously reviews and grades student work, and so on. The controller cannot avoid the specific rules that apply to this type of processing by intentionally and fictitiously involving human intervention in the processing. For example, if an employee of the controller routinely applies automatically generated profiles to individuals without any real impact on the processing outcome, it would still be a decision based solely on automated processing. Human involvement in the processing of personal data entails meaningful oversight of the decision, rather than just a symbolic gesture, carried out by someone who possesses the necessary knowledge, authority, and competence to change the decision, taking into account the available data and the logic of the processing.

Profiling is a narrower concept and refers to any form of automated data processing used to evaluate certain personal characteristics. The legal framework for personal data protection explicitly provides examples of such processing, including predicting the work performance of an individual, their economic situation, health status, personal preferences, interests, reliability, behaviour, location, movement, etc. Profiling involves the processing of personal data that enables the assessment of personal aspects and the prediction of future behaviour. Although profiling in practice involves processing large amounts of personal data using advanced processing technologies such as machine learning, the qualification of profiling is not determined by the volume and sensitivity of personal data or the sophistication of the technology used, but rather by the effect - the evaluation of personal characteristics of an individual. Hence, merely restructuring data or making certain classifications based on age, gender, or height does not constitute profiling.

Examples

Recitals 70 and 71 of the GDPR Preamble provide practical examples of profiling:

- Creating user preferences based on previous purchases or clicks
- Maintaining customer profiles for more effective direct marketing
- Establishing systems for assessing financial stability and making automated decisions on credit applications
- Implementing automated recruitment systems without human intervention

Dilemmas

Automated making of individual decisions can occur with or without profiling, while profiling can take place without automated decision-making. However, profiling and automated decision-making are not necessarily separate processes.

Although it is not explicitly stated in the regulatory framework, profiling does not solely refer to automated data processing; it can be based on the analysis of statistical data or processed in other ways. The Guidelines on Automated Decision-Making and Profiling issued by the Article 29 Working Party provide examples, such as a bank profiling an individual's creditworthiness to assess their eligibility for a mortgage, with the final decision made by the bank's risk analysis department after further analysis.¹ Another example involves an insurance company determining insurance premiums based on individuals' driving behaviour.

¹ Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 (wp251rev.01)



Criteria such as distance travelled, time spent driving, and other information related to road conditions may be collected automatically through sensors in a smart car, combined with other data to better understand driver behaviour. The collected data is used to create profiles to identify driving patterns, such as sudden acceleration, hard braking, or speeding.

Regarding profiling for marketing purposes, the Austrian supervisory authority has taken the position that the GDPR distinguishes between profiling under Article 4(4) of the GDPR and automated individual decision-making under Article 22 of the GDPR. Consequently, the supervisory authority determined that it is not necessary for this processing activity to be performed exclusively in an automated manner for it to qualify as profiling.²



² GDPR Hub, DSB (Austria) – 2020-0.436.002

Although the legal framework for personal data protection does not establish an explicit prohibition on automated decision-making and profiling, it provides specific rights to individuals in this regard, which can be interpreted as a general prohibition on these types of processing. Data subjects have the right to request to be exempted from decisions based solely on automated processing, including profiling, if such decisions produce legal effects concerning them or significantly affect their position (more about these rights in Chapter XI). However, these rights are not applicable when the automated processing is:

1. Necessary for the conclusion or performance of a contract between the data subject and the data controller;
2. Based on a legal requirement that provides for appropriate safeguards for the rights, freedoms, and legitimate interests of the data subject; or
3. Based on the explicit consent of the data subject.

Example

The legal framework allows for automated processing of personal data in cases of performing tasks of public interest for the protection of national security and public health, provided there is a prior specific justification established by law based on legitimate expectations. Also, in the case of job recruitment where a large number of candidates have applied, the employer has the right to use specialized software to select a narrower pool of candidates based on predefined criteria if the candidates have given their consent to the automated processing, which they have been informed about through their application, indicating their intention to enter into an employment relationship with the employer.

Practice

The Finnish supervisory authority issued an opinion in 2022 at the request of a healthcare provider regarding the compliance of a planned patient data processing system for disease diagnosis and prevention. The system would process patients' medical records to identify those at risk and invite them for preventive check-ups. The supervisor assessed whether the processing of personal data would lead to automated individual decision-making but also noted the differences depending on whether patients would be invited for preventive check-ups. For individuals identified as at-risk through profiling, the profiling result would only be considered as one element in the decision-making process. The final decision would be made by a competent person, ensuring significant human involvement. However, for the other group, the competent person would not conduct further assessment. Therefore, the supervisor assessed whether profiling would have legal or other effects on the position of these patients: not being invited for preventive check-ups could have significant adverse consequences on their health. Consequently, in this case, the prohibition on automated individual decision-making and profiling would apply, and one of the three prior conditions would need to be met to justify the lawfulness of the processing.¹



¹ GDPR Hub, Tietosuojavaltuutetun toimisto (Finland) – 3895/83/22

As there is an increased risk of violating the rights and freedoms of individuals in profiling, additional appropriate measures of protection must be taken. It is common for individuals whose data is being processed to be unaware of the data collection and analysis for profiling purposes, leading to a breach of transparency principles stating that it is necessary for individuals to be informed about the purpose and methods of analysing their personal data. When relying on explicit consent as the legal basis for profiling, data controllers must demonstrate that individuals accurately understand what they are consenting to and must also bear in mind that consent is not always an appropriate basis for processing. In all cases, individuals should have sufficient relevant information about the intended use and consequences of the processing to ensure that any consent they provide represents an informed choice. Profiling that leads to discrimination against individuals based on special categories of personal data is expressly prohibited. In this regard, regular monitoring of algorithms and other profiling methods is recommended to ensure that there is no discrimination or incorrect decision-making.

Trusted resources

The breakneck development of artificial intelligence raises concerns among both general public and experts, particularly regarding the risks associated with the mass processing of personal data. The Spanish supervisory authority has prepared a useful guide detailing the application of the legal framework for personal data protection to the development and use of artificial intelligence systems.¹ Additionally, recognizing the significance and prevalence of machine learning technologies, the same supervisory authority has addressed some common misconceptions about smart machines in a separate document.² These documents are freely available in English.

¹ AEPD, *GDPR compliance of processings that embed Artificial Intelligence – An introduction*

² AEPD, *10 Misunderstandings about Machine Learning*



7. Key roles

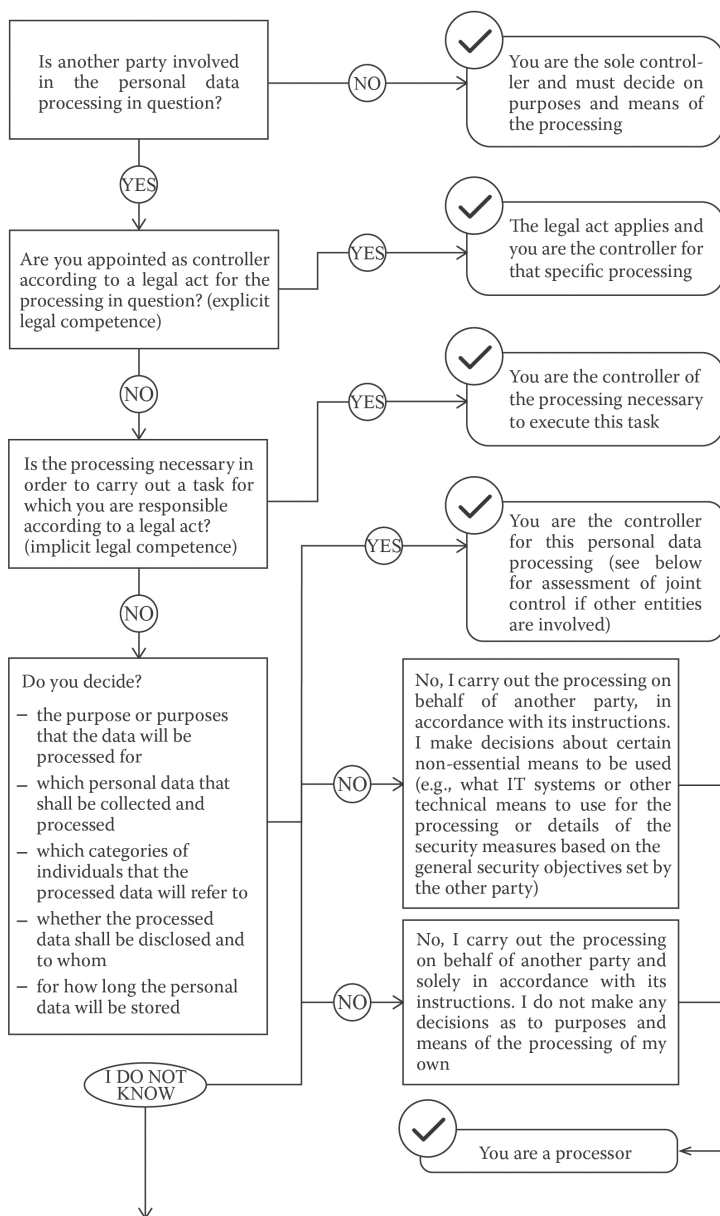
The legal framework for personal data protection aims to establish a system of accountability for the protection of personal data by defining rules and responsibilities for specific actors involved in the processing operation. It outlines the responsibilities of entities that interact with personal data, including controllers, joint controllers, processors, data recipients, and third parties.

The controller and processor are key roles in the processing of personal data. Their rights and obligations differ but also overlap to some extent. Specifically, the controller makes the decision to initiate the data processing and has its own interest in processing the data for a specific purpose. Hence, the controller determines the means and purposes of the data processing. On the other hand, the processor processes the data entrusted to them by the controller, acting on behalf of and in the interest of the controller. While the controller has a broader range of legal obligations compared to the processor, the processor is also required to fulfil a set of obligations prescribed by the Law.

The rapid development of the data processing market, its diversification and specialization, leads to the emergence of new services and relationships among the actors. Their mutual relationships can no longer be characterized as a simple relation between a controller and a processor, as expertise and interests related to the processing outcomes can often be found on multiple sides. Therefore, it is necessary to carefully examine each relationship in order to determine the key roles in data processing. It is important to assess who determines the purpose and means of data processing, and who carries out the processing on behalf of and in the interest of others, regardless of how the roles are distributed within a broader business relationship (client/service provider, buyer/seller, etc.). Hence, anyone processing personal data must determine whether they act as a controller, joint controller, or processor in relation to a specific processing, as their legal obligations and responsibilities towards the data subjects depend on their role.

Regardless of who presents themselves as a controller or processor publicly, in privacy policies and in documentation, the role is determined based on objective circumstances of the case and the specific role of each actor. The allocation of roles is thus derived from an analysis of factual elements or circumstances of the case and is not entirely subject to negotiation. Parties are not able to freely determine the roles in an individual data processing operation through a contract and thereby manage legal responsibilities. For example, an entity that has predominant control over the processing cannot transfer the role of a controller to another entity through a contract. Of course, if there is no doubt that the contractual allocation of roles accurately reflects the reality, there are no obstacles to the parties respecting the contract in this regard.

Furthermore, the interpretation of contracts between the parties involved in the processing, even when the contract does not explicitly mention who is the controller and who is the processor, may be relevant in determining the roles, as it can help consider who is in a position of control. Additionally, the regulation of relationships in other areas of law, such as intellectual property rights over databases, is not of particular significance when determining roles within the field of personal data protection.



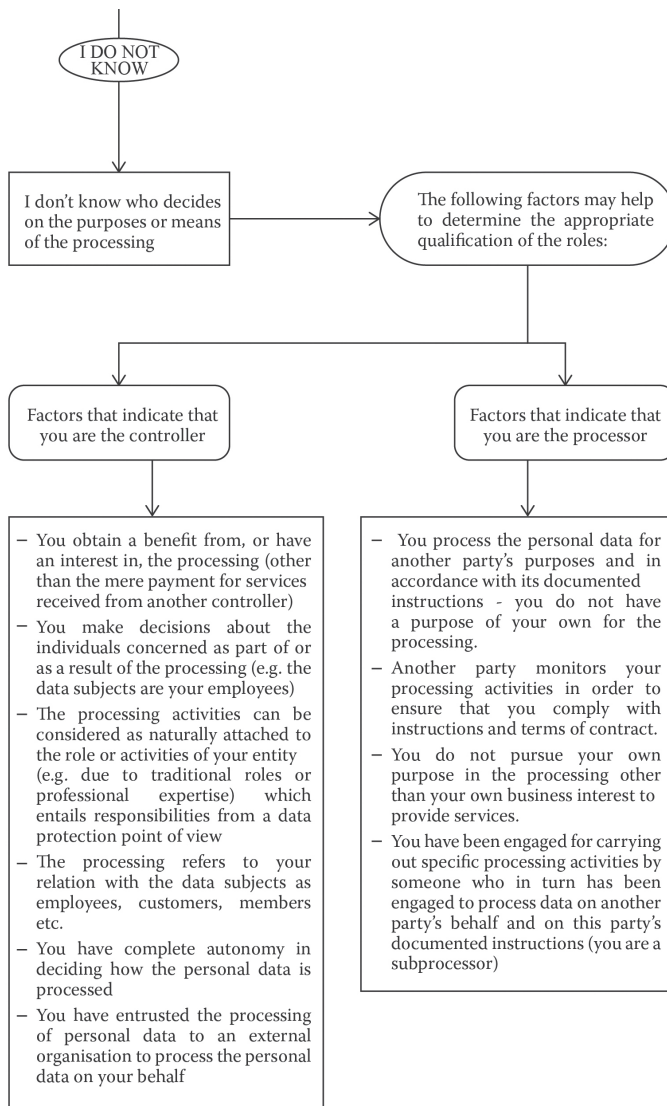


Figure 1: Flowchart for applying the concepts of controllers, processors, and joint controllers in practice

The same person can have the role of a controller with respect to one group of data and the role of a processor with respect to another. It is even possible for the same person to be a controller in one processing operation and a processor in another when the same data is processed for two different purposes, resulting in different roles for that person in those processing operations. However, in relation to a specific processing operation, an individual must have an exclusive role, either as a controller or as a processor.

7.1. Data controller

Relevant provisions: *GDPR* – Articles 4 and 24; *PDPL* – Articles 4 and 41.

When determining the role in data processing, the following questions need to be asked: 1) Who decides to initiate the data processing? 2) Whose interests are being pursued through the processing operation? 3) Who determines the purpose for which the data is processed? and 4) Who decides on the means and methods of the processing? The answer to all these questions is the controller – a natural or a legal person, or public authority that is the main decision-maker regarding the specific processing of personal data.

The controller is the entity that bears the highest level of responsibility for compliance with the legal framework for data protection, both for themselves and for other individuals involved in the processing operations. The controller also has a duty to demonstrate compliance and bears the risk of facing actions from the Data Protection Authority and citizens in case of any infringement of data protection rights guaranteed by the law.

Example

Data controller examples:

- An employer is a controller in relation to the personal data of their employees.
- An IT company that owns an application collecting user data is a controller in relation to the data of its users.
- A company organizing a conference and collecting participant data for registration and attendance purposes is a controller in relation to the participant data.
- A restaurant that takes delivery orders from customers and collects their personal data (phone number, delivery address, name) is a controller in relation to such data.
- A hotel is a controller in relation to the data it collects about its guests.

Guidelines

The allocation of roles is determined through a factual analysis of each individual case, and the controller is identified by answering the previously posed questions. The EDPB guidelines on the concepts of controller and processor under the GDPR provide that the controller can be easily and clearly determined by referring to specific legal and/or factual circumstances from which “influence” can usually be inferred unless other elements indicate otherwise.¹ The guidelines differentiate between two categories of these situations:

¹ EDPB, Guidelines 07/2020 on the concepts of controller and processor in the GDPR



1. Control resulting from legal provisions - a situation where certain organizations are legally vested with authority that encompasses a specific processing of personal data. For example, the law imposes an obligation on municipal authorities to provide social welfare benefits to citizens based on their financial situation. In order to make these payments, the municipal authorities must collect and process data on the applicants' financial status. Although the law does not explicitly state that the municipal authorities are the controllers of this processing, it implicitly follows from the legal provisions.
2. Control arising from factual influence - a situation where all relevant factual circumstances that must be taken into account indicate that a specific actor exercises decisive influence regarding the processing of personal data. For example, the provision of electronic communication services such as SMS messaging. The provider of such services is typically considered the controller with regard to the processing of personal data necessary for the functioning of the service itself (e.g., traffic and billing data). However, since the sole purpose and role of the service provider is to enable the transmission of electronic messages, the provider will not be considered the controller with respect to personal data contained within the message itself. The controller in relation to all personal data contained in the message will typically be considered the person from whom the message originates, rather than the service provider offering the transmission service.

Although a natural person can be a controller, attention should be paid to whether they are involved in the processing on their own behalf or as an employee/representative of an organization with legal personality, which is most often the case. In general, it can be assumed that any processing of personal data by employees within the scope of the organization's activities is under the control of that organization, and therefore the employees in such cases are not considered controllers. Furthermore, although in practice specific organizational units are operationally responsible for the processing of personal data within an organization, it does not mean that these units and departments can be considered controllers; it is always the legal entity to which they belong.

Example

The finance department of a technology start-up is launching a crowdfunding campaign for a new product that will be available on the market in the near future. This department decides on the nature of the campaign, the crowdfunding platform, the means to be used (email, social media), the target audience, and the data to be used to make the campaign successful. Even if the department operates with significant independence, the start-up will be considered the controller since it initiates the campaign, which takes place within its business activities and for its own purposes.

When a person determines the purpose and means of processing, i.e., answers the questions of why and how the processing should be carried out, that person is undoubtedly considered the controller. If the processing is then entrusted to another person whose activities are limited to following detailed instructions, that person will not be considered a controller. In practice, it may happen that the person to whom the processing is entrusted, the processor, decides on certain aspects of the processing because it is more practical in that specific case, considering their higher domain expertise related to that processing. In order to avoid being classified as a controller, the processor must limit their decisions to matters concerning the “ancillary means” of processing.

Guidelines

The EDPB guidelines on the concepts of controller and processor within the GDPR address situations where there may be some room for the processor to influence certain decisions related to processing.¹ However, the guidelines recognize the need to create clearer instructions regarding the level of influence on the “why” and “how” that qualifies an entity as a controller and the extent to which a processor can make decisions independently. The main dilemma revolves around where to draw the line between decisions reserved for the controller and decisions that can be left to the discretion of the processor. Decisions regarding the purpose of processing are always the responsibility of the controller. As for determining the means of processing, a distinction can be made between essential and ancillary means. Essential means are naturally reserved for the controller, while ancillary means can be determined by the processor. Essential means are closely linked to the purpose and scope of processing, such as the type of personal data processed (“what data will be processed?”), the duration of processing (“how long will it be processed?”), the categories of recipients (“who will have access to it?”), and the categories of data subjects (“whose personal data is being processed?”). Along with the purpose of processing, essential means are closely connected to the question of whether the processing is lawful, necessary, and proportionate. Ancillary means refer to more practical implementation aspects, such as the choice of specific hardware or software or detailed security measures, which can be entrusted to the processor to decide upon.



¹ EDPB, Guidelines 07/2020 on the concepts of controller and processor in the GDPR

The guidelines provide for situations where the existing influence of the processor does not concern essential means of processing and, therefore, cannot qualify them as controllers:

1. Company X, as a provider of cloud computing services, offers clients the possibility to store large amounts of personal data. This service is completely standardized, and clients have little or very limited options to customize the service according to their needs. The contract terms for the service provided by Company X are standardized on an access basis, according to a “take it or leave it” principle. Company Y wants to engage Company X for storing personal data.

Company Y will be considered the controller of that data because it made the decision to engage a specific cloud computing service provider and entrusted them with the data processing. Since Company X does not process personal data for its own purposes and stores it on behalf of its clients (in this case, Company Y), it will be considered the processor, even though it decides on certain primarily technical aspects of the processing. However, in order for Company X to retain its role as a processor, it must not make decisions regarding key data-related issues and, considering this is a data storage service, it must delete the data in all cases according to the controller's instructions.

2. Company A, as an employer, engages Company B to process salary payments to its employees. Company A provides clear instructions to Company B regarding who should be paid, the amounts, deadlines, which bank to use, how long the data should be retained, what data needs to be reported to the tax authority, etc. In this case, data processing is carried out for the purpose of Company A paying salaries to its employees, and Company B must not use the data for any of its own purposes. The manner in which Company B processes the data is clearly and firmly defined. However, Company B may make decisions about certain aspects of the processing, such as the choice of software or which employees within Company B will have access to this personal data, etc. This does not change Company B's role as a processor as long as Company B adheres to Company A's instructions regarding the processing.

The question of whether the controller has direct control over the data and manages the infrastructure, information systems, and applications used for data processing is fundamentally irrelevant in determining their status. Even if a person does not have access to the personal data itself, they will be considered a controller when they determine the means and purposes of processing and derive an interest from the results.

Guidelines

The EDPB guidelines on the concepts of controller and processor in the GDPR provide examples of when a data analytics service purchaser is considered a controller and when they are not:¹



¹ EDPB, *Guidelines 07/2020 on the concepts of controller and processor in the GDPR*

1. Company ABC wants to know which types of consumers are most likely to be interested in their products and contracts with a service provider, XYZ, to obtain relevant information. Company ABC provides instructions to XYZ regarding the type of information they are interested in and provides a list of questions to ask those participating in the market research. Company ABC only receives statistical information (e.g., identification of consumer trends by region) from XYZ and does not have access to the personal data itself.

However, Company ABC has decided to initiate the processing operation, determined the purpose, and provided XYZ with detailed instructions on the information to collect. Therefore, Company ABC should still be considered the controller regarding the processing of personal data carried out for the purpose of delivering the requested information. XYZ can only process data for the purpose specified by Company ABC and in accordance with their detailed instructions, thus being considered a processor.

2. Company ABC wants to know which types of consumers are most likely to be interested in their products. Service provider XYZ is a market research agency that has gathered information on consumer interests through various questionnaires covering a wide range of products and services. XYZ has independently collected and analysed this data according to its own methodology, without any instructions from Company ABC. To respond to Company ABC's request, service provider XYZ will generate statistical information, but they do so without any further instructions on which personal data to process or how to process it to generate this statistics. In this example, service provider XYZ acts as the sole controller, processing personal data for market research purposes and independently determining the means of processing. Company ABC has no specific role or responsibility under the personal data protection framework regarding these processing activities since Company ABC receives anonymised statistics and is not involved in determining the purpose and means of processing.

The Serbian Commissioner

Does a company that provides its clients with parcel pickup and delivery services have the status of a controller or processor? Commissioner dealt with this issue examining the Postal Services Act and determined that the postal operator is obligated to process personal data of its service users. This occurs, for example, when issuing a receipt to the sender for the reception of a parcel and maintaining a special record of parcels, or when verifying a personal identification document with a photograph and recording the registration number of the representative's identification document for parcel submission. Since the postal operator, in accordance with the Postal Services Act, provides the appropriate postal service to a specific user and is obliged, among other things, to process personal data to fulfil the purpose of processing, the Commissioner has concluded that the postal operator, in relation to the personal data of its service users processed within the scope of postal activities, qualifies as a controller.¹

¹ *Protection of personal data: Positions, opinions and practice of the Commissioner, publication no. 7, Belgrade, 2022. Case number: 073-14-1639/2021-02, pp. 161-163 [in Serbian]*



Practice

In a case before the Court of Justice of the European Union, the question arose as to whether an entity that lacks control and access over the processing of personal data can be considered a controller.¹ Specifically, the German company *Fashion ID* had integrated a Facebook “Like” button on its website, which resulted in the personal data of website visitors being transmitted to Facebook. *Fashion ID* had no control over such data nor any influence on how Facebook further processed that personal data. However, the court ruled that *Fashion ID* should still be considered a joint controller with Facebook regarding the collection and sharing of data with Facebook, even though it later had no control or access to the data. The reason for this decision was that *Fashion ID* had made a conscious decision to integrate the “Like” button on its website and share visitor data with Facebook. In other words, Facebook would not have gained access to the personal data of website visitors if *Fashion ID* had not integrated this button. Additionally, *Fashion ID* benefited economically from this integration, as the products sold through the website gained visibility on the social network. Therefore, *Fashion ID* had a direct interest in the processing of user data through the sharing of this data with Facebook.



¹ GDPR Hub, Judgment in Fashion ID, C 40/17, ECLI:EU:C:2019:629

7.2. Joint controllers

Relevant provisions: *GDPR* – Article 26; *PDPL* – Article 43.

It is not uncommon for two or more persons to be involved in a personal data processing operation and jointly make decisions regarding the purposes and means of the processing. In such cases, they will be considered joint controllers and will have an obligation to transparently determine the responsibilities of each of them for complying with the rights and obligations prescribed by law, particularly in terms of respecting the rights of the data subjects.

Whether two or more persons are considered joint controllers, separate controllers, or in a relationship of controller and processor should be assessed in each specific case, taking into account all relevant facts. The nature of their relationship and how that relationship is structured is not relevant to this determination. What matters primarily is whether each joint controller individually meets the conditions to be considered a controller in relation to the same processing operation and whether they have jointly determined the purposes and influenced the means of processing in relation to it.

Guidelines

Informative examples of joint controllers can be found in the guidelines of both Working Group 29¹ and the EDPB.²

1. Company X, which uses the services of employment agency Y, where the agency formally employs workers who actually perform their duties at Company X. In this case, X and Y will be in a joint controller position, along with the agency, as both determine the purposes and means of the processing. Company X, as the factual employer, enables workers to perform their tasks, while agency Y, as the formal employer, is responsible for employment contracts and fulfilling its obligations under relevant laws.
2. Joint controllers can be a tourist agency X and hotel chain Y, who decide to establish a joint website for online accommodation bookings. They agree on which data to collect and how, for what purposes, how long to retain it, who can access it, and similar matters. Each of the joint controllers must fulfil all obligations prescribed by the legal framework, and each is fully responsible to the individuals whose data is being processed.
3. Companies A and B have launched a co-branded product and want to organize an event to promote it. For this purpose, they decide to share data of their current and potential customers to create a guest list for the event. They also agree on the methods of sending invitations, collecting feedback during the event, and subsequent marketing actions. Companies A and B can be considered joint controllers for the processing of personal data related to the organization of the promotional event, as they jointly decide on the defined purpose and essential means of data processing in this context.

¹ Article 29 Data Protection Working Party, Opinion 1/2010 on the concepts of "controller" and "processor"

² EDPB, Guidelines 07/2020 on the concepts of controller and processor in the GDPR



However, when two controllers exchange data without prior joint determination of the purpose and means of processing does not make them joint controllers but separate controllers. For example, a company that processes employee data for the purpose of payroll and tax contributions has a legal obligation to share certain personal data with tax authorities for conducting specific tax controls. In this case, although both the company and the tax authority process the same employee data, they are separate controllers because each has a distinct purpose of processing and independently determines the means of processing the data.

Example

Employer X transfers information to Bank Y through a payroll system to facilitate salary payments to X's employees. This activity involves the processing of personal data performed by the bank as part of its operations. Within this activity, the bank independently decides which data to process for the provision of its service, how long the data should be retained, and so on, without influence from Employer X due to financial regulations governing these matters. Therefore, Bank Y should be considered a separate controller for this processing, and the data transfer through the payroll system should be seen as information sharing between two controllers, from Employer X to Bank Y.

Processing the same or a similar set of data on the same infrastructure by two entities does not automatically make them joint controllers. If the processing can be separated in a way that each entity can independently carry out the processing and achieve its own purpose, then they are not joint controllers. For example, if a group of companies uses the same customer database stored on the servers of the parent company, the parent company acts as a processor in terms of data storage. However, if each member of the group enters data for their own customers and processes such data solely for their own purposes, deciding on access, retention periods, correction, or deletion of the data, and there is no possibility for members to access or use each other's data, then each company will be a separate controller. The fact that these companies use a shared infrastructure does not imply that they have the role of joint controllers.

Practice

In the CJEU case concerning Jehovah's Witnesses, the court considered that the religious group should be regarded as a joint controller with its members who collect personal data in the field, even though it did not have access to the personal data collected by its members. This is because the religious group participated in determining the purpose and means of data processing by organizing and coordinating the activities of its members in order to spread its beliefs.¹

An interesting CJEU decision prior to the GDPR's entry into force relates to a lawsuit filed by a Spanish citizen against a newspaper and *Google*. The lawsuit arose because, upon entering the individual's name in the search engine, *Google* immediately displayed a link to two pages of the defendant newspaper mentioning the person's name in connection with a debt.²

¹ Judgment in Jehovah's witnesses, C-25/17, ECLI:EU:C:2018:551, paragraph 75

² GDPR Hub, CJEU - C-131/12 - Google Spain



When Spanish authorities sought clarification, the case came before the CJEU, which considered that the internet search engine (in this case, *Google*) should be considered a controller regarding the processing of personal data appearing on web pages published by third parties (in this case, an online news article published by the newspaper). The search engine was deemed a controller regarding search, indexing, temporary storage, and making personal data available to network users. In this case, the search engine is required to remove the data concerning an individual that is published by a third party (the online edition of the newspaper) from the list of search results displayed when a specific person's name is entered in the internet search engine..

7.3. Data processor

Relevant provisions: *GDPR* – Article 28, Recital 81; *PDPL* – Article 45.

Processor is a natural or legal person, or a government authority, who processes personal data on behalf of the controller. This means that the processor:

- 1) Represents a separate, external entity from the controller (it does not belong to the controller's organization, and an employee of the controller cannot be considered a processor),
- 2) Does not independently determine the purpose and means of processing personal data, but carries out the processing as a delegated task, on behalf of and in the interest of the controller.

Typically, the role of a processor is assumed by an organization with specialized skills and knowledge that the controller engages to perform a specific task, which includes the processing of personal data. The relationship between the processor and the controller is such that the processor is generally required to act in accordance with written instructions from the controller, which means that the controller has control and manages the processing activities. If an entity has no vested interest in the processing of the data and acts solely based on the instructions of the client from whom it expects compensation for the job, they will likely be considered a processor – even if they make some technical decisions on how the data should be processed.

Examples

If company X, seeking a new employee, does not want to spend its resources on the candidate selection process, it can hire a staffing agency, company Y, for that purpose. In this case, agency Y will process personal data of many candidates whom company X will never know about because they did not pass the selection process. However, agency Y will do so on behalf of and for the purpose determined by company X. As long as agency Y acts in accordance with the written instructions of company X, which ultimately controls the purpose and manner of data processing (by providing instructions on which data to process and how), agency Y will be considered a processor, and company X will be the controller of the personal data of job applicants

However, if company X only gives a general instruction to agency Y to provide potential candidates, while the agency itself determines which data to process at each stage of the selection process, how to process it, and by what means - then agency Y itself has the status of a controller in relation to the processing it performs, or possibly the status of a joint controller with company X.

Company X engages company Y to maintain its technical infrastructure, consisting of workstations, networks, and data storage and exchange infrastructure. In this case, company Y, as a provider of technical support services, plays the role of a processor because it maintains the technical infrastructure in accordance with the instructions of the controller - company X, which has entrusted these authorizations to the service provider..

Although operating within the framework defined by the controller and following their instructions, a processor may autonomously decide on certain aspects of the delegated processing that relate to ancillary processing means, as long as it is done in order to fulfil the purpose established by the controller. The processor may make decisions on numerous matters while still maintaining their role, such as:

- Which methods to use for collecting personal data,
- Which IT systems to utilize for data processing,
- How to store personal data,
- Details regarding the security of personal data,
- Means used for the transmission of personal data,
- Means used for the erasure or disposal of data.

This list is not exhaustive but illustrates the differences between the roles of controllers and processors. In certain circumstances, and where permitted by contract, a processor may have the freedom to utilize their technical expertise to decide how to carry out specific activities on behalf of the controller.

Example

A bank hires an IT company to develop a mobile application for customer communication. The bank controls how and why the data is used and determines the data retention period. However, in reality, it is the IT company that will decide on the optimal way to store the data based on their technical expertise. Although the IT company has the ability to make technical decisions, they are still a processor, not a controller, in relation to the bank's data precisely because the bank retains exclusive control over determining the purpose of the data processing, even though it does not have exclusive control over determining the means of processing.

However, when a processor goes beyond the instructions given by the controller and starts determining their own purposes or essential processing means, their status expands, and they may be considered a controller. For example, a company processing data on behalf of another entity for direct marketing services may acquire the status of a controller if they decide to use the provided customer database for the purpose of improving their own products.⁴⁵ In this case there are no joint controllers; instead, these companies will be separate controllers due to the differing purposes, while maintaining a controller-processor relationship regarding the initial purpose.

7.4. Data recipient

Relevant provisions: *GDPR* – Article 4, Recital 31; *PDPL* – Article 4.

According to the legal definition, a recipient is any individual to whom personal data is disclosed, whether it is a third party or not, excluding authorities receiving personal data within the framework of a specific investigation based on legal authority and processing this data in accordance with personal data protection rules related to the purpose of processing. Therefore, in principle, any individual who comes into possession of personal data that is subject to processing has the status of a recipient, including processors. However, entities such as tax or customs authorities, for example, which process personal data within the scope of their authorities, are not considered recipients.

In accordance with the rules regarding transparency of processing, specifically the preparation of privacy notices, the controller is obligated to make information about the recipients of the data available to the data subjects. Additionally, under the rules regarding the right of access, these individuals have the right to request information from the controller at any time about the recipients or categories of recipients to whom their personal data has been or will be disclosed, in order to be aware of the movement of their data.

Example

The conference organizer arranges travel, accommodation, and other services for conference participants. In this process, the organizer provides personal data of the participants to airlines, bus companies, taxi services, and hotels involved in the organization of the conference. These entities should be regarded as recipients of the data. In this specific case, they act as controllers regarding the processing they carry out for their own purposes (e.g., an airline needs to process personal data of passengers in compliance with aviation regulations and its internal procedures).

⁴⁵ The legality of the processing in this example is a separate issue.

Practice

According to a decision of the Stockholm Administrative Court, a controller is obliged to inform data subject about the specific recipients of the data in the best possible manner if the individual explicitly requests it.¹ In this case, the data subject submitted a request to the bank for access to their data. However, the bank did not provide all the requested information, including the data about the recipients to whom the personal data of the individual - the requester - was disclosed. In the outcome the Stockholm Administrative Court ruled that the controller must respond to such a request from an individual to the best of its abilities. The court determined that the bank, as a controller, has the means to provide the requested information, and providing such information would not disproportionately burden its resources.



¹ GDPR Hub, Förvaltningsrätten – Mål nr 11453-22

The legal framework for personal data protection does not impose specific obligations on recipients and third parties; it only describes their relationship to the controller or processor and the processing operation. A recipient of personal data or a third party can simultaneously be considered a controller or processor from different perspectives. For example, actors who are regarded as recipients or third parties from the perspective of one processing operation may be controllers for another processing operation in which they determine the purpose and means of processing the previously obtained data.

7.5. Third party

Relevant provisions: *GDPR* – Article 4; *PDPL* – Article 4.

A third party is defined by negative enumeration as a natural or legal person, or public authority, who is not the data subject, controller, nor processor in the context of a specific processing operation. Additionally, a third party is not an entity authorized to process personal data under the direct supervision of the controller or processor, such as employees.

Dilemmas

Who is authorized to process personal data under the direct supervision of the controller or processor?

Both the Law and the GDPR are ambiguous regarding this concept, which can only be found in the definition of a third party. The EDPB guidelines on the concepts of controller and processor under the GDPR note that these entities include not only employees but also individuals who are otherwise engaged in a very similar employment relationship.¹ In accordance with domestic labour regulations, this would include relationships based on temporary and occasional work contracts, volunteering agreements, professional training agreements, contracts for temporary employee placement, and contracts for rights and obligations of directors. However, domestic practice also involves cases where individuals are engaged to perform specific tasks that involve the processing of personal data based on service contracts, as well as the engagement of persons in the status of entrepreneurs for similar types of work, raising the dilemma of whether they could be covered by this concept (more on this in the “Employees” section).

¹ EDPB, Guidelines 07/2020 on the concepts of controller and processor in the GDPR



Guidelines

An interesting example of a third party can be found in the EDPB guidelines on the concepts of controller and processor.¹ Company A, in relation to maintaining hygiene in its premises, enters into a contract with a cleaning services company. The cleaners do not have authorization to access or otherwise process personal data. Although they may occasionally come across such data while moving around the office, they can perform their task without any access to the personal data processed by Company A as the controller. The cleaners are not employees of Company A, nor are they considered to be under its direct supervision. There is no intention for the cleaning services company or its employees to process personal data on behalf of Company A. Therefore, the cleaning services company and its employees must be regarded as third parties, and the controller must establish adequate security measures to prevent access and define confidentiality obligations in case they inadvertently come across personal data.

¹ EDPB, Guidelines 07/2020 on the concepts of controller and processor in the GDPR



8. Principles of data processing

8.1. Importance of principles

The principles are abstracted key rules of personal data processing that have normative significance. Considering that they are explicitly incorporated in the text of the Law on Personal Data Protection and the General Data Protection Regulation, the principles are legally binding key guidelines primarily intended for data controllers. Therefore, regardless of formally complying with other obligations under the law, it is possible to establish liability if the manner in which those obligations are implemented is not in line with any of the principles. Violating the principles of personal data processing also entails the most severe penalties – according to Serbian law, the penalty for an individual offense that violates any of the principles amounts to 2,000,000 RSD, while in cumulative cases, the penalty can be twice as high. According to the GDPR, the highest possible penalty can be imposed for violating the principles, amounting to 20 million euros or 4% of the total annual revenue, whichever is higher.

The principles of personal data processing within the Law and GDPR have a long history and are based on the principles outlined in Article 5 of the 1981 Convention 108,⁴⁶ and to a large extent, they are consistent with Article 6(1) of the previous Data Protection Directive 95/46/EC.⁴⁷

The principles serve as a general barrier against unauthorized and excessive processing of personal data, regardless of the context. Although they consist mostly of generalized rules that cannot be characterized as specific and precise behavioural instructions, the principles form the fundamental pillars for compliance with the Law, general guidelines to be followed when aligning with the legal framework for personal data protection. In order for the personal data processing to be compliant, it is necessary to respect the logic established by the principles during its development in a responsible manner. Specifically, the principles dictate that it is necessary to first determine the purpose of processing, define the set of personal data and processing operations that enable the achievement of the purpose, and select an appropriate legal basis in order to make decisions that will determine the data retention period, design and implement the processing operation in a way that ensures accuracy, integrity, and confidentiality of the data, and then establish fair and transparent relationships with the data subjects.

The principles also practically guide the interpretation of specific provisions that may be unclear. Therefore, if a data controller or processor is uncertain about how to

46 Convention 108 and Protocols <https://www.coe.int/en/web/data-protection/convention108-and-protocol>

47 Directive 95/46/EC <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A31995L0046>

apply a particular provision, they should always rely on the interpretation that is in line with these principles. Additionally, when creating a Code of Conduct and other self-regulatory and internal policies, special attention should be paid to the principles.

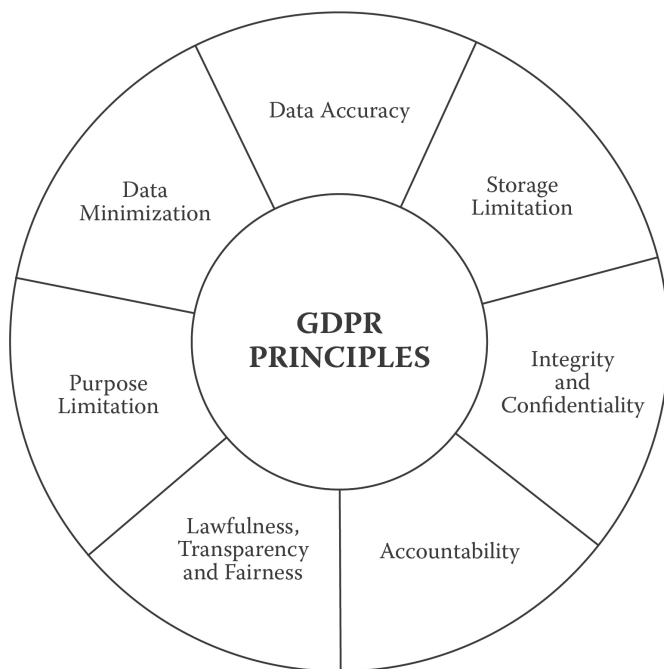


Figure 2: Principles of personal data processing

8.2. Lawfulness, fairness, and transparency

Relevant provisions: *GDPR* – Article 5, Recitals 39-40, 58, 60-62; *PDPL* – Article 5.

Personal data must be processed lawfully, fairly, and transparently in relation to the data subject (“lawfulness, fairness, and transparency”). Lawful processing refers to processing carried out in accordance with this law or other laws governing processing.

From the wording of this principle, it is clear that it consists of several interconnected but separate parts. Namely, this principle contains rules that personal data must be processed lawfully, fairly, and transparently in relation to the data subject. Essentially, this principle requires data controllers not to abuse their disproportionately stronger position compared to the individuals whose data is being processed, in relation to whom there is an asymmetry of information, but to have a fair and honest attitude. This attitude implies that data controllers behave in a manner that their clients, users, or partners, whose data they process, would consider acceptable and expected.

Lawfulness of processing means that data can only be processed if there is an appropriate legal basis for the specific processing. In other words, we can say that the processing of personal data is generally unlawful, and the unlawfulness is remedied by selecting an adequate legal basis and ensuring compliance with its requirements. Regardless of the appearance that something is allowed “because it is common practice in the sector and everyone is already doing it”, in the absence of an appropriate legal basis, such processing is automatically unlawful. Therefore, before commencing processing, the data controller must choose one of the six legal bases provided by Article 12 of the Law on Personal Data Protection and continue with the alignment in accordance with that decision. Additionally, if the processing involves special categories of personal data, lawfulness may require additional conditions prescribed by Article 17 of the Law. Finally, in addition to an adequate legal basis, the processing of data must comply with all regulations outside the field of personal data protection that may be applicable to such processing. Thus, data processing will be unlawful when it violates copyright (processing photos of individuals that represent copyrighted works), breaches confidentiality obligations (processing data that has been entrusted to the controller based on a confidentiality agreement solely for the purpose of accessing the data), or in other cases where data processing violates contractual obligations and sectoral laws, or human rights provisions.

Practice

A common example of a breach of lawfulness of processing is the public disclosure of personal data without an appropriate legal basis. This violation can occur both unintentionally and with the awareness that the publication of a certain document containing personal data constitutes processing that requires a legal basis. For instance, the Spanish supervisory authority, AEPD, identified a breach of the lawfulness principle when an individual posted a restaurant bill on Twitter that contained the owner's personal data,¹ and when a party in a legal proceeding shared a decision of a local court on Facebook that included personal data of the other party.² These types of violations are common in the era of the internet and social media, where data about present and former employees, service users, or participants in competitions are published, often considered justified under the circumstances. Regardless of whether such disclosure would actually be legitimate, the person publishing documents containing personal data must first be aware that such publication constitutes data processing and is obliged to determine the appropriate legal basis beforehand. Failure to do so will likely result in liability for unlawful processing of personal data

¹ GDPR Hub, AEPD – PS/00050/2020

² GDPR Hub, AEPD – PS/00070/2020



However, it should be noted that the Serbian legislator, following the European regulatory framework, has provided a journalistic exemption from strict data protection rules, including the principle of lawfulness, allowing for the free publication of personal data when it is done in the public interest within the scope of journalistic work.³

Misuse of personal data and false representation also constitute a breach of the lawfulness principle. AEPD fined an individual 1,200 EUR under these circumstances, as they had used someone else's photograph on the social network Tinder and the affected person reported the case to the supervisory authority.⁴ In another case, the same supervisory authority found the data controller liable for entering into a contract with a person who falsely represented themselves, without taking the necessary measures to verify their actual identity.⁵ The controller was fined 36,000 EUR for this breach of the lawfulness principle.

³ More on journalistic exception in chapter 13.1: Freedom of expression and information

⁴ GDPR Hub, AEPD – PS/00278/2020

⁵ GDPR Hub, AEPD – PS/00308/2020



Fairness of processing establishes the duty of data controllers to at all times consider the interests and reasonable expectations of the data subjects and to act fairly in the specific circumstances, taking into account the specific characteristics of the categories of individuals whose data they process. This principle is of an inherently general nature and establishes the expectation that relationships in the field of personal data processing are established on fair grounds, allowing for significant flexibility in situations where this is not the case. In accordance with the principles of our contract law, data controllers are obliged to adhere to the principles of conscientiousness and fairness, as well as to adhere to good business practices. Additional guidance can be found within consumer law, through the interpretation of the concept of unfair business practices, particularly considering that consumer rights can often be applied to relationships in the field of personal data processing. It is particularly important that in cases of processing personal data based on consent, the principle of equal value exchange is taken into account, so that individuals are not unfairly drawn into relationships that require disproportionately large concessions from them and provide minimal benefits.

Smernice

The EDPB Guidelines 4/2019 on data protection by design and by default provide an open list of certain elements of fairness of processing that should always be respected.¹ The list is particularly detailed, and the examples range from granting data subjects a high level of autonomy in controlling the processing to requirements for fair algorithms and the right to human intervention. Other important officially recognized elements of fairness include the expectation of individuals regarding the reasonable use of their data and the right not to be discriminated against or exploited due to certain psychological vulnerabilities. The power imbalance between the data controller and data subjects, which often exists in certain intrusive profiling and processing practices, is also covered by this principle. The EDPB clarifies that, in order for processing to be fair, deception and misleading of data subjects are not permitted, and all options should be presented in an objective and neutral manner, avoiding any deceptive or manipulative language or design.



¹ EDPB, Guidelines 4/2019 on Article 25 Data Protection by Design and by Default

Practice

When considering the mechanism for obtaining consent for cookies on a media website, the Danish supervisory authority, *Datatilsynet*, identified a breach of the fairness principle.¹ Users were presented with three options on the website, marked with colours: 1) only necessary cookies (in a red box); 2) cookie settings (in a grey box); and 3) accept all cookies (in a green box). The supervisor found that marking the options with a “traffic light system” constituted a type of manipulative nudging that affected users' ability to make an informed decision. The supervisor concluded that data controllers have freedom regarding the appearance and content of the information provided to users, as long as the design solutions do not hide information or involve unfair processing.



¹ GDPR Hub, Datatilsynet – 2021-41-0149

Guidelines

The EDPB Guidelines 3/2022 on dark patterns state that they are interfaces and user experiences implemented on social media platforms that lead users to make unintended, involuntary, and potentially harmful decisions regarding the processing of their personal data.¹



¹ Guidelines 3/2022 on Dark patterns in social media platform interfaces: How to recognise and avoid them

Dark patterns aim to influence user behaviour and can hinder their ability to effectively protect their personal data and make informed choices. According to the Guidelines, supervisory authorities are responsible for sanctioning the use of dark patterns if they violate the requirements of the GDPR.

Fairness of processing serves as a starting point for assessing whether a design pattern actually constitutes a "dark pattern". The principles relevant to this assessment are transparency, data minimization, accountability and, in some cases, purpose limitation. Legal assessment is sometimes also based on compliance with the requirements for valid consent. Compliance with individuals' rights also carries significant importance in the assessment. Finally, the requirements of embedded and default privacy play a vital role, as their implementation prior to making decisions on interface design would assist online service providers such as social media platforms in avoiding dark patterns.

Transparency of processing requires that from the moment data collection begins, the data subject has the right to know how their data is being treated. This includes the right to be informed that their data is being processed, to what extent, for what purposes, who the data controller and processors are, as well as the risks associated with the processing, the rules and protective mechanisms governing the data processing, how their rights are exercised, and more. It is essential that this information is available, accessible, and communicated in an easily understandable manner. The transparency of processing is regulated within Chapter 3 of the Law on Personal Data Protection, which sets out detailed obligations for data controllers regarding transparency of processing and the ways in which related individual rights are exercised.⁴⁸ The Law differentiates between the information provided to individuals whose data is collected directly from them and those collected from other sources.

Guidelines

According to the opinion of the European Data Protection Board (EDPB), transparency is a principle that is relevant in all aspects of personal data protection rules and is effective in three central areas: (1) informing individuals about fair processing; (2) how data controllers communicate with data subjects regarding their rights; and (3) ways in which data controllers can assist individuals in effectively exercising their rights. Additionally, the principle of transparency is equally important throughout all stages of data processing: before the start of processing, during the processing itself - which includes communication based on the right to be informed and other rights, and in the event of unforeseen circumstances during processing that may compromise the security and confidentiality of the data.¹

¹ Article 29 Working Party, Guidelines on Transparency under Regulation 2016/679 (wp260rev.01).



As an example, we can imagine a situation where a data controller publishes a privacy policy on their website, disclosing to their clients, whose data they collect through their online service, all the data collected about them, the legal basis for processing, the retention period, and even sharing the data with some of their business partners (often stating that the partners are “reliable”). However, this principle of protection would be fundamentally violated if the privacy policy text fails to mention the fact that the data controller has no control over how exactly the partners use the data, what data they acquire, how long they retain it, and whether they further share it with an unspecified group of entities - thus revealing that the processing occurring on the data controller's online platform is insignificant compared to the processing conducted by various partners, of which the data subjects are unaware.

Practice

Data controllers managing complex data processing systems that utilize machine learning or other artificial intelligence technologies to make decisions through automated processing of personal data face specific challenges in terms of transparency. Food delivery applications are examples of such systems that automatically determine which driver will take on an order and perform its delivery. In 2021, the Italian supervisory authority conducted inspections of delivery services provided by two companies, *Foodinho*¹ i *Deliveroo*² and identified a series of violations, including breaches of the transparency principle, resulting in fines of 2.6 million EUR and 2.5 million EUR, respectively. In both cases, the supervisor found that there were failures to inform the drivers about the data processing methods related to their location, the decision-making logic employed by the algorithm in selecting drivers, and the consequences of such decisions.

¹ GDPR Hub, Garante per la protezione dei dati personali (Italy) – 9675440

² GDPR Hub, Garante per la protezione dei dati personali (Italy) – 9685994



Dilemmas

In practice, the question often arises as to whether the consent given by individuals whose data is being processed, even if validly obtained, can cover or legalize a violation of any of the principles of processing. The Article 29 Working Party provided a clear answer to this question, advising the following: “Consent does not negate nor diminish in any way the obligations of the controller to comply with the principles of processing contained in the GDPR, especially in Article 5 relating to fairness, necessity and proportionality, and the quality of the data.

Even if the processing of personal data is based on the consent of the data subjects, this circumstance cannot ensure the lawfulness of the practice of collecting data that is not necessary for the specific purpose of processing and that would be fundamentally unfair.⁴¹



¹ Article 29 Working Party, Guidelines on consent under Regulation 2016/679

8.3. Purpose limitation

Relevant provisions: *GDPR* – Article 5, Recitals 39, 50 and 61; *PDPL* – Articles 5-7.

*Personal data must be collected for specific, explicit, justified, and lawful purposes, and it cannot be processed in a manner that is incompatible with those purposes (“purpose limitation”).*⁴⁹

The principle of purpose limitation essentially consists of two fundamental guidelines: (1) before starting the processing, it is necessary to precisely define and explicitly explain why the data is being collected, and (2) data collected for the initial purpose cannot be further processed for any other incompatible purpose.

The legal framework for personal data protection does not prescribe which purposes are allowed and which are not; instead, it grants the data controller the freedom to define the purpose in line with the objective of establishing data processing. The principle of purpose limitation in the processing of personal data instructs the data controller to collect data for specific, explicit, justified, and lawful purposes and ensures that, after collection, the data is not used for purposes that are incompatible with the initially stated purpose.

The data controller must determine the purpose of the processing at the latest when collecting the data, which is the moment when the processing begins. This means that the data controller must be certain about the objective of processing the data beforehand; therefore, it is not permissible to initiate processing under the motto of “let’s collect the data now that we have the opportunity, we don’t know what we might need it for”. Once the purpose is determined, it becomes the cornerstone of data processing, and as a rule, the data controller is no longer able to easily change the purpose and generally cannot deviate from the boundaries set by that purpose.

Dilemmas and Best Practices

Determining the purpose is the first step in the compliance process with the Personal Data Protection Law and the foundation from which the necessary documentation is developed. The expectations of the Commissioner and the data subjects are that the data controller will demonstrate compliance through documentation prepared prior to the beginning of data collection. Having documentation on the processing operation prior to commencing the processing facilitates demonstrating adherence to this principle.

⁴⁹ Serbian Personal Data Protection Law, Article 5, paragraph 1, point 2.

Therefore, the data controller must define a **specifically determined purpose** based on their predefined objectives. This means that vague and broad purposes cannot be chosen; instead, precise, understandable, and specific purposes need to be defined based on the processing objectives. In practice, it is desirable to have multiple specifically determined purposes for a data processing operation, while it is risky to have multiple data processing operations based on one broadly stated purpose.

Guidelines

The data controller might think that when initiating the processing, it is best to set a broad purpose to encompass all possible future processing scenarios. However, this is not allowed. According to the opinion of the Article 29 Working Party on purpose limitation, the purpose cannot be defined in general terms such as “improving user experience”, “marketing purposes”, “research”, or “cybersecurity”.¹ The specificity of the purpose requires that it be expressed in clear and unambiguous terms that enable understanding of the exact nature of the purpose.²

For example, the EDPB opinion on video surveillance states that the purposes of surveillance must be specified for each surveillance camera in use and that “video surveillance whose purpose is 'security' or 'for your safety' is not sufficiently specific”.³ However, in appropriate circumstances, it would be sufficient to specifically define compliance with the obligations of the employer-data controller in accordance with the specific occupational health and safety regulations applicable to the case.

¹ Article 29 Working Party, *Opinion 03/2013 on purpose limitation*

² *Ibid.*

³ EDPB, *Guidelines 3/2019 on processing of personal data through video devices*



Finally, it is necessary for the purpose to be **justified and lawful**. Lawfulness of the purpose refers to the circumstance that it does not violate other imperative provisions of the Personal Data Protection Law or provisions of other relevant regulations, such as those in the field of contract law, consumer law, or labour law. The explicit requirement that the purpose must be justified is somewhat specific to the Law. Justifiability of the purpose should be understood as its compliance with public order and general societal values, which can be expressed through a broader regulatory framework, self-regulatory instruments, and generally accepted social norms. Therefore, justifiability should be accepted as quite flexible and locally specific. For example, a process that represents a justified processing in one location may theoretically be an unjustified processing in another location, or processing that was unjustified before the COVID-19 pandemic may be justified after the outbreak of the pandemic.

Guidelines

The opinion of the Article 29 Working Party on purpose limitation states that the lawfulness of the purpose is determined in relation to the entire legal framework, from constitutional principles, through laws and subordinate regulations, to case law.¹ Furthermore, when assessing the lawfulness of the purpose, customs and business practices, self-regulatory codes, ethical codes, contracts, as well as the context and circumstances in the specific case, including the nature of the relationship between the data controller and the individual, can be taken into account.



¹ Article 29 Working Party, Opinion 03/2013 on purpose limitation

Data collected for the initial purpose cannot be further processed for any other incompatible purpose. For example, Julia visited her lawyer and disclosed family circumstances related to her mother's health condition and challenges with managing the family property. Her inquiries were focused on selling her mother's property to cover the costs of a rare disease therapy, while her mother did not want to sell the property and intended for it to be inherited by the descendants. The following week, Julia receives an email stating that her mother has been enrolled in a state program supporting therapies for rare diseases. It turned out that the lawyer's daughter, after the father shared Julia's distressing story with her, decided to independently enrol her in the program. In addition to breaching his duty of confidentiality,⁵⁰ the lawyer violated the principles of lawfulness of processing and purpose limitation since Julia shared this information solely for the purpose of analysing the legal aspects of property alienation and not for finding other sources to cover medical expenses or for enrolment in state support programs.

As an **exception to the principle of purpose limitation**, it is provided that in certain circumstances the data controller may proceed with further processing of personal data beyond the initial purpose for which they were collected, when such processing is compatible with the original purpose. This means that deviation is allowed when it is considered customary and expected in specific circumstances. In this process, the data controller is obligated to make a decision to expand the purpose based on conducting a compatibility test as provided in Article 6(2) of the Personal Data Protection Law, which is based on the following criteria:

1. The existence and nature of the connections between the initial purpose and the purpose of further processing - it is not necessary for the new purpose to be a "sub-purpose" of the initial purpose, but it is sufficient for the new and initial purposes to be normally pursued together or for the new purpose to be a logical consequence of the initial purpose.
2. The context in which the data was initially collected and the relationship between the data controller and the individuals whose data is processed,

⁵⁰ Serbian Legal Profession Act, Article 20.

that is the reasonable expectations of those individuals in the given situation regarding the specific data controller, taking into account the established practice between them.

3. The nature of the personal data, especially whether it involves special categories of data.
4. The possible consequences of further processing (taking into account both positive and negative consequences).
5. The protective measures that have been implemented (e.g., encryption, pseudonymisation).

It should be noted that this list of criteria provided by the Law is not exhaustive, and in accordance with the principle of fairness, the data controller should consider other relevant criteria in the specific case.

Guidelines

The UK supervisory authority ICO takes the position that the compatibility test considers similar factors to the balancing test when establishing legitimate interest as a legal basis.¹ Therefore, if you are unable to establish processing based on legitimate interest in a specific case, it is unlikely that the expansion of purpose will be possible. Accordingly, ICO notes that if the initially collected data was based on consent, the data controller will generally be obligated to obtain new consent to ensure that the processing is fair and lawful.



¹ ICO: *A guide to the data protection principles*

Dilemmas and Best Practices

It is advisable to document the decision to initiate processing for other purposes by conducting a compatibility test and to assess how this expansion of purpose affects the established framework of compliance with the Personal Data Protection Law.

Let's take an example of a data controller who operates a sports centre and holds a large collection of data about its users, their habits and interests, collected for the purpose of their training in the sports centre and to fulfil their user agreements. Meanwhile, the data controller establishes a business collaboration with a new sports brand in the market. In order to promote the new brand, the sports centre provides certain personal data of its users to its partner, so that they can receive offers for sports equipment based on their interests. Although the data controller believes that users would be happy to receive such offers, as they include certain discounts, this involves using the data for a completely different purpose than the one for which it was initially collected. As a result, this processing cannot be qualified as an expansion of purpose in accordance with the compatibility test. Instead, an entirely new data processing must be established with its own purpose, legal basis, and other specificities.

Practice

After a technical glitch caused server malfunctions, the data controller created a test database in which copies of personal data of one-third of users were entered. The original database contained data of subscribers to the controller's newsletter for direct marketing purposes. The original database also contained data of system administrators who provided access to the website interface.

When the data controller learned that an ethical hacker had gained access to the test database containing the data of 320,000 individuals, they signed a confidentiality agreement with the hacker, rewarded them, and deleted the test database. Within 72 hours, the data controller informed the competent supervisory authority, which initiated a supervisory procedure. The supervisory authority determined that the data controller had violated the principles of purpose limitation and storage limitation, as they had failed to delete the test database one and a half years after conducting necessary tests and fixing errors. After the supervisory authority imposed a fine of EUR 248,000, the data controller appealed the decision, leading the court to refer a preliminary question to the Court of Justice of the European Union: "Does the principle of purpose limitation allow the data controller to store personal data, collected and stored lawfully and for a specific purpose, in another database?"¹

The data controller and the supervisory authority disagreed on the nature of the purpose of processing data in the test database. While the data controller argued that the test database was necessary to ensure uninterrupted access for their clients until the errors were fixed and that the purpose was identical to the original purpose, the supervisory authority considered the processing within the test database to be further processing for the purpose of conducting tests and fixing errors. The CJEU held that the creation of a new database and the transfer of personal data to this database constituted a form of further processing. Although the CJEU left it to the national courts to decide whether the purpose of further processing was compatible with the original purpose, it provided additional guidance to the national court by stating that the purpose of conducting tests and fixing errors was linked to the performance of the subscription agreement, considering the potential impact of errors on the execution of the agreement.



¹ GDPR Hub, CJEU – C-77/21

Therefore, if after establishing the processing and determining the purpose, the data controller decides to have additional objectives and wants to process the collected data for additional purposes, this can generally be done in three ways:

- Establishing a new data processing operation and determining a new processing purpose that requires its own implementation logic in accordance with the Law;
- Further processing, outside the original purpose for which they were collected, when it is determined that such processing is in line with the original purpose through the compatibility test; or

- Further processing for archiving purposes in the public interest, for scientific and historical research, and for statistical purposes (more on this in Chapter XIII).

8.4. Data minimisation

Relevant provisions: GDPR – Article 5, Recital 39; PDPL – Article 5.

Personal data must be adequate, relevant, and limited to what is necessary for the purpose of processing (“data minimization”).⁵¹

Until the new legal framework for the protection of personal data was established, processing practices often involved data controllers collecting and processing a wide range of personal data, following the maxim “the more, the merrier”. However, the fundamental requirement set by the principle of minimization is proportionality, which means that the personal data being processed must be limited to what is necessary for the established purpose of processing, and they must be adequate and relevant specifically for that purpose. The established limitation applies to both the scope and quality of the data. For example, if a data controller wants to send notifications to clients exclusively via email, they only need their email addresses for that purpose, and processing all other data for this purpose would be unnecessary. If, when sending notifications, the data controller wants to differentiate clients by sending different notifications to different age groups, then it would be appropriate to process the date of birth in addition to the email address. However, if the data controller wants to differentiate minors from adults in a specific case, it may be sufficient to process data indicating whether the person is over 18 years old. In other words, precise definition of the processing purpose is of fundamental importance in respecting this principle, and any data that is not necessary to fulfil the processing purpose is considered excessive and violates this principle through excessive processing. The application of this principle is directly related to individuals’ rights to erasure and restriction of processing.

Guidelines

In accordance with Article 39 of the GDPR, excessive processing refers to processing data in a situation where the purpose of processing can reasonably be achieved by other means. Specifically, this means that the data controller is required to assess whether there are reasonable alternatives to achieve the purpose of processing. Therefore, to comply with the principle of minimization, two conditions must be cumulatively met:

- Processing only data that is necessary for that purpose of processing; and
- The purpose of processing cannot reasonably be achieved by collecting less data or less sensitive data.

⁵¹ Personal Data Protection Law, Article 5, paragraph 1, point 3.

Let's imagine an online bookstore that enters into a contract for the sale of books with its customers, for which it requires information on payment and delivery. The principle of minimization would be violated if the online purchase form includes mandatory fields for data that is not necessary for the execution of this contract, such as date of birth, phone number, gender, and similar information, and if the online purchase cannot be completed without entering this data.

Illustrative example can also be a company whose activities involve some dangerous or high-risk jobs. While processing data on the blood type of employees performing such tasks may be justified in case of an incident, it is not necessary to request such data from workers who perform administrative tasks in their offices.

Practice

There have been numerous violations of the minimization principle in European practice. Hence, in numerous decisions it has been established that **excessive processing** occurs when:

- Amusement parks take photographs of their visitors upon entry.¹
- Conference centres require identification documents when purchasing tickets.²
- Hotels scan passports of their guests.³
- Scooter rental companies track the location of their scooters every 30 seconds.⁴
- Data controllers require identification documents to grant rights to the individuals concerned.⁵

¹ GDPR Hub, AEPD (Spain) – PS/00068/2021

² GDPR Hub, Persónuvernd (Iceland) – 2020010611

³ GDPR Hub, AEPD (Spain) – PS/00078/2021

⁴ GDPR Hub, CNIL (France) – SAN-2023-003

⁵ GDPR Hub, AEPD (Spain) – PS/00003/2021



The CJEU has provided guidelines on how to assess whether a specific data processing activity (in the specific case, in video surveillance) can be considered necessary for the legitimate interests pursued by the data controller.¹ The Court ruled that the necessity of processing data must be examined in connection with the principle of data minimization, which restricts the options of the data controller to “adequate, relevant, and not excessive” data for the purposes of collection. The Court clarified that the data controller must, among other things, consider “whether it is sufficient for the video surveillance to operate only at night or outside working hours, or whether it is necessary to block or blur the images in areas where surveillance is not required”.

Particularly significant are numerous decisions by European supervisory authorities that have identified violations of the minimization principle in relation to the implementation of video surveillance. Violations often involve recording areas that are outside the established purpose of surveillance, such as public spaces (streets, playgrounds, etc.) or private spaces (rooms or private gardens of neighbours), and cases of excessive video surveillance in the workplace are not uncommon. Referring to the principle of minimization, the Hungarian supervisory authority, NAIH, emphasized that video surveillance, due to its invasiveness, is an appropriate processing activity only in situations where the purpose cannot be achieved in any other way.² Therefore, it is advisable to examine whether the purpose can be achieved through alternative means before implementing a video surveillance system. If it is possible without significantly greater resources, considering legal and ethical risks, video surveillance may not be the best choice.

¹ CJEU, Case C-708/18, TK v Asociația de Proprietari bloc M5A-ScaraA, 11 December 2019 (rectified 13 February 2020), margin number 51

² GDPR Hub, NAIH (Hungary) – NAIH-3748-1/2021



The Serbian Commissioner

The retention of citizens' ID cards by various institutions for the purpose of identification and security checks when entering premises was a topic addressed by the Commissioner in 2015. It was common practice for individuals, especially when entering government institutions, to be asked to submit their ID cards, which were then copied or retained until they left the building. The Commissioner deemed this practice unjustified and unnecessary, as the same goal could be achieved in a less intrusive manner. The Commissioner stated: “While it may be justified in some situations for an official in the public or private sector, for preventive or possibly subsequent protection of property and individuals, to identify individuals by inspecting their ID cards and recording certain information

(name, surname, ID number, time and reason for entry and exit, etc.), it certainly does not justify retaining or copying the ID card, as that is obviously unnecessary for the purpose of processing.¹

¹ Commissioner, *Retention of identity cards - unauthorized processing of personal data*, 06/09/2015. [in Serbian]



The principle of data minimization is closely linked to the GDPR concepts of privacy by design and privacy by default, which are incorporated into the Personal Data Protection Law through Article 42. These concepts require data controllers and processors to establish systems during the development and design phase that do not contain data that is not necessary for processing. Therefore, data controllers must understand that having an excess of data can lead to complications, and they are obliged to carefully determine the extent of data necessary to achieve the processing purpose.

Dilemmas and Good Practice

A particular challenge in terms of personal data protection is the development of machine learning solutions when the input data contains personal data. The concept of processing large amounts of data, inherent in machine learning and other artificial intelligence technologies, is conceptually opposed to the principle of data minimization. Generally, it is possible to develop machine learning models with minimal processing of personal data in most cases, although their accuracy may be slightly lower. For these reasons, it can be said that the legal framework for personal data protection somewhat limits the development of artificial intelligence and affects the quality of its results.

DataJust is a project initiated by the French Government aimed at harmonizing court practice in the area of compensation. DataJust is essentially an AI-based technology that processes large amounts of personal data from accessible case law. This has raised questions regarding the lawfulness of data processing, processing of sensitive data, violations of the principle of data minimization, and the unacceptable limitation of individuals' rights. Despite criticism, the Supreme Administrative Court approved the implementation of the project for a two-year period and took the position that, in order to achieve accurate results, it is necessary to process a large number of court decisions, which will be pseudonymised in this process. The court concluded that the established processing procedures are not contrary to the principle of data minimization.¹

¹ GDPR Hub, CE – 440376.



8.4. Accuracy

Relevant provisions: *GDPR* – Article 5, Recital 39; *PDPL* – Article 5.

*Personal data must be accurate and, if necessary, kept up to date. Taking into account the purpose of processing, all reasonable measures must be taken to ensure that inaccurate personal data is promptly erased or corrected (“accuracy”).*⁵²

The principle of data quality, or accuracy, requires diligence from data controllers in processing personal data. The data being processed must be accurate and, when necessary, kept up to date to reflect any changes. Considering the purposes for which the data is processed, the data controller must ensure that inaccurate data is promptly erased or corrected.

In certain situations, the application of this principle can have significant and far-reaching consequences for individuals. This is particularly true when decisions about rights or opportunities are made based on personal data, such as when approving a loan. An everyday example could be a store processing customers' addresses to deliver purchased products on a weekly basis, and it must effectively update this information when a customer changes residence. The application of this principle is directly related to the right to rectification and completion of data.

Practice

In a case involving an Italian electricity distributor, a consumer was mistakenly classified as insolvent within the distributor's operations. As a result of the inaccurate data being shared with the institution maintaining the insolvency register, the consumer missed the opportunity to switch distributors and achieve certain savings. The consumer approached the Italian supervisory authority, which found that tens of thousands of consumers had been denied a change of distributor due to the same error. As a result of this and other relevant GDPR violations, the distributor was fined 1 million EUR.¹

In a similar case in Spain, an electricity distributor failed to adequately process information about a consumer's change of residence. The distributor continued to send bills to an address where the consumer was no longer able to receive them.

¹ GDPR Hub, Garante per la protezione dei dati personali (Italy) – 9832979



Consequently, the distributor reported the payment default to a credit bureau, impacting the consumer's credit rating. The Spanish supervisory authority determined that this case involved a continuous violation of the accuracy principle and fined the distributor 50,000 EUR (the total fine amounted to 100,000 EUR, as it involved other violations as well).²



² GDPR Hub, AEPD – PS/00220/2020

The concept of data accuracy should be interpreted broadly and contextually in relation to the purpose of processing. Data can be considered inaccurate even if it is incomplete or taken out of context.⁵³ The extent and cause of the inaccuracy, as well as the responsibility for the inaccuracy (whether it lies with the controller or a third party) or whether the data was inaccurate at the time of collection or became inaccurate later, are not relevant. However, the nature of the data can impact the application of this principle. When it comes to data that can be considered **objective facts** (such as personal name, height, education level, etc.), the accuracy principle is applied uncompromisingly, and inaccurate data must be corrected with accurate information. When discussing opinions and predictions, the situation is somewhat more complex.

The accuracy principle cannot be applied on **opinions and assessments** expressed by third parties regarding the data subject, due to their subjective nature, meaning that we cannot challenge the accuracy of opinions. For example, you cannot request a correction of a comment on the Airbnb platform stating that you left the kitchen in poor condition, even if you believe you made an effort to leave it clean and tidy before leaving the property. A professor who is evaluated by students at the end of a semester cannot dispute the grades assigned to his teaching performance. Therefore, the controller has a duty to distinguish between facts and opinions, and when appropriate, attribute opinions to the individuals expressing them and the circumstances under which they were expressed. It matters whether an assessment of an employee's capabilities is provided by a direct supervisor, a colleague competing for the same promotion, or a customer with whom the employee had only indirect contact. If the data subject challenges the accuracy of opinions about them, it is good practice to record such complaints and the supporting arguments

Predictions of future behaviour and assessments of individuals resulting from profiling, artificial intelligence technologies, and machine learning systems cannot be considered subjective opinions or information. Therefore, the accuracy principle generally applies to them. Evaluating someone as a high-risk customer when they are not can result in violations of the accuracy

53 R cker, D., Kugler, T. (eds.), 2018, *New European General Data Protection Regulation: A Practitioner's Guide*, C.H. Beck, Hart, Nomos, p. 68.

principle and potentially infringe on the rights of the individual. In such cases, all the data used for processing may be accurate, but the outcome itself may be flawed due to processing logic deficiencies. For example, if an individual legally receives periodic income in cash while complying with tax regulations, they should not be assessed as high-risk solely because money does not regularly appear in their bank accounts every month. This violation can be severe and, in addition to liability under data protection regulations, may lead to claims for compensation, especially if the misjudgement resulted in missed opportunities or stricter contractual terms for the data subject. Of course, if an individual can prove that the assessment is inaccurate, they have the right to request its correction

The accuracy principle also includes a specific duty for the controller to take reasonable measures to ensure that the personal data they process is up-to-date and aligned with any changes that have occurred since the data was collected. This duty is not absolute and will depend on the nature and purpose of the processing. For example, when circumstances involve continuous data processing with potentially significant consequences for individuals' rights, periodic data accuracy checks are necessary. When data processing is one-time or the processing of inaccurate data does not affect individuals' interests, such as when processing email addresses for sending promotional messages, periodic updating may not be necessary. Instead, accuracy concerns will be addressed based on data subject requests for rectification and completion. If the controller regularly processes personal data collected from established databases of third parties, there is a reasonable expectation for periodic data updating to align with any changes that have occurred in the meantime.

The Serbian Commissioner

When applying the accuracy principle, it is not enough for the controller to state in their general policy that their employees are obliged to collect only accurate data and ensure its currency. According to the Commissioner, the controller must take specific organizational, technical, and personnel measures to ensure that their employees act in such a manner. This includes specifying in their policy the exact actions that their employees should take for this purpose, without shifting the responsibility for such actions onto them. It is also not sufficient for the controller to obligate individuals intending to enter into a contract with them to provide accurate and up-to-date personal data. The controller must take active steps to verify which individuals the data pertains to and the accuracy of that data by taking all reasonable measures.¹

¹ *Protection of personal data: Positions, opinions and practice of the Commissioner, publication no. 6, Belgrade, 2021. Case number: 072-07-2076/2020-07, pp. 38-40. [in Serbian]*



Praksa

After a company that owed a certain amount to a Spanish bank changed their legal representatives, the bank provided information about the previous representative to a debt collection agency. Based on the provided data, the agency contacted the individual to demand payment. Since the individual was no longer associated with the debtor as a representative or in any other way, they initially approached the controller with a request to delete their data. When this request was denied, the individual turned to the supervisory authority, which found a violation of the accuracy principle and imposed a fine of 60,000 EUR on the controller (the fine was reduced to 36,000 EUR by a higher instance decision).¹



¹ GDPR Hub, AEPD – PS/00219/2019

Depending on the purpose and legal obligations, it may be important for the controller to keep the entire history of changes for a particular piece of data, including previous inaccurate and updated data, as well as information about when and why they were changed. Let's consider a hospital patient receiving an incorrect diagnosis during treatment and taking a certain therapy for weeks based on that diagnosis. After further analysis, the diagnosis was changed, and the patient received a new therapy. However, the initial incorrect therapy had consequences on their body that also need to be monitored. For successful treatment, it is equally important to keep all relevant data, regardless of their accuracy. Therefore, in order to assess the need to retain previously amended data, it is advisable to apply the minimization principle and consider whether the purpose can be achieved without the amended data.

The duty of the controller to ensure data accuracy also extends to the obligation to inform all recipients to whom personal data has been disclosed about any correction or erasure of personal data or the restriction of its processing, unless it is impossible or requires excessive time and resources. The data subject should also be informed about these actions.

8.5. Storage limitation

Relevant provisions: *GDPR* – Article 5, Recital 39; *PDPL* – Articles 5 and 8.

*Personal data must be kept in a form that allows the identification of individuals only for the period necessary to fulfil the purpose of processing (“storage limitation”).*⁵⁴

Načelo ograničenja čuvanja se sastoji od dve komponente:

⁵⁴ Article 5, paragraph 1, point 5.

1. Obligation to determine in advance the retention period for the data, depending on the purpose of processing, and this period must be necessary to fulfil the purpose, i.e., there must be a rational and compelling justification for why the purpose cannot be achieved within a shorter period; and
2. The duty to delete or anonymise the data (so that identification is no longer possible) after the expiration of that period.

In theory this principle is also referred to as the “temporal aspect of the minimization principle”.

Personal data may only be kept in a form that allows the identification of individuals for as long as necessary to fulfil the purpose for which the data is processed. Therefore, after determining the specific purpose and defining the scope and quality of the data that need to be processed to achieve the purpose, the controller should also determine how long it is necessary to keep the data in their possession.

The retention period is directly related to the legal basis for data processing. For example, a controller who has installed video surveillance to secure business premises from theft or unauthorized entry should determine how long it is necessary to retain those recordings to fulfil this purpose and delete the recordings after that time. In the case of a store that installs security cameras between shelves to prevent theft and conducts monthly inventory checks to identify any shortages, it is not justified to retain the security camera footage for an extended period.

Practice

The controller's negligence and a lack of care for the personal data being processed are the most common reasons for a violation of the principle of storage limitation. Since this issue is not difficult to establish, there have been numerous European decisions where violations of this principle were identified, resulting in significant fines. The Danish supervisory authority, *Datatilsynet*, issued a 1,345,000 EUR fine to a bank not having procedures in place for automatic deletion in over 400 systems for personal data processing.¹ The French supervisory authority, CNIL, found that a large financial institution had implemented limited retention policies in only a few areas of its operations. Although the institution was able to demonstrate plans for implementation in all areas, the fact that they had not implemented them in a timely manner resulted in fines of 1,750,000 EUR.

¹ GDPR Hub, Datatilsynet (Denmark) – Danske Bank

² GDPR Hub, CNIL (France) – SAN-2021-010



If personal data is processed in the context of fulfilling a contract, processing on that legal basis ceases once the contract is performed. However, in such cases, the controller will typically have an interest in continuing to retain certain personal data based on legitimate interests, for example, until the expiration of limitation periods, in order to pursue any legal claims against the former contracting party.

Dilemmas and Best Practices

In Serbia, the Law on Records in the Field of Employment is in force mandating permanent retention of all personal data from these records.¹ While there may be questions about whether such provisions themselves comply with the principles of personal data processing, as long as this regulation is in force, employers must ensure the retention of a large amount of personal data on this basis without a time limit. Therefore, it is important to respect all other principles of processing, primarily through the implementation of appropriate organizational and technical measures.

¹ Law on records in the field of labour (Official Gazette of the FRY, No. 46/96 and Official Gazette of the RS, No. 101/2005 - other law and 36/2009 - other law)

Finally, when the retention period expires, the controller is obliged to delete the data without any additional requests from the individuals to whom the data pertains. It is expected that the deletion of data will be carried out automatically, without any further action required by the controller and its employees, whenever possible. Upon the expiration of the retention period, the controller has the option to retain data relevant to its operations, which can later be used for analytical purposes, provided that anonymisation is performed. This allows for the retention of the knowledge that data may contain while simultaneously moving beyond the scope of the data protection legal framework, enabling alternative treatment of the data.

Dilemmas and Best Practices

Good practice entails having internal data retention policies that specify the types of data you process, the purposes for which you use them, and how long you intend to retain them. The purpose of such policies is to establish and document standard retention periods for different categories of personal data. It is also advisable to establish processes that ensure your organization effectively adheres to the established retention periods. For processes involving continuous and/or mass processing, it is desirable to establish time periods after which a review should be conducted to determine if it is still necessary to process all categories of data and to redefine existing policies.

Similar to the principle of purpose limitation, an exception to the principle of limited retention is established in favour of archiving in public interest, scientific or historical research, and statistical purposes. In line with the framework of freedom of expression, longer storage periods are permitted in cases where the public

interest in research and preservation of collective memory prevails. However, the application of this exception does not relieve the controller of the obligation to implement appropriate technical and organizational measures for data processing

8.6. Integrity and confidentiality

Relevant provisions: *GDPR* – Article 5, Recital 39; *PDPL* – Article 5.

*Personal data must be processed in a manner that ensures appropriate protection, including protection against unauthorized or unlawful processing, as well as against accidental loss, destruction, or damage, through the application of appropriate technical, organizational, and personnel measures (integrity and confidentiality).*⁵⁵

Due to the importance of protecting citizens' personal data from various forms of security breaches, integrity and confidentiality are among the six fundamental principles. Following the GDPR, the Law lists unauthorized or unlawful processing, accidental loss, destruction, or damage of data as the most common security breaches. However, this principle also applies to any other situation in which personal data may be compromised in any way.

Data integrity requires that data must be accurate, up-to-date, and complete in accordance with the purpose for which they are processed, aiming to prevent errors, irregularities, and misinterpretation of personal data. Additionally, integrity should guarantee that personal data will not become inaccessible to the data subjects, whether they are destroyed, lost, or locked by malicious attackers. Integrity is expected to ensure trust in the data that represent a resource for processing. **Data confidentiality** principle demands that personal data must be stored and processed in a manner that protects privacy and ensures their safeguarding against unauthorized access, alteration, deletion, and theft, with the goal of preserving privacy and preventing unauthorized access and misuse of personal data. Confidentiality is expected to ensure that access to data and processing means is enabled exclusively to authorised individuals, in order to build trust in the processing operation.

To ensure compliance with this principle, data controllers are obliged to implement appropriate technical, organizational, and personnel measures that guarantee the integrity and confidentiality of personal data.⁵⁶ This constitutes the practical aspect of this principle. It involves the use of security technologies and procedures, as well as training employees who handle personal data, to reduce the risk of unauthorized access, alteration, or unauthorized disclosure of this data. Neither the GDPR nor the domestic Law prescribes the specific measures that have to be implemented, as they always depend on the specific situation, risk assessment, and a range of additional factors such as the type and quantity of data, the purpose

⁵⁵ Article 5, paragraph 1, point 1.

⁵⁶ More on measures in Chapter X - Responsibility and compliance

of processing, retention periods, storage methods and locations, and more. Threats can come from external actors like cybercriminals, but they can also arise from within the organization (e.g., if employees handling personal data are inadequately trained), and they can be the result of intention, negligence, or accidents.

Therefore, the decision on appropriate technical, organizational, and personnel measures is one of the decisions that the data controller should make before commencing processing. However, due to the rapid development of technology and changes in internal organization, it is necessary to continuously assess the adequacy of existing measures and introduce appropriate enhancements and adaptations to maintain an optimal level of security and processing safety.

Example

A company uses a software application in its operations that processes both customer and employee data. From the perspective of appropriate organizational and technical measures, it is not acceptable for all user accounts to have access to all data. The data controller should implement access controls through role-based systems and authorizations, ensuring that only the HR department can access employee data, while employees can access relevant customer data needed for their work. Additionally, in an organization where a larger number of employees can access customer data, the data controller is obliged to establish a log management system that records data access and documents all processing actions and changes. Log management is essential for determining responsibility regarding data accuracy and unauthorized processing, detecting security incidents and operational issues, and serves as an invaluable tool in IT audits and forensics.

In the role of a data controller, a physical clinic keeps information about the exercise program that each client should undergo with the physiotherapist, including sensitive health data. For practical reasons, besides electronic form, this information is also kept on paper, which is used each time the client comes for therapy. Appropriate protective measures involve keeping the paper form under lock and key, with access granted only to authorised personnel, and ensuring that the paper form is destroyed as soon as it fulfils its purpose.

Recently, examples of data encryption during malicious ransomware attacks have been prevalent in various sectors, particularly within healthcare systems and medical institutions. In these cases, individuals can be harmed not only due to unlawful processing of personal data but also as a result of the loss of this data. For instance, if a hospital loses access to patients' personal data during a ransomware attack, patients may be deprived of adequate treatment guaranteed by the healthcare system. Therefore, the hospital must ensure that patients' personal data is resilient to such attacks and not susceptible to being deleted or altered in any other way.

Practice

After a patient requested copies of her medical documents regarding a past mammogram, the data controller responded that they couldn't provide her with the mammogram images due to the system only retaining them for three months. Additionally, the data controller claimed that the images were stored on an external data storage device after the Greek supervisory authority initiated an inspection. However, the data controller was still unable to access the image. The supervisory authority determined that the data controller had lost access to the images containing personal data, thus preventing the patient's right of access. However, considering that data retention for this type of processing was mandated for a period of 10 years from the patient's last visit, the supervisory authority identified a violation of the principles of integrity and confidentiality and imposed a fine of 30,000 EUR on the medical diagnostic centre due to insufficient technical and organizational security measures.¹



¹ GDPR Hub, HDPa (Greece) – 36/2022

8.7. Accountability

Relevant provisions: *GDPR* – Article 5, Recitals 39 and 74; *PDPL* – Article 5.

*The data controller is responsible for the implementation of the provisions stated in paragraph 1 of this article and must be able to demonstrate their compliance (“accountability”).*⁵⁷

In the early years of the internet, it was challenging to hold companies accountable for poor data collection and protection practices. This was partly due to the underdeveloped legal framework, where the duties of data processors were still unclear or not established at all. Gradually, the legal framework transformed, recognizing the significance and value of data and its connection to privacy and other human rights. However, data controllers and processors resisted regulation and evaded or diluted their responsibility by hiding behind the technology-driven complexity and obscurity created by. Organizations often held data processing systems or processors accountable for their decisions, avoiding their own responsibility. Data controllers dismissed requests directed at them, redirecting them to processors and other actors involved in the processing. These actors, in turn, evaded any form of responsibility as they had no direct relationship or duty towards the individuals whose data was being processed. Without clear rules and established practices, and with limited understanding of the complex information ecosystem, individuals were left largely unprotected in terms of their rights. The legal framework for personal data protection, primarily established by the

⁵⁷ Article 5, para 2 of PDPL

GDPR and later by the Serbian Data Protection Law, creates a chain of responsibility that extends from data controllers to processors and sub-processors, with little room for contractual or other forms of avoidance of responsibility. Within the EU, the chain of responsibility is strengthened by the fact that supervision is entrusted to independent supervisory authorities with considerably high powers in terms of penalties.

As the six fundamental principles of data processing represent key rules for compliance with the legal framework for personal data protection, the additional principle of accountability precisely establishes the duty of the data controller to ensure the implementation of the processing principles within their organization and be able to demonstrate their compliance. Previously, data controllers were required to register their data collections with the competent authority, such as the Commissioner for Information of Public Importance and Personal Data Protection, and this mechanism was supposed to provide controllers with a kind of confirmation that their collections were lawful and their data processing practices were in line with legal rules. However, it has been proven that this logic of aligning processing operations with legal rules is not efficient, as it is not feasible to allocate enough resources to verify the lawfulness of every registered collection. In practice, this obligation has been reduced to a mere administrative requirement of registering the collection, devoid of its essence. The practice of prior registration of data collections is still applicable in legal systems that have not aligned with the GDPR.

However, in the European Union, the Republic of Serbia, and other jurisdictions that have modernized their data protection legal frameworks, data controllers themselves must ensure the implementation of all necessary rules within their personal data processing systems, and the verification of their compliance with regulations is only conducted when the controller is required to prove their compliance in a specific procedure (e.g., a supervisory procedure initiated by the Commissioner or procedures initiated by data subjects).

As the principle of accountability demands an active approach by the data controller towards the legal framework for personal data protection, there is often a dilemma about how far the controller should go in implementing and documenting adherence to the six fundamental principles. The effort that a data controller needs to undertake will essentially depend on the type of organization they represent, as well as the scope, frequency, and complexity of the processing operations they manage. The expectations for small and medium-sized enterprises, in principle, are lower than those for corporations, and they will also differ depending on whether it is a traditional business or an organization operating in the digital economy. However, sometimes organizations with only a few employees operate at such a high level of process automation that their large-scale personal data processing operations far exceed the risks of processing in traditional sector organizations with dozens or thousands of employees. In such cases, the obligations of these micro-organizations in the context of personal data processing will be extensive, and the size of the organization will not affect the principle of accountability.

In other words, every data controller must implement the principle of accountability in accordance with the specific circumstances of the case.

Primer

The data controller has launched an online game that requires basic identification information during registration: full name, date of birth, email address, and the player's time zone. During registration, players are adequately informed about all processing activities, and their consent is required to enter the game. After registration, players have the opportunity to build their avatar, an online identity that is fully public and serves the purpose of successful interaction with other players. The game is accessible through a publicly available web browser page, and player data is stored on servers designated for that purpose. To align with the legal framework for personal data protection, the data controller has created records of processing, appointed a data protection officer, obtained ISO27001 certification for the website, and implemented internal procedures that restrict access to identification and contact data to only a few individuals within the organization (those involved in customer support and notifying players about game changes). The data controller has organized training and informed all employees that this data must not be shared with any third party or processed for other purposes within the organization. Additionally, the data controller has employed an information security consultant, who has implemented secure data transfer between the website and designated servers, as well as two-factor authentication for all individuals potentially accessing personal data. Considering the nature, scope, circumstances, and purposes of the data processing, as well as the risks associated with the processing of personal data, it appears that the data controller has taken appropriate measures to comply with the framework for personal data protection:

- The processing is lawful and proportional, with a clearly defined purpose.
- The ISO 27001 certification and the mechanism for secure data transfer between the website and servers demonstrate compliance with privacy requirements.
- The establishment of processing records, internal procedures, training, and two-factor authentication mechanisms confirm the implementation of appropriate technical, organizational, and personnel measures.
- The appointment of a data protection officer and engagement of a consultant in information security indicate additional measures taken and capacity for ongoing compliance monitoring.

Detailed overview of the responsibilities of data controllers and processors is presented in Chapter X.

9. Lawfulness

Relevant provisions: *GDPR* – Article 6, Recitals 40-50; *PDPL* – Articles 12-14.

9.1. When is processing lawful?

Lawfulness of processing means that data can only be processed if there is a proper legal basis for the specific processing, i.e., if the processing is based on one of the six available legal bases prescribed by the law.

Therefore, after making a decision to initiate the processing of personal data and determining the purpose, the data controller must identify the most appropriate legal basis for the processing before collecting and further processing the data. If the processing for the intended purpose cannot be based on any of the available six legal bases, such processing is prohibited, i.e., unlawful and must not be carried out.

None of the available legal bases is stronger or better than others, and there is no hierarchy among them - the legal basis is chosen according to which one best suits the specific purpose before commencing the processing.

According to our Law, in line with the GDPR, the following legal bases exist:

1. Consent of the data subject,
2. Execution of a contract with the data subject,
3. Compliance with legal obligations of the data controller,
4. Protection of vital interests,
5. Performance of tasks carried out in the public interest,
6. Legitimate interests pursued by the data controller or a third party.

If the processing involves special categories of personal data, the law prescribes additional conditions for the processing to be lawful.

Once the appropriate legal basis is identified, the data controller is obliged to document the existence of the legal basis in accordance with the principle of accountability. If the legal basis is legitimate interest, the data controller can explain it within the records of processing activities or in a separate document (more about the balancing test will be discussed later). Alternatively, if processing is based on consent, the data controller should be able to document the obtained consent. Documenting can be done electronically or in printed form.

When multiple legal bases are applicable to a specific processing activity, the data controller should choose the most appropriate one. It is contrary to the principle of lawfulness, fairness, and transparency to have more than one legal basis for a single processing activity. The circumstances need to be assessed, and each time the legal basis that best reflects the essence of the relationship between the data controller and the individuals should be chosen. For example, it often happens that when entering into a contract with a user, the data controller relies on consent as the legal basis instead of the execution of a contract. In such cases, consent is not necessary if all the personal data collected is necessary for the conclusion and execution of the contract.

Trusted resources

The UK supervisory authority ICO has developed a tool that helps data controllers make informed decisions about the appropriate legal basis.¹ This tool is fully applicable in the EU and in the Republic of Serbia.



¹ ICO, *Lawful basis interactive guidance tool*

Guidelines

In its guidance on personal data protection, the UK supervisory authority ICO recognizes the common dilemma when choosing a legal basis: whether to rely on legitimate interests or consent.¹ The ICO guidance requires considering the broader context, including the following questions:

- Who benefits from the data processing?
- Do individuals expect this processing to take place?
- What is the relationship between the data controller and the individuals?
- Does the data controller have a significantly stronger position than the individuals?
- What impact does the processing have on individuals?
- Are individuals members of vulnerable categories?
- Are there likely to be objections to the processing from individuals?
- Can the data controller stop the processing at any time upon request?

It is advisable to consider legitimate interests as a legal basis if you want to retain control over the processing and take responsibility for proving that it aligns with individuals' reasonable expectations and does not have an unjustified impact on them. On the other hand, if you prefer to give individuals full control and responsibility regarding their data (including the ability to change their mind about the continuation of the processing), you may want to rely on consent.



¹ ICO, *UK GDPR guidance and resources – Lawful basis*

Furthermore, one of the fundamental rights of individuals is the right to be informed, which entails that the data controller informs the individual about various aspects related to the processing of their data, for example, through a privacy policy or in another suitable manner. Hence, the data controller must inform the individual about the legal basis for processing their data.

Once the purpose of processing and the legal basis are determined, the data controller should not later change the legal basis unless there is a change in the purpose of processing. Changing the legal basis, especially when the initial one was consent, can be particularly challenging. If the data controller changes the purpose of processing, it is necessary to assess whether the previous legal basis remains appropriate. In such cases, the data controller should inform the data subject about the changed purpose, determine a new legal basis (or retain the existing one if it is still the most appropriate for the new purpose), and inform the individual about their rights in light of the changed circumstances.

Example

The data controller is a telecommunications company that collects and processes certain customer data given while entering a contract for providing mobile telephony services. For this purpose, the data controller processes customer data based on the conclusion and execution of a contract, including the customer's email address to send monthly service invoices. The data controller also wants to process the customer's email address for marketing purposes, in order to email promotional offers. Since this is a different purpose of processing, the data controller should determine a new legal basis, which in this case would be the customer's consent that needs to be obtained before initiating the processing

If the individual later decides to withdraw their consent regarding the processing for marketing purposes, exercising their right to do so, the question arises whether the data controller could continue the processing by relying on legitimate interests as the legal basis. However, even if the data controller initially could have relied on legitimate interests, they cannot do so later because it is not possible to change the legal basis once the initially chosen basis was found to be inappropriate. Therefore, it was necessary to clearly communicate to the individual from the beginning that the processing is based on legitimate interests. Leading individuals to believe they have a choice when the choice becomes irrelevant later is unjust and contrary to the principle of fairness. The data controller must, therefore, stop the processing once the individual withdraws their consent..

The significance of legal bases is manifold. In addition to the fact that different legal bases are established and documented in different ways, they establish different relationships between controllers and data subjects. Considering that the data controller selects the legal basis, their choice establishes the foundations of the relationship with the individuals whose data is being processed. Therefore, depending on the legal basis chosen, individuals have different rights, considering that the rights are generally not absolute. The legal bases create a relationship that grants varying degrees of authority to individuals in order to protect their interests

		Legal basis					Legitimate Interest
		Consent	Contract	Legal Obligation	Vital Interests	Public Interest	
Data subject rights	Information	✓	✓	✓	✓	✓	✓
	Access	✓	✓	✓	✓	✓	✓
	Rectification	✓	✓	✓	✓	✓	✓
	Erasure	✓	✓	✗ Not applicable ¹	✓	✗ Not applicable	✓
	Restriction of processing	✓	✓	✓	✓	✓	✓
	Portability	✓	✓	✗ Not applicable	✗ Not applicable	✗ Not applicable	✗ Not applicable
	Object	✗ Not applicable: You should withdraw consent	✗ Not applicable	✗ Not applicable	✗ Not applicable	✓	✓ At all times for Direct Marketing
	No fully automated decision incl. profiling	Right to a human intervention	Right to a human intervention	Right to a human intervention	✓	✓	✓

¹Erasure can be requested if the personal data has to be erased for compliance with a legal obligation

Figure 3: Legal bases and rights of citizens

9.2. Conclusion and execution of contracts

Relevant provisions: GDPR – Article 6, Recitals 40 and 44; PDPL – Article 12.

A common legal basis for processing in business relationships between the data controller and partners and customers, when processing is necessary for the performance of a concluded contract or when the data subject requests certain actions to be taken before the conclusion of the contract.

This basis is used when conclusion of a contract is necessary in order to provide a specific service to the data subject, or if actions are carried out to prepare for the conclusion of the contract. This would, for example, be the case when an individual sends a request to a seller for an offer for purchasing a product, and the seller retains the data such as the name and (email) address for a certain period of time to send them an appropriate offer, even if the contract is not ultimately concluded.

Example

An individual wishes to conclude a comprehensive car insurance contract for their vehicle, so they contact several different insurance companies requesting sales quotes to compare and choose the most favourable offer. Insurance companies ask for certain personal data from the individual in order to provide a quote, using contract conclusion as the legal basis for this purpose. Eventually, the individual will decide to enter into a contract with only one of these companies, and the other companies with whom a contract is not concluded should delete the data, as they no longer have a legal basis for processing.

Under this legal basis, it is important to ensure that the data is truly necessary for the conclusion or execution of the contract, and no other data are collected in line with the principle of minimization. Therefore, the data controller must ask themselves: what is the nature of the service I am providing to the individual whose data I am processing, what are the essential elements of the contract, and what are the reasonable expectations of an average person to whom I am providing services/selling products regarding the data I can request from them in order to provide the service/sell the product. If the processing of certain data is not truly necessary for the conclusion and execution of the contract, i.e., the requested service can be provided without processing specific data, then the data controller should find another appropriate legal basis, such as consent or legitimate interest, for example.

Example

An individual wants to enter into a contract with a fitness centre in order to use its services. During this process, they fill out a standard contract that includes the input of specific personal data. The fitness centre requests the individual to provide additional data about their workplace and occupation, in addition to basic contact information. However, such data is not necessary for the conclusion of a contract with the fitness centre, so the legal basis of contract conclusion and execution cannot be used for their processing. Furthermore, the fitness centre violates the principle of data minimization, as the purpose can be achieved with the processing of a smaller amount of data. In order for the fitness centre to rely on contract conclusion and execution as a legal basis for processing, it needs to collect only basic contact information from its future users. If there is another purpose for collecting additional data, the fitness centre should find another legal basis for their processing such as consent, in case for example the fitness centre aims to profile its users based on their occupation.

Guidelines

EDPB emphasizes that providing online services often involves targeting users with various advertising content based on the analysis of their online behaviour, which practically involves tracking and profiling such users, mainly using technologies like cookies.¹ Contract conclusion and execution in the context of providing online products/services cannot be a valid legal basis for profiling user behaviour, their preferences and choices, as the data controller is not engaged in such profiling. The user has entered into a contractual relationship with the data controller to receive a specific service or purchase a particular product. Therefore, the data controller needs to obtain user consent for cookies before initiating profiling and tracking user behaviour using such technology.

¹ Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects



What happens to data and the legal basis for processing once the contractual cooperation ends, when the contract ceases to be valid for any reason? In such cases, data controller rarely deletes or ceases processing data of the individual with whom a contractual cooperation existed immediately. However, this means that the data controller now needs to find another legal basis for data processing, as the legal basis of contract conclusion and execution is no longer applicable, since the contractual cooperation has ended.

Example

After concluding a travel organization contract, a travel agency retains certain personal data of travellers even after the tour has ended, in case there is outstanding debt from a traveller. This is done so that the agency can exercise its rights in court and file a lawsuit for damages against the debtor. The agency retains this data until the expiration of statutory limitation periods for filing a lawsuit against non-paying travellers, based on legitimate interest as a legal basis. The agency has a legitimate business interest in seeking legal recovery of travel-related debts.

Practice

An apartment owner noticed high electricity consumption in their building and contacted the Slovenian Data Protection Supervisor. The tenant believed that certain private companies were connected to the electricity supply in the building and that residents were paying their bills as well. The apartment owner had previously inquired with the building manager about the shared electricity connection, but the manager refused to respond, citing data protection.

The Slovenian supervisor ordered the building manager to disclose the requested personal data without the consent of the data subjects. Such disclosure was necessary to determine the obligations of apartment owners in the building, i.e., to establish contractual obligations.¹ Therefore, contract execution as a legal basis allows for the processing of this data, and consent is not relevant in this case.

¹ GDPR Hub, IP - 07121-1/2021/678

Contract execution is a relatively stable legal basis for the data controller, unlike consent, as the individual does not have the authority to withdraw their consent and thereby thwart the data controller's intent. However, in order for the data controller to rely on this legal basis, it is necessary to adequately document the existence of the contract, as proving the existence of verbal contracts can be problematic in practice. Documentation is particularly significant in case of unencumbered contracts, which are difficult to distinguish from consent in practice.

Practice

Provincial Administrative Court in Warsaw annulled a decision by the Polish supervisory authority, as the court considered that the authority did not adequately explain why it held that the personal data of the complainant were processed based on a contract, rather than consent.¹ This case thus concerns a legal dispute regarding the legal basis – whether it is consent or contract conclusion and execution.

The individual whose data were processed lodged a complaint with the Polish supervisory authority against the unlawful processing of personal data by the data controller. The case involved a woman who had given written consent to the data controller (video producer) for the use of her image in a music video without compensation. The data controller later published the video on certain social media and platforms, along with her photographs and full name. The complainant highlighted that she did not enter into a contract with the data controller, nor did she receive any compensation for her participation in the video and the use of her image.

Upon withdrawing her previously given consent, she requested the data controller to erase her personal data and cease processing, which the data controller did not do. She then approached the relevant Polish authority, requesting an order for the data controller to delete her data. The data controller claimed that her data were being processed based on a contract. The Polish supervisory authority dismissed the complaint, leading the individual to appeal to the competent Polish court.

The court annulled the decision of the Polish personal data protection authority, as it deemed that the reasons for holding that a contract had been concluded between the complainant and the data controller, involving her appearance in the video produced by the data controller, were not precisely explained. The court considered that there was a lack of precision and accuracy in the established facts, rendering the conclusions of the Polish supervisory authority regarding the justification of the complaint premature.

¹ GDPR Hub, WSA Warsaw - II SA/Wa 1899/2

9.3. Compliance with legal obligations

Relevant provisions: *GDPR* – Article 6, Recitals 40 and 45; *PDPL* – Article 12.

As a distinct legal basis for processing, the Law stipulates compliance with legal obligations of the data controller, which involves situations where a positive legal provision requires the data controller to collect and process personal data in order to fulfil a specified prescribed obligation. Therefore, in order to use this legal basis for data processing, a specific law must require the data controller to process certain data. This obligation for the data controller cannot arise from a contract, non-binding guidelines, or requests from a government body; it must be a mandatory legal provision. The processing must be necessary for the fulfilment of a specific purpose, also established by law.

Example

A law that regulates mandatory social insurance obligates the employer to enrol their employees in mandatory social insurance. For this purpose, as the data controller, the employer must process specific personal data of their employees in order to fulfil their legal obligation.

The Law on Records in the Field of Labour obligates the employer to permanently keep a large amount of data about their employees, even those whose employment has ceased. To fulfil the obligation prescribed by this law, the employer, as the data controller, maintains records containing a range of personal data about employees, such as names, personal identification numbers, educational background, etc.

The Law on Life Insurance obligates the insurance company to collect and retain various personal data about the insured individual to pay out a premium in the event of an insured incident..

Practice

The Icelandic Data Protection Supervisor decided that the processing of personal data by a financial institution related to a financial transaction is permissible based on Icelandic money laundering law.¹ The supervisor received a complaint regarding a request from the local bank *Landsbankin* for information about the complainant's

¹ GDPR Hub, Persónuvernd – 2020010532



annual balance at another bank, *Kvika banki*, in relation to specific financial transactions with *Landsbankinn*. The complainant transferred a certain sum of money from *Kvika banki* to *Landsbankinn*, and a month later, they requested *Landsbankinn* to withdraw a significant portion of the transferred amount from their account. Citing the Icelandic money laundering law, *Landsbankinn* requested information about the origin of funds and sought information about the complainant's account at *Kvika banki*.

The supervisor concluded that *Landsbankinn* had a legal basis for processing the complainant's personal data based on the Icelandic money laundering law, as such processing was necessary for the bank to fulfill its legal obligation.

Practice

The court of first instance in the Hague rendered a decision that the use of a digital questionnaire by Dutch authorities to assess the psychological condition of firearm owners does not contravene Article 6 of the GDPR that regulates the legal bases for processing, specifically the point of the provision related to the legal obligation of the data controller to process.¹

In the Netherlands, there is a legal obligation to assess the psychological state of individuals applying for a firearm license, with regard to the risk of misuse. The state has developed a digital questionnaire for this assessment, consisting of ten possible risk factors, through which personal data is collected. Hunting and shooting sports associations claimed that the digital questionnaire was contrary to the GDPR.

The judge ruled that the processing within the questionnaire complies with Article 6(1)(c) of the GDPR (legal obligation of the data controller) and that a valid legal basis for data processing exists because the law mandates the data controller's obligation to process the data.



¹ GDPR Hub, Rb. Den Haag - C/09/585239/ KG ZA 19/1221

The Serbian Commissioner

The complainant submitted a request to the Business Registers Agency, as the data controller, to delete their personal identification number from the field "legal representative" in the Business Entities Register on the agency's website, as they did not provide consent for the publication of personal data. The Commissioner, in addressing the complaint, concluded that the Business Registers Agency is not obligated to obtain consent for publishing personal data of the legal representative of a business entity on its website nor to delete the data, as it has a legal basis for data processing, based on compliance with the legal obligations of the data controller,

according to the Law on Business Entities, which in Article 9a stipulates that data about individuals subject to registration obligation are personal name and unique citizen identification number, for domestic natural persons.¹

¹ *Protection of personal data: Positions, opinions and practice of the Commissioner, publication no. 6, Belgrade, 2021. Case number: 072-16-2911/2019-06, pp. 43–44. [in Serbian]*



9.4. Legitimate interests

Relevant provisions: *GDPR* – Articles 6, 13-14 and 49, Recitals 40, 47-50; *PDPL* – Article 12.

If the processing of personal data is necessary to achieve the legitimate interests of the data controller or a third party, such processing can be carried out, except in situations where the interests or fundamental rights and freedoms of the data subject outweigh such legitimate interests, especially if the data subject is a minor.

Example

The most common, though not the only examples of legitimate interests in business practice include:

- Direct marketing;
- protecting individuals and property, preventing harm;
- detecting fraud or criminal activities;
- ensuring the security of the company's information network;
- screening potential clients;
- achieving a legitimate level of operational efficiency.

Legitimate interest is the most flexible legal basis, as it is specifically determined by the data controller in the given circumstances. However, this does not mean that they have free rein, as that would contradict the principles of personal data processing. Therefore, legitimate interest, as a rule, should protect a legitimate interest of the data controller, rather than simply serving as a tool for pursuing their commercial interests. This legal basis is used in situations where individuals could reasonably expect their data to be processed.

For legitimate interest to be used as a legal basis, the data controller needs to establish a legitimate interest, demonstrate that the processing of personal data is necessary to achieve it, and assess that the legitimate interest outweighs the risks to the interests, rights, and freedoms of the data subjects. In cases where these risks are significant, legitimate interest cannot be casually used as a legal basis, and the data controller must either find another legal basis or refrain from initiating such processing.

While the most flexible from the data controller's perspective, this legal basis is legally the most uncertain, as it relies on subjective assessment. It's clear that data controllers cannot simply and unilaterally declare protection of some of their interests (such

as various purely commercial interests), especially considering that the data subjects themselves have certain special rights that they can exercise in these situations, such as the right to object. Therefore, it is crucial for such an assessment to be supported by solid arguments, taking into account all relevant circumstances of the specific case.

While the Law does not impose an obligation on the data controller to conduct a balancing test before using legitimate interest as a legal basis, this standard has emerged in practice and effectively allows the data controller to decide whether their legitimate interest outweighs the rights and freedoms of the data subjects. The balancing test aims to thoroughly assess three key questions:

1. Whether the specific interest is genuinely legitimate in the given circumstances, i.e., whether it is objective, substantial, and real;
2. whether the processing is necessary for achieving the legitimate interest in the specific case; and
3. whether the legitimate interest outweighs the interests or fundamental rights and freedoms of the data subjects.

The data controller needs to document the balancing test to be able to demonstrate, if necessary, that they have taken all relevant circumstances into account before commencing data processing under this legal basis. If the data controller lacks sufficient internal expertise and is uncertain about the decision, they can engage an expert and impartial entity to conduct the balancing test and reach a conclusion.

The Serbian Commissioner

The Commissioner has prepared answers to frequently asked questions regarding legitimate interest and the application of Article 12(1)(f) of the Personal Data Protection Law.¹ In addition to this document, the Commissioner has developed a Model of the Legitimate Interest Assessment, the use of which is not mandatory but facilitates data controllers in conducting a balancing test.² The Model consists of a series of questions that the data controller should answer to perform a self-assessment of whether legitimate interest can be used as a legal basis for processing in a specific case. In developing the Model, the Commissioner used a template created by the UK supervisory authority ICO for this purpose.³

¹ Commissioner, "Legitimate interest as a legal basis for personal data processing" [in Serbian]

² Model of the Legitimate Interest Assessment [in Serbian]

³ ICO, Sample LIA template



Commissioner's Model of the Legitimate Interest Assessment

Part I

Basic information about intended personal data processing

1. Why do you want to process specific personal data – define the purpose of processing?
2. What outcome do you expect to achieve from the intended processing?
3. Would anyone else benefit from the intended processing? If yes, specify who and provide reasoning.
4. Would the processing be beneficial for the broader community? If yes, provide reasoning.
5. How important is the benefit that can be achieved through processing – for you, someone else, and/or the broader community?
6. What would be the consequence of not conducting the intended processing?
7. Which category/categories of individuals do the data relate to?
8. What personal data do you intend to process?
9. What processing actions do you intend to perform? If you intend to transfer data to another country or international organization, specify which one.
10. Besides the Personal Data Protection Law, are there other regulations that should be applied to the intended processing?

Part II

Necessity of processing

1. Does the intended processing genuinely enable achieving the purpose you have defined?
2. Can the same purpose be achieved without processing personal data (e.g., through processing of statistical data)?
3. Can the purpose be achieved with the processing of a smaller amount of data?
4. Can the purpose be achieved with processing less intrusive into the privacy of individuals?
5. Are the data limited to those that are suitable, essential, and necessary in relation to the purpose of processing?

Part III

Preponderance of interests

1) Nature of data

1. Does processing involve special categories of personal data as per Article 17 of the Personal Data Protection Law?
2. Does it concern data related to criminal convictions, offenses, and/or security measures as per Article 19 of the Personal Data Protection Law?
3. Does it concern other data commonly regarded as confidential (such as a personal bank account balance, etc.)?

4. Is it data about minors or individuals belonging to other sensitive social groups, such as unemployed individuals, the elderly, single parents, etc.?
5. Does the data pertain to an individual in their personal or professional capacity?

2) Expectations of individuals

1. Are you processing, or have you previously processed data of that/those individual(s)? If yes, specify the legal basis for processing.
2. If you are processing, or have previously processed data of that/those individual(s), does your relationship with them involve a higher level of confidentiality (e.g., doctor-patient / bank-client)?
3. Are the data you are processing, or have previously processed, collected from the data subjects or from another source?
4. What processing information have you provided to individuals during previous data collection?
5. How much time has passed since the previous data collection?
6. Is the intended processing method common for the specific purpose?
7. Do you intend to introduce a new processing method or other innovation to achieve a specific purpose?
8. Have you collected data about the expectations of individuals regarding the processing of their data through a survey, questionnaire, or other means?
9. Are there other indicators suggesting that, in the given circumstances, individuals expect or do not expect the processing of their data?
10. How do you intend to provide information about the processing to the individual(s) whose data is being processed, before commencing the processing?

3) Consequences that intended processing may have on the interests and fundamental rights and freedoms of the data subjects

1. In what way (desirable, as well as undesirable) can the intended processing impact the individuals whose data is being processed?
2. Is it possible that individuals may lose control over their data due to the intended processing, such as in cases where all information is not provided or effective realization of rights prescribed by the Personal Data Protection Law is not ensured?
3. Considering the circumstances of the intended processing, are you obligated, in accordance with the Personal Data Protection Law, to perform an assessment of the impact of the intended processing actions on the protection of personal data before commencing the processing?
4. Can you apply measures that would reduce the possibility of adverse consequences or the level of risk to the rights and freedoms of individuals?
5. Can an individual decide to exclude their data from the intended processing without adverse consequences?

Assessment

1. Can you apply legitimate interest of the data controller / third party as a legal basis for the intended processing of personal data in the specific case?
2. If you answered affirmatively to the previous question, specify the nature of your legitimate interest in the intended processing of personal data. Provide reasoning.
3. If you fall within the group of data controllers who are required by the Law to appoint a data protection officer, or if you have appointed a data protection officer even though you are not legally obligated to do so, specify whether that officer has provided an opinion on the intended processing. Provide reasoning.

Guidelines

In its 2014 opinion, Working Group 29 recognized the significance and utility of legitimate interest as a legal basis that, under proper circumstances and with adequate safeguards, can help prevent excessive reliance on other legal bases.¹ According to this opinion, legitimate interest should also not be treated as a “last resort” for rare or unexpected situations in which other legal bases cannot provide lawful processing. Additionally, it is not advisable to unjustifiably expand its use based on the perception that it is less restrictive than other bases.

According to the Working Group's opinion, while similar, the concept of “interest” differs from the concept of “purpose”. While purpose represents a specific reason for which data is processed – the goal or intention of data processing – interest encompasses a broader motivation that the data controller may have. For example, the data controller may have an interest in ensuring the health and safety of employees working in a nuclear power plant. In this regard, the data controller's goal may involve implementing special access control procedures that justify the processing of specific personal data to ensure the health and safety of employees. Similar to purpose, interest must be sufficiently clear and precisely defined to enable the performance of a balancing test; interests that are overly unclear or speculative will not suffice.

The opinion asserts that the concept of legitimate interest can encompass a wide range of interests, whether trivial or highly compelling, direct or somewhat controversial. Accordingly, in the second step, when balancing these interests against the interests and fundamental rights of individuals, a more conservative approach is necessary, requiring a detailed analysis.

¹ Article 29 Data Protection Working Party, Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC



Clearly the legitimate interest can be used as a legal basis in situations where processing is necessary to achieve an interest that is objective, serious, and real, and when only the minimum necessary personal data is processed to achieve the purpose. Additionally, processing should be carried out in the least intrusive manner possible (for instance, sending an email instead of making a phone call for direct marketing is less intrusive), and the processing should not be an unpleasant surprise for the individual – in other words, the individual should have a justified expectation of the processing (e.g., the individual has already established a prior relationship or has contacted the data controller for another purpose).

Dilemma

GDPR stipulates that direct marketing (personalized commercial messaging) can be conducted based on legitimate interest. The counterbalance to conducting direct marketing based on legitimate interest is the individual's right to object (for instance, by clicking the "unsubscribe" link if the message was received via email or through a similar method), upon which the data controller must cease such processing, as it is deemed that the data controller's legitimate interest in conducting direct marketing is never more important than the rights, interests, and freedoms of the individuals to whom the direct marketing is directed, as explicitly provided by the Law.

On the other hand, GDPR lists direct marketing as one of the potential examples of legitimate interest. However, the EU's E-Privacy Directive is in effect, adopted by the national legislations of EU member states.¹ According to this directive, prior consent from individuals is required for conducting electronic direct marketing (sending emails, SMS messages, etc.), with some exceptions to consent that vary across national legislations, as well as an exception relating to sending promotional messages to existing customers or consumers.

The Personal Data Protection Law mentions direct marketing in the context of the possibility to object, upon which the data controller must cease processing. Therefore, PDPL implicitly considers direct marketing a possible legitimate interest. An individual whose data is being processed based on legitimate interest can always raise an objection, and the data controller must always honour that objection, particularly when it comes to direct marketing aimed at the individual raising the objection. However, there are various domestic sectoral laws that require consent or approval from individuals for conducting direct marketing (e.g., Consumer Protection Act, Advertising Act, Electronic Commerce Act, etc.). Hence, the question of whether and under what circumstances legitimate interest can be used as a legal basis for processing direct marketing in Serbia remains open.

¹ Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)



The Serbian Commissioner

The complainant, a former member of a religious community, submitted a request for the deletion of all personal data linking them to the community. The data controller responded that they had deleted all data except for the name, surname, and dates of joining and leaving the community. Dissatisfied with the response, the data subject lodged a complaint regarding the violation of their right to data erasure. When assessing the validity of the complaint, the Commissioner determined that the conditions for applying legitimate interest as a legal basis for data processing were met: within the “Legitimate Interest Assessment – Former Members” document, the data controller correctly assessed that their legitimate interest outweighed the interests and fundamental rights and freedoms of the complainant, considering various factors, including the preservation of religious principles, minimal risk to the person whose data is being processed, the complainant's expectations, and the applied protective measures. Therefore, the Commissioner decided that the complaint was not substantiated, as the processing of data regarding former members, including the complainant's data, was based on the legitimate interest of the data controller, which is reflected in the preservation of religious principles that the same person should not be baptized more than once.¹

¹ *Protection of personal data: Positions, opinions and practice of the Commissioner, publication no. 6, Belgrade, 2021. Case number: 072-16-781/2020-06, pp. 40–42. [In Serbian]*



Practice

The Norwegian supervisory authority sanctioned a data controller for the live streaming of camera footage on a YouTube channel.¹ The data controller installed a camera on the roof of their headquarters, which rotated and captured footage of a public road, parking area, entrances to several stores, a bank, city assembly, and several other buildings. The live streams were broadcasted on the company's YouTube channel, which had over a thousand followers. As the data controller did not use the footage themselves and did not determine a legal basis for processing in advance, the supervisor assumed that legitimate interest could be the legal basis. The supervisor identified two processing activities: one involved broadcasting the live stream to provide a service to local citizens, and the other involved storing and retaining the footage for a period of 14 days for the purpose of citizens' safety, with the footage being shared with the police as needed. The supervisor deemed that in this case, the rights and freedoms of individuals outweighed the data controller's interest, as there was no proven actual threat to citizens' safety. Consequently, the supervisor decided that there was no valid legal basis for the processing and imposed a monetary fine on the data controller

¹ GDPR Hub, Datatilsynet (Norway) - 20/01627.



Finally, it should be noted that, according to the provisions of the PDPL, government authorities are not allowed to use this basis for carrying out tasks within their jurisdiction.

9.5. Consent

Relevant provisions: *GDPR* – Articles 4, 6-9, Recitals 32-33, 40, 42-43; *PDPL* – Articles 4, 12, and 15.

Although consent as a legal basis is often emphasized, likely due to the prevailing misconception that it is the most secure legal basis, the fact remains that it should be used cautiously. Since consent can be easily withdrawn, the sustainability of processing is constantly at risk, making its implementation particularly challenging.

Two key reasons mandate the careful use of consent. Firstly, concerning the sustainability of processing with consent, there is uncertainty due to the circumstance that an individual who has given consent for processing can withdraw that consent at any time. This leaves the data controller without a legal basis for processing and requires them to cease processing unless an alternative legal basis can be found. However, the intention of the Law is not for legal bases to change frequently. In situations where it does change, the new legal basis should be appropriate for the same purpose of processing, the individual must be informed of the change in legal basis, and the question arises whether changing the legal basis for the same purpose aligns with the principles of transparency and fairness.

Secondly, consent is a particularly demanding legal basis in implementation, as the data controller must fulfil a series of legal conditions for consent to be legally valid:

- It is given **freely**, meaning it is not given under duress, pressure, or coercion, which, among other things, implies the absence of a significant imbalance in the relationship with the data controller (otherwise, the data controller would find it challenging to prove that such an imbalance did not practically exert pressure on the individual giving consent). For instance, whether the consent given by an employee to an employer for processing is given freely, considering that the employee is in a dependent position in relation to the employer, which raises the question of how much implicit pressure the employee feels to give consent;
- it is **unconditional**, meaning it is not conditioned on accepting other services or terms (e.g., it is not bundled with accepting the entirety of the terms of business);
- it is **specific**, meaning it is given for a particular purpose (if the purpose is overly broad, it could practically lead to a blanket consent for purposes that the individual was not aware of at the time of consenting, hence not knowing what they have actually consented to);
- if there are multiple purposes for which consent is needed, and these purposes are not interdependent and each can be performed separately, consent must be **granular**, implying that clear consent should be given for each individual purpose, and the individual should be able to choose to give consent for only some of them;
- it is **informed**, meaning the individual understands what they are consenting to, having all necessary information from the data controller to make an informed decision, including the categories of personal data to be processed based on consent, the data controller's identity, and the purpose of processing;

- it is **unambiguous**, which means the action of giving consent must be a clear affirmative action, not passive behaviour (active *opt-in*, not *opt-out*). For instance, consent given online would not be valid if the consent checkbox is pre-checked. The individual should provide their consent through an affirmative action (in this case, checking the box). If consent is given on a printed form, signing the form is a clear affirmative action through which consent is given;
- for the data controller to be able to prove valid consent if needed, it must be **documented**. This means the data controller must find an appropriate way to prove that they possess consent. For example, if consent is collected in printed form, the data controller should keep all consents in that form in one place. If consent is given online, the data controller can, for example, maintain a database with consent information or email messages informing the individual that they have given consent, providing information about the processing and their rights;
- it can be **withdrawn** at any time, easily and simply. The data controller must ensure that in the same way consent was given, it can be withdrawn (adding additional formalities, complicated identity verification procedures, lengthy form filling, or specific helpline calls to withdraw consent is not justified, if consent was given via email or online checkbox).

The text of consent should be clear and concise, in easily understandable everyday language that an average person can comprehend.

Guidelines

The EDPB's guidelines on consent take the position that consent can generally be an appropriate legal basis for processing in situations where the individual is offered a genuine choice regarding accepting or declining the offered terms, so that refusal does not entail a risk of harm.¹ When seeking consent, the data controller is obliged to assess whether all conditions for obtaining legally valid consent will be met. Consent granted by data subjects provides control over whether personal data will be processed. Otherwise, the individual's control over the data becomes illusory, and the consent will not be legally valid, rendering the processing activity unlawful. According to the EDPB's stance, obtaining consent should be subject to rigorous requirements prescribed by the GDPR, along with special attention when applying the principles of lawfulness, fairness, and transparency, purpose limitation, data minimization, and accuracy. These guidelines are of paramount importance in understanding various elements crucial for the legal validity of consent and encompass a multitude of useful and relevant examples across different sectors.

¹ EDPB, Guidelines 05/2020 on consent under Regulation 2016/679



The Serbian Commissioner

The data controller has violated Article 15 of the Personal Data Protection Law by not providing the opportunity for the individual to give specific consent via the Consumer Credit Request document for the processing of their personal data for the purpose of direct marketing, separate from other processing purposes stated in that document. By excluding such an option, the data controller has conditioned the submission of a credit request on consent to the processing of personal data for the purpose of direct marketing, which is not necessary for the data controller to respond to the credit request. Therefore, consent for processing for the purpose of direct marketing given through such document cannot be considered voluntary, specific, and unambiguous expression of the individual's will, nor is it freely given consent.¹

¹ *Protection of personal data: Positions, opinions and practice of the Commissioner, publication no. 6, Belgrade, 2021. Case number: 072-04-1750/2020-07, pp. 36–37 [in Serbian]*



Example

A company is organizing a corporate event and wishes to photograph business partners and other attendees for later publication in the media and on social media platforms. Accordingly, they require individuals' consent for taking and publication of photos. At the entrance, the company arranges the signing of a print consent form, which reads:

Welcome to our event!

For the purpose of promoting our company and this business event, we need to process your personal data, including your photograph and name.

By signing this form, you give your consent to company X, headquartered at address XY, the organizer of this event, to take photographs of you at the event and to publish them, along with your name, in the media and on its social media channels, for the stated purpose.

You may withdraw your consent at any time by sending an email to our contact address: X@X.com, after which we will cease processing your data and delete your photographs. Withdrawing your consent will not affect the lawfulness of data processing carried out prior to the moment of consent withdrawal.

Signature

Avoiding the use of consent is advisable in cases where another legal basis would be more appropriate, given that complying with the personal data protection legal framework is demanding when consent is chosen as the legal basis, obtaining it presents an additional burden for the data controller, and it can always be withdrawn. Therefore, when choosing consent as the legal basis, the data controller should assess the possibility of relying on another legal basis.

Example

Company X, engaged in online sales, requests consent on its website for processing personal data necessary for payment of purchased goods. In this situation, the legal basis is the conclusion and performance of a contract, as processing the customer's financial data (card number, code, etc.) is necessary for executing the transaction, i.e., the contract for the sale of goods through the website.

Company X wants its employees to install an application that will track time of their arrival and departure and the time actively spent working. Although the company might think that obtaining employees' consent for such processing is the easiest approach, it would not be an adequate legal basis here. Not only do employees have the right to withdraw consent at any time, but it's also questionable how freely given such consent would be. Additionally, the company could find itself in a situation where it has a legal basis for processing data only for those employees who have given consent. In this scenario, the data controller might consider relying on legitimate interest or the execution of an employment contract as appropriate legal bases, depending on the specific circumstances..

Practice

The Danish supervisory authority decided that the general recording of phone calls by the Danish Business Authority without prior consent constitutes a violation of the GDPR.¹ They found that consent was the only legal basis for such recordings, which were used to document intimidation of employees within the agency and for internal employee training.

The individual whose data was recorded filed a complaint with the Danish supervisor, claiming that the Danish Business Authority was recording phone calls of employees without their consent. It turned out that incoming calls had been recorded for the previous two years and retained for 96 hours. The Danish Business Authority argued that the recording was done to protect employees from criminal activities and for educational purposes, thus falling under the legal basis of protecting vital interests of employees and the agency's obligation to provide general guidance and advice. The supervisor emphasized that processing based on the protection of vital interests can only be carried out if no other legal basis is applicable. They highlighted that recording phone calls cannot be justified by preventing abuse of employees, as it happens extremely rarely and such invasive processing is unwarranted. Additionally, recording for educational purposes is not predominant over the rights and freedoms of the individuals whose conversations are recorded, thus necessitating consent for this type of processing. The supervisory authority therefore concluded that such processing is unlawful and should have been based on consent..

¹ GDPR Hub, Datatilsynet (Denmark) - 2020-32-1566



9.5.1. Consent of minors

Relevant provisions: *GDPR* – Articles 6, 8, 40, 57, Recitals 38, 58, and 75; *PDPL* – Article 16.

Certain specific rules from PDPL apply to the processing of children's data in relation to information society services that are typically provided for a fee, remotely, electronically, and at the recipient's request. If a data controller processes the data of individuals under the age of 15 in this context, the processing of their data will be lawful only if consent is given by the person holding parental responsibility over the child (usually parents). If the individual is older than 15, they can give consent independently. Therefore, data controllers providing services related to information society services should establish mechanisms that allow verifying that every individual giving consent is old enough to do so (without the need to determine the exact age). Depending on the risks associated with data processing, this verification can be done in various ways. One way is to request a simple statement that the user is old enough to provide their own consent. In situations involving higher risks, more effort is required for verification, for example, by using a third-party verification service, through a bank card, email, and similar means.

In any case, if consent is given by minors, the consent text should be specifically adapted to their age.

The Serbian Commissioner

PDPL sets the age limit for independent consent by a minor only in the case of using information society services, which implies services typically provided for a fee, remotely, electronically, and at the recipient's request. Other cases or age limits for a minor's independent consent to data processing concerning them can be determined by other specific regulations.¹

¹ *Protection of personal data: Positions, opinions and practice of the Commissioner, publication no. 6, Belgrade, 2021. Case number: 073-17-1883/2020-02, pp. 100–101 [in Serbian]*



Guidelines

EDPB's Guidelines on consent provide additional explanations regarding the scope of information society services and the responsibilities of guardians, as well as specifics concerning the necessary age for independent consent, which vary across different EU member states.¹

¹ EDPB, Guidelines 05/2020 on consent under Regulation 2016/679



Trusted resources

European Digital Rights has prepared a special guide “Digital Defenders v. Info Intruders” intended for the youngest cyber actors. Presented in the form of a comic and detection of a secret word, the guide introduces children to their rights in the digital environment, including rights related to personal data protection. The guide's text has been translated into many European languages and is freely available for download.¹



¹ EDRi, “Your guide to the Digital Defenders”

Practice

The Irish supervisor fined the company Meta, which owns the platforms Facebook and Instagram, for the lack of a legal basis for processing contact data of business accounts of children on Instagram. The supervisor emphasized that this platform allowed children to switch from personal to business accounts, offering the child user the option to modify their contact information displayed on the public profile. In order to switch to a business account, the child user could (but was not required to) enter an email address or phone number.

To open a personal account on Instagram, the child had to agree to the Terms of Use, which stated two legal bases for processing children's data: the conclusion and performance of a contract and legitimate interest. The supervisor deemed that Meta violated the minimization principle as children's data were publicly displayed on their profiles. Additionally, the supervisor considered that the information provided to children about the processing was inadequate and that children were not properly informed about the publication of their contact information. In the supervisor's view, Meta did not implement adequate technical measures to prevent risks to children. Furthermore, Instagram accounts were previously automatically set to be public, including accounts belonging to children. Therefore, a new account would automatically be public unless the user changed privacy settings, meaning anyone could see the account's content. The supervisor believed that Meta did not clearly and transparently inform child users about the purpose for automatically setting accounts to be public, and this automatic setting was neither necessary nor proportionate to the processing purpose. It should also be noted that children have reduced capacity to perform the necessary settings to switch their account from public to private.

The Irish supervisor published all these conclusions in a draft decision and called on other European supervisory authorities to react. However, others opposed the draft decision for various reasons, prompting the Irish supervisor to submit the draft decision to the EDPB. Among other things, the EDPB concluded that children could not expect their profiles to be public; processing contact information was not essential for Instagram, and it was possible for a business account to function without disclosing children's contact information; the publication of children's contact information posed a significant risk to the rights and freedoms of children.

After the EDPB addressed several objections from other European supervisory authorities regarding the imposed fine, the Irish supervisor amended their initial decision and fined Meta with a monetary penalty of 405 million EUR.¹



¹ GDPR Hub, EDPB - Binding Decision 4/2022 – 'Meta (Instagram)'

9.6. Protection of vital interests

Relevant provisions: *GDPR* – Article 6, Recital 46; *PDPL* – Article 12.

Processing of personal data can also be carried out if necessary to protect the vital interests of the individuals whose data are processed, usually in situations involving matters of life and death. For example, processing is necessary to save someone's life or prevent harm, to control an epidemic, in cases of humanitarian crises, natural and man-made disasters, and so on.

The fundamental assumption underpinning this legal basis is that the right to life and other vital interests of the individual take precedence over the right to the protection of personal data. Therefore, these are exceptional circumstances in which personal data will most often be processed by controllers such as healthcare providers, rescue services, and similar entities, and in which the specific individual is often unable to give consent to the processing.

Example

An individual is urgently brought to the hospital because they have suffered a heart attack. The doctor attending to them needs to check their medical record to determine if there have been previous heart conditions or other relevant circumstances in order to provide immediate medical assistance.

In practice, it is most common for special categories of personal data, such as health data in emergency situations, to be processed in accordance with Article 17 of the Law.

Practice

Estonian data controller *M&M Inkasso OÜ* – a debt collection company, publicly disclosed personal data of debtors (names, photographs, etc.) on its website and social media as a form of retaliation for non-payment.¹



¹ GDPR Hub, AKI (Estonia) - 2.1.-5/22/22012

The national supervisor reacted and initiated an official inspection. The controller claimed that by disclosing debtor data, they intended to protect vital interests, namely to prevent exploitation of individuals who may come into contact with debtors. The company also argued that the data published about debtors had been obtained from the internet and were publicly available.

However, the Estonian supervisor concluded that the protection of vital interests can be used when there is no other more suitable legal basis. The supervisor argued that, in the case of payment delays, the creditor must first use legal remedies available under Estonian law of obligations. According to the supervisor, it was unlawful to publish debtor data related to payment delays as a means of retaliation. Therefore, the publication of this data on social media cannot be considered as protecting the vital interests of the creditor or other individuals.

The supervisor emphasized that, in accordance with Estonian personal data protection law, data can be published for the purposes of public information if the following cumulative conditions are met: there is a public interest in the publication, the publication is in line with the rules of journalistic ethics, and the publication does not violate the rights of the individuals to whom the data relate. The supervisor deemed that the condition of the existence of public interest was not met, and therefore, the publication of data was not carried out for the purposes of public information, as the cumulative conditions were not fulfilled.

In line with the conclusion that the controller processed personal data of debtors without a legal basis, the supervisor issued an order to remove the data and imposed a monetary fine.

9.7. Execution of public authority

Relevant provisions: *GDPR* – Article 6, Recitals 50, 55-56; *PDPL* – Articles 12 and 14.

The legal basis consisting of the performance of tasks carried out in the public interest or in the exercise of official authority vested in the controller will generally only be available to public authorities or institutions entrusted with public powers, and not to other categories of controllers. In order for this basis to be valid, the processing must have its specific legal basis in a law, meaning that a particular law prescribes the public interest that needs to be achieved, as well as the obligation to respect the principle of proportionality in relation to the aim pursued. The processing must be necessary and limited to a specific purpose.

PDPL does not provide definitions specifying what constitutes public interest or legally prescribed authority. However, in accordance with the provisions of Article 42 of the Constitution of the Republic of Serbia, which states that the collection, holding, processing, and use of personal data shall be regulated by law, it is important to clarify what needs to be regulated by law to allow a public authority to lawfully process data necessary for the exercise of its powers and activities. In this sense, the law should regulate:

- (1) Which public authority is authorized to process personal data, where the public authority can be specifically designated or at least determinable;
- (2) the purpose for which the data is processed, which can be regulated directly or indirectly;
- (3) the types or categories of data processed, including specific identification of the data elements and specification of the data subjects; and
- (4) who has the authority to access the data.

Therefore, this legal basis is available to public authorities or institutions with public powers as controllers, and it will not be used by the private sector.

Example

Public notaries in their daily practice process large amounts of personal data in the course of various certifications of signatures, contracts, and the like. As public authorities under the Law, they have legal authorization to process this personal data in accordance with the Law on Public Notaries.¹ For other processing activities where there is no public interest involved, public notaries use other available legal bases.

¹ Law on Public Notary ("Official Gazette of RS", no. 31/11, 85/12, 19/13, 55/2014 - other laws, 93/14 - other laws, 121/14, 6/15 and 106/15) [in Serbian]



Dileme

As the European companies prepared for GDPR, one of the main concerns was the fear that the new regulation would require controllers to have valid legal consent for a large number of their personal data processing activities. Consent became so popular during those months that in certain circles the idea spread that it is the main and superior legal basis, while all other legal bases are less important. This idea is not accurate and can certainly be dangerous. Consent is neither the main nor the best basis, and often not even appropriate. All legal bases are equal and each operates under specific circumstances, while there are situations in which each may not be suitable or even lawful.

The example of a hotel as a data controller can illustrate how the same data can sometimes be processed under multiple legal bases, always depending on the specific purpose of processing. When a guest comes to a hotel to rent a room or request other hotel services, they must provide certain information necessary to conclude and execute an accommodation agreement. The hotel also has an obligation to provide certain data collected in this manner to the police in accordance with relevant legal requirements. During their stay at the hotel, the guest may be offered certain optional benefits, such as participating in a loyalty program – in this case, they give consent for processing the data for this purpose, and they can withdraw their consent at any time without affecting the provision of services based on the main accommodation agreement.

Additional benefits may include, for example, the preparation of specific types of food in line with the guest's religious beliefs or health condition. In this case, explicit consent is required for this purpose, and such data must be treated as sensitive data. If an accident occurs during the guest's stay at the hotel, such as a fire, the processing of guest data for the purpose of protecting their vital interests may be considered. Finally, upon leaving the hotel, the hotel may decide to send certain promotional messages to its former guest based on its legitimate interest.

As for consent, it is not required from data subjects when there is a legal obligation for the controller to collect certain data, or when the data is necessary for the performance of a contract with that individual. In the practice of Serbian companies, for example, it is often the case that employees sign statements consenting to the use of their personal data, while according to positive domestic regulations, employers are obliged to collect dozens of different data from employees in order to fulfil various obligations related to labour, taxes, social security contributions, occupational health and safety, labour records, and the like. Additionally, there is an obligation to execute employment contracts. This certainly doesn't mean that consent shouldn't be sought from employees when that legal basis is the only option – for example, when employees agree that the employer can provide certain benefits on their behalf, such as various types of voluntary insurance, which requires the employer to engage in additional personal data processing beyond what is mandatory.

Furthermore, there is often confusion about whether a controller can rely on legitimate interest for certain processing activities or needs to seek consent. Which of these bases is more appropriate primarily depends on the purpose of processing, as well as other circumstances. However, a controller can always consider the consequences for achieving a specific purpose if the individual withdraws their consent and requests data erasure. Given that the consent rules require that processing must immediately cease if consent is withdrawn, if the controller cannot achieve the desired purpose without processing, consent as a legal basis is not a solution. Additionally, when a controller initially decided to process personal data based on consent to fulfil a certain purpose, if the individual decides to withdraw consent and requests data erasure, the controller does not have the right to change their mind on the established legal basis and continue processing data based on, say, legitimate interest.

If the balancing test has shown that the data subjects' interests are not significantly compromised in a particular situation, however, there is no need to seek any consent for processing from those individuals. If the legal basis for processing is the legitimate interest of the controller, which may have been confirmed by a court or the Commissioner, the individual does not have an unrestricted right to demand that the processing be stopped and the data erased. These rights can only be exercised under certain conditions, and the individual also has other rights available, such as the right to object..

9.8. Lawfulness of processing special categories of data

Relevant provisions: *GDPR* – Article 9; *PDPL* – Articles 17 and 18.

The Law stipulates that the processing of special categories of personal data is generally prohibited, except in specific cases.⁵⁸ In other words, the existence one of the described legal bases is not sufficient for the processing of data in this category; at least one additional condition must also be fulfilled.⁵⁹ Additional conditions under which the processing of special categories of data is allowed include the following situations:

- When the data subject explicitly consents to the processing for one or more specified purposes, unless processing is required by law and not based on consent;
- when processing is necessary for the performance of obligations or exercise of rights of the controller or the data subject in the field of employment, social security, and social protection law, as provided by law or a collective agreement;
- when processing is necessary to protect the vital interests of the data subject or another natural person where the data subject is physically or legally incapable of giving consent;
- when processing is carried out in the course of the legitimate activities of a foundation, association, or other non-profit organization with appropriate safeguards, provided that processing relates solely to members, former members, or individuals who have regular contact with the organization in connection with its aims;
- when personal data that is processed is made public by the data subject;
- when processing is necessary for the establishment, exercise, or defence of legal claims or whenever courts are acting in their judicial capacity;
- when processing is necessary for reasons of substantial public interest defined by law, which shall be proportionate to the aim pursued, respecting the essence of the right to data protection, and provide for suitable and specific measures to safeguard the fundamental rights and interests of the data subject;
- when processing is necessary for preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment, or the management of health or social care systems and services on the basis of the law or pursuant to a contract with a health professional and subject to the conditions of professional secrecy;

⁵⁸ Article 17 of the PDPL.

⁵⁹ This is the position taken by Working Party 29. See, for example, Guidelines for automated decision-making about individuals and profiling for the purposes of Regulation 2016/679 of February 2018: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053.

- when processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of the law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;
- when processing is necessary for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes, which shall be proportionate to the aim pursued, respecting the essence of the right to data protection, and providing for suitable and specific measures to safeguard fundamental rights and interests of the data subject.

In processing special categories of data, due to the general prohibition, the principle of data minimization comes to the forefront. This means that processing should be limited to the absolute minimum necessary to achieve the purpose of processing.

Practice

A person who was an insurance policyholder filed a complaint against the Danish insurance company *Tryg Forsikring A/S* with the national personal data protection authority.¹ The individual believed that they had suffered a violation by the insurance company because they claimed that instead of retaining their data for a period of five years, as agreed upon before the insurance claim was realized, the company retained the data for ten years.

The insurance company argued that they retained the data to determine whether the individual was eligible for insurance premium. According to their perspective, retaining health-related data for a period of ten years was necessary for the establishment, exercise, or defence of a legal claim, which is one of the situations allowing the processing of special categories of data. Additionally, the insurance company stated that the legal basis for data processing was the conclusion and execution of a contract, and they did not rely on consent as a legal basis.

The Danish data protection authority concluded that the insurance company processed the data in accordance with the GDPR, and medical data was collected to determine the individual's eligibility for a premium under the concluded insurance contract. Thus, the Danish authority concluded that the processing of health data was carried out in accordance with Article 9 of the GDPR. It was also determined that the processing was carried out under the legal basis of contract conclusion and performance, as the processing was necessary for the execution of the insurance contract.

¹ GDPR Hub, Datatilsynet (Denmark) - 2020-31-3840



The Serbian Commissioner

The healthcare institution failed to provide adequate protection of the patients' personal data, including protection against unauthorized or unlawful processing, thereby violating the principles of integrity and confidentiality. During the determination of the processing method and throughout the processing itself, the controller did not implement necessary protection mechanisms to fulfil legal processing conditions and protect the rights and freedoms of the data subjects. Technical measures for an appropriate level of security concerning the risk of unauthorized disclosure and access to data were not put in place. As a result, eighteen employees had unauthorized access to the electronic health records of a patient in whose treatment they were not involved. Following the conducted supervision, the Commissioner issued a reprimand to the controller. The controller complied with the reprimand within the set timeframe and informed the Commissioner that disciplinary proceedings had been initiated against all employees and partners due to unauthorized access to the patient's records.¹

¹ *Protection of personal data: Positions, opinions and practice of the Commissioner, publication no. 8, Belgrade, 2023. Case number: 072-04-1476/2022-07, pp. 12–13 [in Serbian]*



The Serbian Commissioner

The healthcare institution installed a facial recognition device in the lobby of the administrative building for the purpose of controlling, recording, and calculating employees' working hours. The controller entered into a service package agreement with the manufacturer and supplier of the facial recognition device, who also acted as a data processor. However, their mutual relationship was not adequately regulated. Upon entry and exit from the building, employees were required to stand in front of the scanning and automatic recognition device based on stored digital photographs. The collected data were transmitted to the data processor's server, where they were further processed, and the processed data on working hours records for each employee were subsequently provided to the controller.

After conducting an inspection, the Commissioner prohibited the controller from further processing employees' biometric data, as it was conducted without a legal basis, contrary to the principle of data minimization, without a prior impact assessment, and without the Commissioner's opinion. The controller was also instructed to delete all personal data of employees that were collected for further processing through the facial recognition device and to inform all employees about the deletion of this data.¹

¹ *Protection of personal data: Positions, opinions and practice of the Commissioner, publication no. 8, Belgrade, 2023. Case number: 072-21-1091/2022-07, pp. 14–15 [in Serbian]*



The Serbian Commissioner

The controller, a clinical hospital centre, established an internal commission for monitoring and preventing sick leave abuse, whereby it independently determined the method of processing employee health data, contrary to the provisions of the Law and the collective agreement. Specifically, the principles of legality, fairness, and transparency were violated, as well as provisions regarding the permissibility of processing special categories of data (Article 17 of the PDPL). In the course of the inspection, it was determined that the controller did not conduct a data protection impact assessment in the legally prescribed manner before commencing processing, including the duty to seek the opinion of the data protection officer.¹

¹ *Protection of personal data: Positions, opinions and practice of the Commissioner, publication no. 6, Belgrade, 2021. Case number: 072-21-2001/2020-07, pp. 150–152 [in Serbian]*



10. Responsibility and compliance

10.1. Key obligations

Following the GDPR as a model, the Serbian Law provides a system of responsibility for personal data protection by establishing rules and obligations for entities involved in the data processing activities. As both the controller and processor play fundamental roles in personal data processing, their responsibilities are particularly regulated. The controller, in accordance with its predominant role, holds a broader spectrum of legal obligations, while the processor is also required to fulfil a range of obligations stipulated by the Law.

Overview of key responsibilities of the controller and processor:

Duties and responsibilities	Controller	Processor	Note
Compliance with processing principles	YES	NO	Processors are required to comply with the principles of integrity and confidentiality.
Determining legal basis in accordance with the principle of lawfulness	YES	NO	
Implementation of appropriate technical, organizational, and personnel security measures	YES	YES	
Maintaining a record of processing activities	YES	YES	Unless the organization is exempted.
Conducting Data Protection Impact Assessment	YES	NO	If the legal obligation to conduct an impact assessment apply, processors are required to assist the controller in the process.
Ensuring privacy by design and by default	YES	NO	Processors are required to assist the controller in the implementation process.
Incident response duty	YES	YES	Processors have a duty to report incidents only to controllers.

Duties and responsibilities	Controller	Processor	Note
Duties related to the transfer of personal data to other countries	YES	YES	If data transfer to other countries is taking place.
Appointment of a representative	YES	YES	If the legal obligation apply.
Appointment of a Data Protection Officer	YES	YES	If the legal obligation apply.
Ensuring the exercise of citizens' rights	YES	NO	Processors are required to assist the controller in ensuring citizens' rights are exercised.

While both the controller and the processor are obligated to process personal data in line with the processing principles, this duty primarily represents a burden for the controller due to the circumstances that only the controller is required to demonstrate compliance with the processing principles. This doesn't imply that the processor is exempt from adhering to the principles; however, since it is not required to demonstrate compliance, its duty is to adhere to the controller's instructions regarding the implementation of the principles, with particular focus on integrity and confidentiality. On the other hand, the determination of the relevant legal basis by selecting one of the six available legal bases in accordance with the principle of lawfulness is an exclusive obligation of the controller, as it defines the purpose of the processing. Additionally, concerning individuals' rights, the controller bears the primary obligation to enable their exercise, while the processor is obligated to assist in these processes.

Implementing adequate technical, organizational, and personnel security measures to comply with the legal framework for personal data protection is the responsibility of all parties involved in the processing activities. Nonetheless, specific duties will depend on the role each party holds in relation to the specific processing activity and the way rights and obligations are established between them. While some duties are clearly regulated by the Law, others depend on the processing circumstances and established contractual relationships.

For this purpose, among other things, the controller and processor are required to prepare documentation and adopt and implement internal policies and guidelines that will determine how personal data is handled within the organization. Depending on the circumstances, this documentation may include mapping of data processing, records of processing activities, data protection impact assessments, and so on. Technical measures primarily involve establishing a processing system in line with the principles of privacy by design and by default and then implementing specific technical measures such as pseudonymisation and data encryption, using and regularly changing access codes to data storage, and similar practices. As an organizational measure within the organization, a role and privilege division

system can be established to specify that only certain individuals have access to specific data, and training and education for employees regarding personal data processing can be organized. To achieve a high level of compliance, continuous monitoring of existing measures and, when necessary, updating or establishing more effective measures is necessary.

In certain situations, the controller has the obligation to notify the Commissioner of a personal data breach, as well as the affected individual, while the processor has the obligation to notify only the controller. Other obligations of the controller and processor related to data processing may include the obligation to appoint a data protection officer, appoint a representative, adhere to rules on data transfers to other countries, and other obligations that will be discussed further below.

Trusted resources

The SHARE Foundation has prepared a self-assessment tool to help you align with the legal framework for personal data protection. Answer a series of questions about the processing of personal data, and you will receive an action plan with specific steps your organization should take.¹



¹ Self-assessment tool [in Serbian]

10.1.1. Joint controller agreement

Relevant provisions: *GDPR* – Article 26, Recitals 79 and 81; *PDPL* – Article 43.

In situations where processing is carried out by joint controllers, the question arises regarding their responsibilities in relation to data processing. Considering the different modalities in which joint controllership can be established, their mutual relationship may vary. It can range from being symmetric, where they equally influence the processing operation and thus share the responsibility for compliance evenly, to having different levels of involvement in the processing, resulting in different allocation of duties, with one party assuming more significant obligations than the other.

Each joint controller individually has a duty to ensure that there is an appropriate legal basis for processing,⁶⁰ and that data is processed solely in accordance with the pre-defined purpose of processing. The mutual responsibilities concerning the processing of personal data by joint controllers are regulated through the

⁶⁰ The necessity of the existence of a legal basis for each joint controller was also confirmed by the Slovenian supervisor in their advisory opinion, https://gdprhub.eu/index.php?title=IP_-_07121-1/2020/2281.

conclusion of an agreement that clearly and transparently establishes the distribution of such responsibilities. Failure to conclude this agreement is a direct basis for accountability, in accordance with PDPL which regulates this obligation, as well as the minimum content of the agreement.

Key issues that must be addressed by the agreement include the purpose of processing, circumstances related to the obligation to inform, and the manner of exercising the rights of individuals whose data is processed. This includes whether individuals can exercise all rights with all joint controllers or if certain rights can only be exercised with one of them. Additionally, the agreement can address responsibilities such as the implementation of appropriate technical, organizational, and personnel measures, notifying obligations in case of personal data breaches, engagement of processors, and others.

For example, joint controllers can agree that only one of them informs the data subjects about the processing details, such as by posting a privacy policy with necessary explanations on the website of one of the controllers. This way, it will not be necessary for all joint controllers to do so separately. Additionally, joint controllers can decide through the agreement that only one of them is responsible for notifying the Commissioner or the data subjects in case of a personal data breach.

The essence of the agreement between joint controllers must be made available to the data subjects, and it must designate a contact person so that citizens know which specific controller to address regarding the exercise of their rights. It is crucial that this information is clear and precise, as any ambiguity in this regard may lead to a violation of the principle of transparency. It's important to note that PDPL explicitly stipulates that regardless of the provisions of the agreement, the data subject can individually exercise their rights established by the Law against each of the joint controllers.

The Serbian Commissioner

In the course of an inspection, the Commissioner found that joint controllers were collecting photocopies of medical records and processing health-related data in violation of the Law. Namely, a daily newspaper initiated a campaign in collaboration with a general hospital to provide free specialist examinations and surgical procedures. Personal data, including copies of their medical records, were requested from readers who applied for the campaign. Such processing violated the principles of lawfulness and transparency, as well as provisions that prescribe conditions for processing special categories of personal data. The joint controllers also failed to transparently regulate their mutual relationship through an agreement in terms of responsibilities for complying with obligations prescribed by PDPL.¹

¹ *Protection of personal data: Positions, opinions and practice of the Commissioner, publication no. 6, Belgrade, 2021. Case number: 072-21-244/2020-07, pp. 71–74 [in Serbian]*



Practice

Considering a request for access to surveillance camera footage, the Danish supervisor determined that the Danish Football Association and the Danish League had violated the principles of lawfulness, fairness, and transparency given that they provided different contradictory information regarding the responsibility for processing and exercising rights. The supervisory authority issued a reprimand in this regard.¹



¹ GDPR Hub, *Datatilsynet (Denmark) - 2020-832-0028*

Although the Law does not prescribe a specific legal form for the agreement, it is recommended that it be concluded in writing to ensure greater transparency and accountability of the joint controllers. Regardless of the content of the agreement, the data subject can exercise their rights individually against each joint controller, while the Commissioner, when deciding on a request related to the processing by joint controllers, is not bound by the provisions of the agreement between them.

It should be noted that, in accordance with the discussion from the third chapter, being qualified as joint controllers is not conditioned by the existence of an agreement. Thus, in practice, supervisors can determine within their oversight that two or more entities are joint controllers, even if they didn't plan it and therefore haven't concluded an agreement, or have regulated their relationship in some other way, such as a data processing agreement between the controller and processor. In these situations, it is expected that the supervisor would order the conclusion of such an agreement.

Practice

The Slovenian supervisor found that the controller-processor arrangement established between the company and the cloud computing service provider, did not adequately reflect the relationship of the actors, given that both parties were making decisions regarding the purposes and means of processing. Through its investigation, the Slovenian DPA established that, in the essence of the specific cloud computing business model, the controller managed complex technical aspects of processing in order to allow clients to fully focus on the content of processed data. Since clients either had no, or very limited influence over the technical and organizational measures used by the cloud computing service provider, the supervisor took the stance that a joint controllership relationship existed and ordered the cloud computing service provider to conclude a joint controllership agreement with the clients.¹



¹ GDPR Hub, IP (Slovenia) – 0612-23/2019/19.

According to the provisions of the PDPL, the liability of joint controllers towards third parties is joint and several, and each controller is liable for the entire amount of damage compensation.

10.1.2. Controller and processor relationship

Relevant provisions: *GDPR* – Article 28, Recitals 78-79, 81 *PDPL* – Article 45.

The law stipulates that in a situation where processing is carried out by a processor, the controller can only engage a processor that guarantees the application of appropriate technical, organizational, and personnel measures in a manner that ensures that the processing is in accordance with the law and protects the rights of the data subjects. In practice, this means that the controller must make efforts to assess whether the processor they intend to engage truly meets the necessary conditions. If the processor wishes to engage a third party (sub-processor) for data processing entrusted to them by the controller, the processor can do so only if the controller agrees. The logic behind this solution is clear – all entities in the data processing chain must ensure the confidentiality and integrity of data. The legislator's intention is to ensure the same level of data security as when, in addition to the controller, one or more processors or sub-processors are processing the data. Considering that the controller determines whether and which processors to engage, the data subject should not be at a disadvantage if their data is entrusted to a processor or sub-processor that does not meet appropriate technical and organizational measures.

The law mandates the controller and the processor to conclude a data processing agreement in writing, which would regulate their relationship regarding the processing of personal data. In the case where the processor engages a sub-processor and entrusts the controller's data to them, it is also necessary for a data processing agreement to be signed between the processor and the sub-processor, which would ensure the same obligations as those stipulated in the processing agreement between the processor and the controller. The processor is responsible to the controller for any damage caused by the sub-processor.

The Serbian Commissioner

The Commissioner issued a warning to a business entity that processes personal data through video surveillance in its retail premises, due to entrusting this processing to a processor without a contract or other legally binding written agreement, among other reasons.¹ During the inspection, it was determined that the processor had carried out the installation of cameras and other equipment for the video surveillance system; was not an employee of the controller; was not in a contractual relationship with the controller; had access to stored footage from the video surveillance system, as well as access to the DVR device and application.

¹ *Protection of personal data: Positions, opinions and practice of the Commissioner, publication no. 7, Belgrade, 2022. Case number: 072-04-1580/2021-07, pp. 12-21 [in Serbian]*



The mandatory elements of a data processing agreement are prescribed by the law, and the data processing agreement needs to specify that the processor is obligated, among other things, to:

- Process data solely based on written instructions from the controller;
- take appropriate technical and organizational measures necessary to ensure the integrity of the processed personal data;
- after completing the agreed processing activities, and based on the controller's decision, either delete or return all personal data and delete all copies of this data, unless there is a legal obligation to retain the data;
- make all necessary information available to the controller to demonstrate the fulfilment of the processor's obligations.

Additionally, some of the mandatory elements of the data processing agreement include the subject and duration of the processing, the nature and purpose of the processing, the types of personal data and categories of data subjects, as well as the rights and obligations of the controller.

Trusted resources

The German regional supervisor for the Baden-Württemberg area has prepared a template for a comprehensive data processing agreement between a controller and a processor in English.¹

¹ Article 28 (3) General Data Protection Regulation (GDPR) Controller Processor Agreement



Practice

The Italian supervisor issued a EUR 30,000 fine against *Verizon Connect Italy S.p.A.*, a company providing geolocation services, for failing to conclude a data processing agreement with its controller, *Giessegi Industria Mobili*, in accordance with the GDPR.¹ Verizon provided geolocation services to Giessegi by installing geolocation devices on its vehicles and allowing Giessegi to track the whereabouts of its vehicles. An employee of Giessegi, who was unaware of this business relationship, filed a complaint against Verizon when they discovered a geolocation device on a vehicle used for deliveries, as their employer had not informed them about the existence of this device.

¹ GDPR Hub, Garante per la protezione dei dati personali (Italy) - no. 9856694



During the inspection, Verizon claimed to be merely a processor and asserted that it had no control over the data, and that Giessegi was the controller. However, the Italian DPA determined that no data processing agreement had been concluded between these two companies, and therefore, Verizon was subject to the same

obligations as a controller, including the obligation to adhere to data processing principles and the requirement to establish a legal basis for processing. The Italian supervisor concluded that Verizon had violated the obligation to adhere to data processing principles, lacked a legal basis for processing, and had not concluded a data processing agreement between the controller and the processor, leading to the monetary fine.

The controller is liable for the harm suffered by the data subject due to unlawful data processing, but the processor also holds responsibility if the processing is conducted outside of legal and contractual provisions, or if the processor acts contrary to lawful instructions provided by the controller regarding processing.

According to the provisions of the PDPL, in cases where processing is carried out by multiple controllers or processors, or jointly by a controller and a processor, each controller or processor is liable for the entire amount of damage. If one of the controllers or processors has paid the full amount of damages, they have the right to claim reimbursement of a portion of the compensation amount corresponding to their liability for the occurrence of the damage.

Practice

The Spanish DPA imposed a fine of EUR 100,000 against a processor who failed to delete and return personal data that it processed to the controller, as well as their copies, after the termination of the relationship with the controller. In this case, EHR, a tourist and hospitality services company, hired the IT software company Signalia as a processor to manage data and servers on behalf of the controller. The processing agreement between the controller and the processor stipulated that Signalia must return all data and data copies to EHR after the business relationship ends. Following the controller's decision to stop using the processor's server and requesting the return of data, the processor failed to comply. As a result, the controller filed a complaint with the Spanish DPA. The controller suffered significant damage as they were unable to access the servers, leading to a monetary fine of EUR 100,000 imposed against the processor.¹

¹ GDPR Hub, AEPD (Spain) – PS/00315/2020



Dilemma

Responsibility for complying with the legal framework for personal data protection primarily rests with the controller. However, in a case from 2021, the Croatian supervisory authority decided to fine only the processor.¹ In this instance, a breach of individuals' rights occurred due to the actions of an employee of the processor

¹ GDPR Hub, AZOP - Decision of 22 February 2021



who recorded a video surveillance screen with a mobile device, shared the recording with a third party, and subsequently the recording spread to social media and the press. The processor did not inform the controller about the security incident and the breach of personal data; the controller was informed by the individuals whose leaked personal data was involved.

As this is a unique decision where the responsibility of the processor was established without determining the responsibility of the controller, it remains to be seen whether this approach will become a rule or if it is an exception that diligent controllers cannot rely on..

The Serbian Commissioner

A data subject filed a complaint with the Commissioner against a healthcare facility acting as a controller, for violating the right to erasure of personal data from the medical records. Specifically, the note in question read: “The patient complained, was rude and unpleasant, shouted in the office.” The complainant stated, among other things, that despite the controller issuing a decision in response to their request, the requested data had not been deleted by the time of filing the complaint. The controller explained that the doctor was unable to delete the note from the complainant's electronic medical records as only the processor was capable to delete it – a company engaged for maintaining the medical information system.

The Commissioner held that the controller is responsible for processing actions regarding personal data, including data erasure, and that the processor is obligated to act based on the controller's instructions and assist the controller in ensuring the rights of the data subjects. Therefore, the Commissioner ordered the healthcare facility to delete the requested data within eight days.¹

¹ *Protection of personal data: Positions, opinions and practice of the Commissioner, publication no. 7, Belgrade, 2022. Case number: 072-16-1584/2021-6, pp.93-97 [in Serbian]*



10.2. Documentation

Relevant provisions: *GDPR* – Articles 24 and 28; *PDPL* – Articles 42 and 45.

To comply with the law, primarily the controller but also the processor are obliged to prepare documentation and adopt and implement internal policies and guidelines that determine how personal data is handled within the organization. The documentation may consist of process mapping, records of processing activities, assessments of the impact of processing on personal data protection, privacy policies, certification confirmations, and other documents depending on the processing circumstances. While the legal framework doesn't explicitly impose the obligation to create these documents, it should be noted that the preparation

of certain documentation is a duty for some controllers in line with the principle of accountability. Depending on the purpose and content of such documents, they can be publicly available (for example, privacy policies published on a website), but they can also be created in the form of internal policies, aiming to regulate internal procedures and processes (for example, a policy for handling personal data). This doesn't mean that all companies will have the same obligations regarding the internal documents. A small company, which processes a limited amount of personal data, is very likely not to have the need to adopt such policies.

Trusted resources

The Greek supervisory authority, in collaboration with partners, has developed an online tool that facilitates GDPR compliance for small and medium-sized enterprises. Upon answering ten simple questions about their organization, business, and personal data processing practices, users receive a package containing templates of recommended documents, along with instructions for filling them out and adapting them to their context.¹



¹ Online Toolkit of the by Design project.

10.2.1. Mapping processing activities

In the process of aligning business practices with the law, it is logical for an organization that processes personal data to start with the mapping of processing activities. Mapping involves identifying processing activities and personal data that the organization processes, with the aim of establishing a comprehensive overview of processing, enabling the initiation of the compliance process with the legal framework for personal data protection. It is quite common, especially within large organizations, for personal data being processed to be scattered across different technical infrastructures and various databases, managed by different departments. As a result, such data is often managed inadequately, and data is processed in a manner not in accordance with the law. It is not uncommon for organizations to possess a significant amount of personal data that is objectively no longer needed, and data mapping will help identify and delete such data.

Mapping the processing activities allows the identification and separation of each processing activity, assigning it a specific purpose, and enabling the implementation of processing logic based on principles. On a technical level, mapping assists in structuring databases and determining processing means, identifying data sources, and defining the flow of data within the organization. This includes determining which employees within the organization have access to the data and why, whether data is transferred outside the organization and shared with third parties, whether it is exported out of the country, and similar considerations. Through the mapping of processing activities, both the controller and the processor will be able to identify deficiencies and take adequate measures to eliminate or reduce such deficiencies and risks.

In practical terms, mapping can be conducted, for example, by identifying different databases that are processed, individual processing activities, as well as the flow of data within the organization. Mapping can be carried out, for example, based on categories of individuals whose data is processed (employee database, customer database, job applicant database, user database, etc.). For each database, individual processing activities and associated circumstances can be mapped out (where data is stored, how long it is retained, who within and outside the organization is responsible for processing, whether data is shared and with whom, which categories of data are processed within the database in each processing activity, etc.). The legal content of the controller's record-keeping could potentially serve as a foundation for the data mapping process. In practice, mapping can be performed using tools like Excel spreadsheets or specialized software.

Although not a legal obligation, mapping the processing activities is of exceptional importance in organizations that base their operations on data processing. Mapping serves to strategically overview all processing activities within an organization and enables the optimization of personal data processing by reducing the number of processing activities, the volume of processed data, the number of locations where data is processed, the number of external and internal parties involved in the processing activity, and similar aspects.

10.2.2. Records of processing activities

Relevant provisions: *GDPR* – Article 30, Recital 82; *PDPL* – Article 47.

The legal framework for personal data protection mandates maintaining records of processing activities for both controllers and processors, with controllers being required to record a greater number of different processing-related circumstances. Records are kept in written and/or electronic form and are stored permanently. The Commissioner has the authority to request access to records of processing activities, and this is usually the first step taken during an inspection. Records of processing activities often stem from the mapping of data processing activities.

In order not to impose excessive obligations on small or beginning business owners, organizations with fewer than 250 employees are exempted from the duty to establish records of processing. However, this exemption cannot be relied upon in cases where:

- The processing could result in a high risk to the rights and freedoms of data subjects;
- the processing is not occasional;
- the processing involves special categories of personal data or data relating to criminal convictions and offenses and security measures.

Regardless of the fact that the exemption from this obligation is broadly defined, it is good practice for controllers and processors to maintain records

of data processing even when not required to do so. These records enable them to better understand the processing activities and the personal data being processed, identify poor processing practices and potential illegal activities, and take necessary measures to align their processing with the legal framework. Additionally, records of processing activities are very useful for controllers as a means to demonstrate their compliance with the law, in line with the principle of accountability.

The Serbian Commissioner

The fact that a business entity has fewer than 250 employees is not the sole condition to be met for exemption from the obligation to maintain records; additional conditions related to the assessed risk to the rights and freedoms of individuals, the frequency of processing, and the type of personal data processed in business operations must also be fulfilled. According to the Commissioner's opinion, this specifically means that even in the case of a business entity with fewer than 250 employees but engaged in regular processing of personal data of externally engaged individuals (i.e., not occasional processing), such company would not be exempt from the obligation to maintain records of processing.¹

The same rule would apply if a smaller company, for example, processes data about health status, political opinions, religious beliefs, or any other special category of personal data; in such cases, the exemption from the obligation to maintain records of processing would not apply. The Commissioner emphasized that records of processing activities are a valuable tool that should also be used for assessing the impact of any personal data processing within a specific organization. It is also a significant means by which controllers and processors can demonstrate their compliance with data protection regulations, including to the Commissioner, in the event of proceedings before this authority. Additionally, maintaining these records contributes to fulfilling the principle of accountability, and it is certainly beneficial for organizations to possess such records.

¹ *Protection of personal data: Positions, opinions and practice of the Commissioner, publication no. 6, Belgrade, 2021. Case number: 073-14-1459/2019-02, pp. 64-65 [in Serbian]*



10.2.2.1. Controller's records

The PDPL comprehensively lists the information that must be included in the record of processing activities for which the controller or their representative is responsible. Such record must include information about the controller's name and contact details, joint controllers if applicable, the controller's representative if designated, the purpose of processing, the type (category) of personal data processed within a specific database, data transfers outside Serbia to other countries or international organizations, data retention periods,

descriptions of technical and organizational measures taken to ensure data confidentiality and integrity, as well as other relevant information.

10.2.2.2. Processor's records

The record of processing activities maintained by the processor contains much less information than the controller's record. The PDPL stipulates that the processor's record must include information about the name and contact details of each processor and each controller on whose behalf the processing is carried out, or the representative of the controller or processor, and the data protection officer if appointed, the types of processing carried out on behalf of each controller, transfers of personal data to other countries or international organizations, as well as a general description of the implemented technical and organizational measures aimed at preserving the confidentiality and integrity of data.

10.2.3. Policies and templates

Although PDPL does not impose a specific obligation on controllers or processors to implement certain internal procedures related to the processing of personal data, it is sometimes very useful to adopt and implement procedures that facilitate data management within the organization. The existence of such internal procedures and policies can help the organization handle personal data lawfully and reduce the risks of potential fines and negative consequences.

For example, an organization can adopt a **Personal Data Internal Policy**, which would be mandatory for all employees within the organization. This document would clarify how employees should handle personal data, what protection measures apply, whether data is shared and under what conditions, which departments within the organization have access to data and why, etc. Such internal policy, along with appropriate training, can simultaneously educate employees and prevent certain unlawful actions with data that could expose the organization to the risk of potential penalties.

Organizations can also adopt a **Personal Data Breach Procedure** for specific security incidents that compromise data. This procedure would make it easier to locate the data and breach and promptly inform the Commissioner and the individuals whose data has been compromised if the obligation to notify exists under the law. This procedure could also include suggestions for possible measures to mitigate the consequences of the breach.

Regarding non-internal forms, a controller may decide to make available a **request form** that data subjects can use to exercise their legal rights. Additionally, a controller can publish a **privacy policy** as a separate document on their website, thereby fulfilling the obligation to inform data subjects, as the privacy policy will provide them with information about all aspects of processing in accordance with the law.

10.3. Data Protection Impact Assessment

Relevant provisions: *GDPR* – Articles 35-36, Recitals 78, 83-84, 89-95; *PDPL* – Articles 54-55.

The legal framework for personal data protection prescribes the obligation of the controller to carry out a Data Protection Impact Assessment (DPIA) in certain situations. The goal of this process is to assist controllers in identifying and mitigating the risks associated with the processing of personal data, particularly concerning the rights and freedoms of the data subjects.

The law requires that the controller, before commencing processing, conducts a DPIA if it is likely that a certain type of processing, especially using new technologies and considering the nature, scope, context, and purposes of the processing, would result in a high risk to the rights and freedoms of natural persons. The law also provides for the possibility of a joint impact assessment, but only if multiple similar processing operations could cause similar high risks to personal data protection.

The law defines specific situations where conducting a DPIA is necessary:

- Systematic and comprehensive assessment of status and personal features of individuals carried out through automated processing of personal data, including profiling, which leads to decisions of significant legal impact or significantly affects the individual in a similar manner.
- Processing of special categories of personal data or personal data relating to criminal convictions and offenses on a large scale.
- Systematic monitoring of publicly accessible areas on a large scale.

Guidelines

The European Data Protection Board has issued Guidelines on Data Protection Impact Assessment and determining whether the processing is likely to result in high risks.¹ The Guidelines emphasize that DPIA is an essential accountability tool, as it helps controllers not only comply with GDPR requirements but also demonstrate that appropriate measures have been taken to ensure compliance.

The Guidelines also aim to promote the development and harmonization of:

- Common lists of processing operations for which DPIA is mandatory;
- common lists of processing operations for which DPIA is not mandatory;
- common criteria for the methodology of conducting DPIA; and
- common criteria for determining when to consult the supervisory authority.

The Guidelines provide concrete examples of processing and relevant criteria for determining whether conducting an impact assessment is mandatory.

¹ Guidelines on Data Protection Impact Assessment (DPIA) (wp248rev.01)



Examples of processing	Possible relevant criteria	DPIA likely to be required?
A hospital processing its patients' genetic and health data (hospital information system)	<ul style="list-style-type: none"> - Sensitive data or data of a highly personal nature. - Sensitive data or data of a highly personal nature. - Data processed on a large-scale. 	YES
The use of a camera system to monitor driving behaviour on highways. The controller envisages to use an intelligent video analysis system to single out cars and automatically recognize license plates.	<ul style="list-style-type: none"> - Systematic monitoring. - Innovative use or applying technological or organisational solutions. 	
A company systematically monitoring its employees' activities, including the monitoring of the employees' work station, internet activity, etc.	<ul style="list-style-type: none"> - Systematic monitoring. - Data concerning vulnerable data subjects. 	
The gathering of public social media data for generating profiles.	<ul style="list-style-type: none"> - Evaluation or scoring. - Data processed on a large scale. - Matching or combining of datasets. - Sensitive data or data of a highly personal nature. 	
An institution creating a national level credit rating or fraud database.	<ul style="list-style-type: none"> - Evaluation or scoring. - Automated decision making with legal or similar significant effect. - Prevents data subject from exercising a right or using a service or a contract. - Sensitive data or data of a highly personal nature. 	
Storage for archiving purpose of pseudonymised personal sensitive data concerning vulnerable data subjects of research projects or clinical trials	<ul style="list-style-type: none"> - Sensitive data. - Data concerning vulnerable data subjects. - Prevents data subjects from exercising a right or using a service or a contract. 	

<p>A processing of “personal data from patients or clients by an individual physician, other health care professional or lawyer” (Recital 91).</p>	<ul style="list-style-type: none"> - Sensitive data or data of a highly personal nature. - Data concerning vulnerable data subjects. 	<p>NO</p>
<p>An online magazine using a mailing list to send a generic daily digest to its subscribers.</p>	<ul style="list-style-type: none"> - Data processed on a large scale. 	
<p>An e-commerce website displaying adverts for vintage car parts involving limited profiling based on items viewed or purchased on its own website</p>	<ul style="list-style-type: none"> - Evaluation or scoring. 	

The Guidelines also provide instructions for conducting an impact assessment, outlining the general process to be used as a framework.

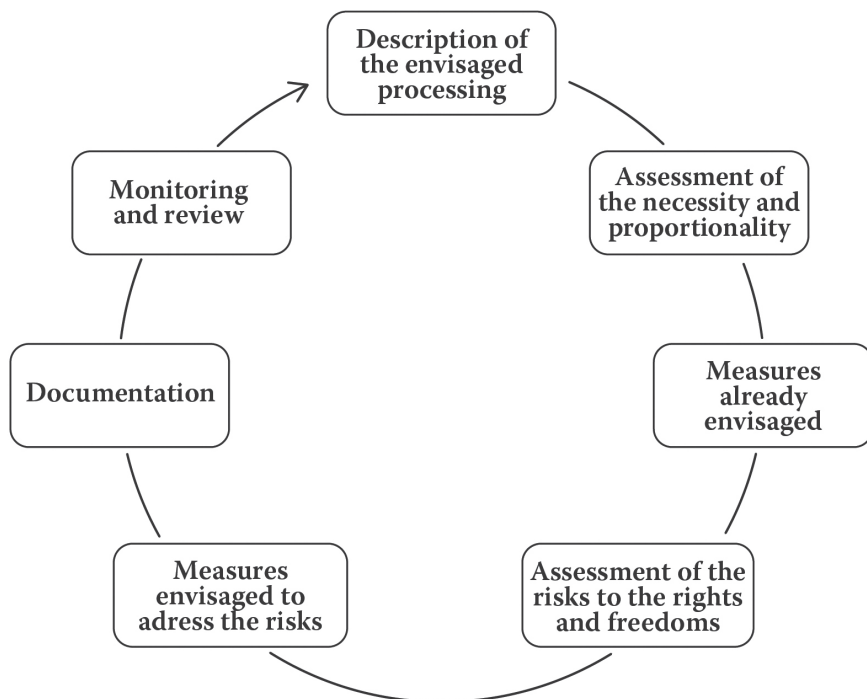


Figure 4: Data Protection Impact Assessment Process

Trusted resources

The Spanish supervisor has prepared an online tool that supports the implementation of the risk analysis of personal data processing, as well as, when necessary, the assessment of the impact on the protection of personal data. This tool generates a report that serves as accompanying documentation for risk management implementation and in no way replaces the actions that controllers and processors are required to take.¹



¹ Manage GDPR: Data processing Records and Risk Assessment

The Serbian Commissioner

Along with accompanying instructions, the relevant decision exhaustively lists the types of processing actions for which an impact assessment on personal data protection must be carried out and when the opinion of the Commissioner must be sought.¹

¹ Decision on the list of types of personal data processing operations for which an impact assessment on personal data protection must be carried out and the opinion of the Commissioner for Information of Public Importance and Personal Data Protection must be sought ("Official Gazette of the RS", No. 45/19, 112/ 20) [in Serbian]



An impact assessment is carried out in case of:

- 1) Systematic and comprehensive assessment of the status and features of an individual, carried out using automated processing of personal data, including profiling, based on which decisions of significance for the legal position of the individual are made or that significantly affect the individual in a similar manner.
- 2) Processing of special categories of personal data, that is, data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, as well as processing of genetic data, biometric data for the purpose of uniquely identifying an individual, data concerning health, or data concerning the sex life or sexual orientation of an individual, or data relating to criminal convictions and offenses and security measures, on a large scale.
- 3) Systematic monitoring of publicly accessible areas on a large scale.
- 4) Processing of personal data of children and minors for profiling, automated decision-making, or marketing purposes.
- 5) Use of new technologies or technological solutions for the processing of personal data, or the processing of personal data used for analysing or predicting economic situation, health, personal preferences or interests, reliability, behaviour, location, or movements of individuals.
- 6) Processing of personal data in a manner that involves tracking the location or behaviour of an individual in the case of systemic processing of communication data generated through the use of phones, the internet, or other communication means.

- 7) Processing of biometric data for the purpose of unique identification of employees by the employer and in other cases of processing of personal data of employees by the employer using applications or systems for tracking their work, movement, communication, etc.
- 8) Processing of personal data by cross-referencing, linking, or verifying matching from multiple sources.
- 9) Processing of special categories of personal data for the purpose of profiling or automated decision-making.

After the impact assessment on the protection of personal data has been conducted, the controller is obliged to request the Commissioner's opinion on the assessment before commencing with the processing.

The Commissioner's practice so far has encompassed a solid range of various impact assessments on the protection of personal data for which opinions have been provided, predominantly in the field of workplace monitoring:

- A system for analysing the location and movements of employees, including data on entries, exits (end of work hours), official departures, private departures, official visits, and breaks;¹
- processing of personal data of employees using remote work monitoring software;²
- processing of employees' personal data using an application indicating a mismatch between the employee's IP address and the address held by the controller;³
- processing of personal data of social media users who express interest in a business bank's credit card;⁴
- processing of personal data of employees through silent monitoring options, allowing supervisors to access employees' computers and monitor their work while providing support to end-users;⁵
- processing of employees' personal data using an automated entry/exit control system via cards, as well as identity verification of the cardholder;⁶
- processing of geolocation data of field workers in marketing and sales;⁷
- preventive action of an observational and prospective nature to be conducted in multiple healthcare institutions by a pharmaceutical company.⁸

¹ *Protection of personal data: Positions, opinions and practice of the Commissioner, publication no. 7, Belgrade, 2022. Case number: 073-15-1234/2020-02, pp. 106-110 [in Serbian]*

² *Ibid.* Case number: 073-15-2774/2020-02, pp. 110-115.

³ *Ibid.* Case number: 073-15-1124/2021-02, pp. 115-119.

⁴ *Ibid.* Case number: 073-15-1322/2021-02, pp. 119-123.

⁵ *Ibid.* Case number: 073-15-1261/2021-02, pp. 123-127.

⁶ *Ibid.* Case number: 073-15-1819/2021-02, pp. 127-133.

⁷ *Ibid.* Case number: 073-15-2067/2021-02, pp. 133-137.

⁸ *Ibid.* Case number: 073-15-1957/2021-02, pp. 137-141.



To facilitate controllers in conducting impact assessments on the protection of personal data, the Commissioner has issued guidelines for creating DPIA.¹ These guidelines include explanations of all important questions:

- Who is obligated to conduct an impact assessment?
- When is an impact assessment carried out?
- In which cases is the controller required to perform an impact assessment?
- What are the mandatory components of an impact assessment?
- When is the opinion of the data subject required?
- When is the opinion of the data protection officer required?
- When is the prior opinion of the Commissioner required?
- How does the Commissioner handle requests for prior opinions?
- Should an impact assessment be published, and when?
- What are the penalties for failure to fulfil obligations related to impact assessments?
- How is an impact assessment conducted in the process of preparing legislation?

¹ *Protection of personal data: Positions, opinions and practice of the Commissioner, publication no. 8, Belgrade, 2023, p. 88 [in Serbian]*



The law also states that the impact assessment must minimally include a comprehensive description of the intended processing actions, the purpose of processing, a description of the controller's legitimate interest if applicable, an assessment of the necessity and proportionality of the processing in relation to the purpose of processing, an assessment of the risks to the rights and freedoms of the data subjects, as well as a description of the measures to be taken to avoid risks.

If the impact assessment indicates that the intended processing actions will pose a high risk to the data subjects unless measures are taken to mitigate the risk, the controller is obligated to seek the Commissioner's opinion before commencing with the processing.

Practice

The Finnish supervisor fined a Helsinki taxi service 72,000 EUR for failing to assess the risks and effects of processing personal data before introducing a surveillance camera system that records audio and video footage in their vehicles.¹ In addition to violating several other provisions of the GDPR (failure to comply with the minimization principle, failure to inform individuals about all processing circumstances in accordance with the GDPR, failure to identify roles in processing, especially taxi drivers, etc.), the Helsinki taxi service did not conduct an impact assessment of processing actions on personal data protection, thereby breaching Article 35 of the GDPR.

¹ GDPR Hub, Tietosuojavaltuutetun toimisto - 8393/161/2019



The French supervisor ordered the Ministry of the Interior in France to cease using drones with cameras because, among other reasons, the Ministry had not previously conducted an impact assessment on personal data protection.¹ The drones were used to monitor compliance with quarantine measures imposed during the COVID-19 pandemic. The French supervisor determined that the drone cameras were efficient enough to allow for facial recognition and thereby the identification of individuals being recorded. The Ministry argued that a face-blurring program was implemented several months later, allegedly anonymising the data and exempting it from GDPR. The French supervisor held that the blurring program had been implemented only in recent drone operations and that the pilot's monitor was not blurred. Additionally, access to unblurred footage was possible. In this case, an impact assessment was required as this type of processing could pose significant risks to fundamental rights and freedoms. According to the supervisor, these drones indeed posed such a risk, particularly given the Ministry's ability to ascertain beliefs and opinions of individuals participating in protests, especially since they were unaware of being recorded. An impact assessment is also necessary when implementing new mechanisms, as was the case with the French police's use of drones



¹ GDPR Hub, CNIL - SAN-2021-003

Example

Arguably the most complex and simultaneously most controversial example of conducting an impact assessment in Serbia was a series of assessments carried out by the Ministry of Interior for the purpose of establishing video surveillance with biometric functions in public spaces.¹ By the time this Handbook was written, MOI has produced four versions of impact assessments, the first two of which received a negative opinion from the Commissioner, while the last two were presented to stakeholders in the civil sector during consultations for the development of a new draft law on internal affairs.



¹ SHARE Foundation, *Biometric Surveillance of Public Spaces in Serbia, position paper*, 12. 12. 2022

The initial announcements that the police planned to cover Belgrade with cameras for biometric surveillance, which would have the capability of matching with facial recognition and license plate recognition software, were made by the former Minister of Interior in early 2019. This advanced and insufficiently probed surveillance system was procured from the Chinese company Huawei.

In accordance with the Personal Data Protection Law, the Commissioner for Information of Public Importance and Personal Data Protection requested the Ministry of Interior to conduct an impact assessment of the new surveillance system on citizens' rights.² MOI prepared the first impact assessment in 2019,³ and after it was rejected as unsatisfactory,⁴ MOI presented a new version of the assessment in mid-2020.⁵ However, the second impact assessment also did not meet the requirements stipulated by the law nor by accepted international standards.⁶

After the Draft law was withdrawn from the procedure in 2021⁷ MOI invited interested civil society organizations, as well as experts and academia, to participate in a total of seven consultative meetings from September 2021 to November 2022, discussing technical and legal aspects of processing personal data using the biometric video surveillance system. In a meeting held in May 2022, MOI introduced a new working version of the impact assessment,⁸ to which the SHARE Foundation

² SHARE Foundation, *MOI should suspend the introduction of the smart video surveillance system*, 18. 11. 2019 [in Serbian]



³ MOI, *Assessment of the impact of processing on the protection of personal data using a video surveillance system*, September 2019 [in Serbian]



⁴ The Commissioner's opinion on the act of the Ministry of Internal Affairs - *Assessment of the impact of processing on the protection of personal data using the video surveillance system*, 12. 11. 2019 [in Serbian]



⁵ MOI, *Assessment of the impact of processing on the protection of personal data using modern video-surveillance technologies within the project "Safe Society" in Belgrade*, March 2020 [in Serbian]



⁶ SHARE fondacija, *Kamere bez upotrebne dozvole / Procena uticaja 2.0*, 31. 7. 2020 [in Serbian]



⁷ SHARE Foundation, *Draft withdrawal a step towards moratorium on biometric surveillance*, 23. 9. 2021 [in Serbian]



⁸ MOI, *Assessment of the impact of personal data processing actions using biometric data processing software in the video surveillance system of the Ministry of the Interior on the protection of personal data*, May 2022 [in Serbian]



provided comments.⁹ While MOI considered certain comments from the SHARE Foundation and incorporated them into the new version of the assessment document in November 2022,¹⁰ the fundamental issues related to biometric surveillance were not resolved, as highlighted by the SHARE Foundation in a new round of comments on the working document.¹¹

⁹ SHARE Foundation, *Comments on the draft assessment of the impact of personal data processing using biometric data processing software in the video surveillance system of the Ministry of the Interior on the protection of personal data*, 3. 6. 2022 [in Serbian]



¹⁰ MOI, *Assessment of the impact of personal data processing actions using biometric data processing software in the video-surveillance system of the Ministry of the Interior on the protection of personal data*, November 2022 [in Serbian]



¹¹ SHARE Foundation, *Comments on the Draft Assessment of the Impact of Personal Data Processing Using Biometric Data Processing Software in the Video Surveillance System of the Ministry of the Interior on Personal Data Protection*, 8. 12. 2022 [in Serbian]



The Ministry of Interior put forth a new version of a set of police laws for public debate,¹² which was again withdrawn under public pressure. “Extensive consultations” have been announced for further work on the draft legislation, aimed at “clarifying all uncertainties of the public and ensuring that everyone understands the intention of the law that is of particular importance for the security of all citizens of the Republic of Serbia.”¹³ It is expected that MOI will revise its proposals and soon release a new draft law, along with a new impact assessment.

¹² SHARE Foundation, *Biometrics again in the Draft Law on Internal Affairs*, 8. 12. 2022 [in Serbian]



¹³ SHARE Foundation, *Round two of the battle against mass biometric surveillance*, 9. 1. 2023



10.4. Privacy by Design and by Default

Relevant provisions: *GDPR* – Article 25, Recitals 74-78; *PDPL* – Article 42.

The principles of privacy by design and by default stem from privacy as a fundamental requirement when establishing processing activities, necessitating the implementation of appropriate technical, organizational, and personnel measures both at the moment of selecting processing means and during the processing

itself. These principles also take into account usability and functional aspects: a processing system that is overly complex to use will be abandoned, regardless of how good the technical standards for privacy and security protection are.

Although the principles of privacy by design and by default are similar, there are differences between them. Firstly, “by design” is a broader concept than “by default”, as the focus of the latter principle is on ensuring data minimization and confidentiality. To adequately apply the principle of privacy by design, attention is required in all stages of processing activity development, whereas privacy by default focuses on the end result: Are the settings configured in such a way as to ensure data minimization and confidentiality? However, factory settings can be appropriately set to a default configuration that is most suitable for privacy protection if this issue is considered during the development process. Therefore, the implementation of these principles should have a synergistic effect.

Example

The manufacturer of a smart home device is obliged to incorporate into the system the capability for the user to control the type and quantity of data collected within the confines of their private residence (privacy by design). Furthermore, when the user unpacks the device and installs it for the first time, default settings must be configured in a way that the principles of data minimization and confidentiality are already ensured (privacy by default), and only the consumer can, through their decision, expand the scope and quality of the collected data and with whom it is shared..

A personal data processing system can consist of a set of different software and databases, procedures defined by the organization itself, and practices that emerge in its work, which is precisely the case with many small organizations. For instance, an organization might use Microsoft Office for office tasks, Dropbox for data storage and synchronization, and Slack for collaborative project management. If, within the scope of its operations and use of these services, the organization processes personal data, it is obliged to take into account the principles of privacy by design and by default and to consider whether the established and planned processes adequately protect the rights and freedoms of the data subjects.

Principles of privacy by design and by default require that attention be given to the characteristics of the data processing system at every phase of planning, development, and implementation, in order to simplify the process of compliance and protect the rights and freedoms of citizens. Therefore, an *ex ante* approach is required – before the commencement of processing, the privacy requirements that need to be considered during the design and development of the processing activity must be defined, as well as determining the default settings of the final product. This encourages data controllers to think about the technical, organizational, and personnel measures needed to meet these requirements in the earliest stages of the processing activity development. Those who fail to consider these issues during the planning phase are at risk of developing a processing system that may not

be able to align with the legal framework for personal data protection, or it may require serious and costly adaptation, an expense that is usually not budgeted for. Thus, an organization that complains about excessive costs of compliance with the legal framework for personal data protection likely did not adhere to this principle when it should have.

Guidelines

The GDPR has set a standard for data protection laws to include requirements related to built-in and default privacy. However, these requirements were not new: as early as the mid-1990s, the then-Information and Privacy Commissioner of Ontario, Canada, published seven fundamental principles of fair data processing practice¹ on which the concept of privacy by design is based:

1. **Proactivity instead of reactivity** – entails recognizing and reducing as many risks as possible to prevent most threats from occurring.
2. **Privacy as the default setting** – the system is preconfigured with conservative data values, implementing minimized data processing without additional “optional” processing. If a user chooses to use additional features, they consciously opt for enabling additional processing.
3. **Privacy embedded into design** – involves designing and managing the system in a way that considers the privacy of data subjects within that system. This principle follows the entire processing lifecycle, from its planning to data destruction.
4. **Full functionality** – “positive sum” instead of “zero-sum” implies that privacy implementation does not burden business operations; rather, these measures are implemented to encourage business development rather than hinder it with obligations.
5. **End-to-end security** – personal data protection measures are applied from the beginning to the end of processing, from data input and processing to transfer, storage, and deletion.
6. **Visibility and transparency** – the data processing activity and implemented protection measures are transparently explained to the data subjects.
7. **Respect for individual privacy** – the essence of personal data protection is actually the protection of an individual's privacy, and the entire system is oriented around an individual's right to privacy.²

¹ Privacy by Design: The 7 Foundational Principles

² Cavoukian, A., 2010, Privacy by Design – The 7 Foundational Principles



Dilemmas

Some authors differentiate between data protection by design and privacy by design.¹ These concepts are often used synonymously, although they can differ in practice. Data protection by design implies that technical measures related to processing means (hardware or software) are implemented to ensure minimally invasive processing of personal data. On the other hand, privacy by design is more concerned with the principles of data minimization and the overall amount of data being processed. Thus, these two concepts together serve to protect collected data by preventing excessive processing, but they manifest in different ways.

¹ Sharma, S., 2020, Data Privacy And GDPR Handbook – John Wiley & Sons, str. 85

The concepts of privacy by design and by default today represent an international standard, and although not explicitly mentioned in the Serbian PDPL as they are in the GDPR, the essence of these principles is elaborated in Article 42 of the PDPL, outlining the requirements that should be considered and integrated into the processing activity during establishment and throughout its duration.

Privacy by design requires:

- Minimization of the amount of personal data subject to processing through pseudonymisation; and
- implementation of necessary protection mechanisms during processing to fulfil the conditions for processing prescribed by the Personal Data Protection Law and to protect the rights and freedoms of individuals whose data is processed.

When fulfilling these requirements, the data controller should take into account:

- Current technological advancements;
- costs of implementing technical, organizational, and personnel measures;
- nature, scope, circumstances, and purpose of processing; as well as
- the level and probability of risks to individual rights and freedoms arising from the processing.

Privacy by default requires the processing of only those personal data that are necessary to achieve each specific processing purpose. This requirement pertains to:

- The amount of personal data;
- the scope of processing;
- the retention period; and
- data accessibility.

These requirements apply to the data controller regardless of the size or complexity of their processing operations, both during initiation and throughout the processing duration.

Guidelines

The EDPB guidelines on privacy by design and by default provide a comprehensive and practical framework for organizations to apply these principles in accordance with the GDPR.¹ The practical contribution of the Guidelines lies in providing concrete advice on how to implement the principles of privacy by design and by default during the implementation of the GDPR principles. For illustrative purposes, we will present some advice for one of the GDPR principles.

A specific requirement of the accuracy principle is to take all reasonable steps to ensure that inaccurate personal data are erased or rectified without delay. It is necessary to prevent the processing of inaccurate data, especially when it poses an increased risk to the rights and freedoms of individuals, such as leading to incorrect diagnosis or the application of the wrong medical protocol. For effective implementation of the accuracy principle, the principles of privacy by design and by default, according to the Guidelines, encompass the following elements:

- **Data source** – Sources of personal data should be reliable in terms of data accuracy.
- **Degree of accuracy** – Each personal data element should be as accurate as necessary for the specified purposes.
- **Measurably accurate** – Reduce the number of false positives/negatives, for example biases in automated decisions and artificial intelligence.
- **Verification** – Depending on the nature of the data, in relation to how often it may change, the controller should verify the correctness of personal data with the data subject before and at different stages of the processing (e.g. to age requirements).
- **Erasure/rectification** – The controller shall erase or rectify inaccurate data without delay. The controller shall in particular facilitate this where the data subjects are or were children and later want to remove such personal data.
- **Error propagation avoidance** – Controllers should mitigate the effect of an accumulated error in the processing chain.
- **Access** – Data subjects should be given information about and effective access to personal data in accordance with the GDPR articles 12 to 15 in order to control accuracy and rectify as needed.
- **Continued accuracy** – Personal data should be accurate at all stages of the processing, tests of accuracy should be carried out at critical steps.
- **Up to date** – Personal data shall be updated if necessary for the purpose.
- **Data design** – Use of technological and organisational design features to decrease inaccuracy, for example present concise predetermined choices instead of free text fields.



¹ EDPB, Guidelines 4/2019 on Article 25 Data Protection by Design and by Default

The Guidelines further provide a concrete example of implementing these elements. The data controller is a healthcare institution seeking methods to ensure the integrity and accuracy of personal data of its patients.

1. In situations where two persons arrive at the institution at the same time and receive the same treatment, there is a risk of mistaking them if the only parameter to distinguish them is by name. To ensure accuracy, the controller needs a unique identifier for each person, and therefore more information than just the name of the client.
2. The institution uses several systems containing personal information of clients, and needs to ensure that the information related to the client is correct, accurate and consistent in all the systems. The institution decides to mitigate the risk by using a hashing technique² that can be used to ensure integrity of data in the treatment journal.



² MathWorld, *Hash Function*

Trusted resources

The Spanish supervisor has prepared comprehensive guides on privacy by design¹ and by default² which are freely available in the English language.



¹ A Guide to Privacy by Design



² Guidelines for Data Protection by Default

10.5. Data processing security

Relevant provisions: *GDPR* – Article 32, Recital 49; *PDPL* – Articles 50-51.

Inadequate protection of personal data within an information system can lead to various issues, ranging from financial penalties imposed by domestic and European regulations to impacting the continuity of operations or endangering the security of data subjects. The consequences for the credibility and reputation of an organization that has experienced a security incident are long-term and can result in severe losses.

The legal framework for personal data protection does not specifically prescribe duties related to the technical measures needed to ensure an adequate level of data protection. Article 50 of the Personal Data Protection Law outlines the required level of security to be applied during personal data processing. According to this provision, determining an appropriate level and measures should be based on available technology, the nature, scope, and purpose of processing, as well as risk assessment, i.e., the potential implications an incident could have on human rights. This approach takes into consideration the pace of technological development and the relative relationship between currently appropriate measures and technological advancement over a given period.

There are many factors considered relevant in defining security measures and protocols, including the size of the organization, the type of data collected and processed, the type of employees interacting with the data, and more. However, the most important factor is the risk assessment conducted on a case-by-case basis; there is no general risk that can be attributed to a specific type of data, as the context can vary widely.

Four types of measures emerge from Article 50(1) of the PDPL and Article 32 of the GDPR, and while they may seem broadly stated, they cover all aspects of system security and reliability. These are:

1. the pseudonymisation and encryption of personal data;
2. the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
3. the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
4. a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

10.5.1. Risk Assessment

The first step in selecting appropriate measures to protect data integrity and security without hindering business operations is risk assessment.⁶¹ This practically means identifying all potential threats to security and assessing the likelihood of their occurrence. For instance, if the data server is located in the basement, the data is at risk of flooding – this doesn't necessarily mean that a flood will definitely occur, but it would be reasonable to place servers on elevated supports.

A prerequisite for a good risk assessment is a thorough understanding of the system, the equipment used, hardware and software, as well as the classification of the processed data. In other words, resources need to be mapped out. In the case of equipment, this typically involves listing individual devices and regularly updating the list based on the type and model of the device, the date of acquisition, any license, support, or insurance expiration, the employee using the device or is responsible for its use, and similar factors.

⁶¹ The international standard governing the field of incident management is ISO 31000, Risk management – Guidelines.

Data is classified according to its level of sensitivity or confidentiality, based on which specific protection measures are applied, as well as access procedures. The level of data confidentiality depends on the nature of the business and internal decisions within the organization, while data sensitivity is a criterion prescribed by the law (regarding special categories of data) and must be respected regardless of organizational interests.

Example of Data Classification:

Data type	Protection measures
Public data	Procedures for data integrity protection (technical measures ensuring service availability; e.g., antivirus program, physical equipment security)
Data accessible to employees	Procedures for protecting internal data
Data accessible to the management	
Confidential data	Procedures for protecting confidential and sensitive/special category data
Highly confidential data	
Sensitive/special category data	

Data mapping example:

Data set	Where is it stored?	Who can access?	Level of sensitivity	Protection measures
Confidential information database	Protected file on cloud server	Database owner only	Highly Confidential / Special	Procedure for protecting confidential and special data
Business history database	Web server	Anyone	Public data	Procedure for data integrity protection
Information on company salaries	Payroll journals	Financial manager and director	Confidential Data	Procedure for protecting internal data

Once it is determined what resources are available, where they are located, and how they can be accessed, it is necessary to *identify threats*, or determine what could potentially compromise the information system. The methodological approach is a matter of an internal decision, based on the organisation's own needs and the circumstances in which it operates, but it is important to encompass all parts of the organization, as each of them may be exposed to different threats. It is important to list a broader range of threats, regardless of how likely they are, whether they come from external sources or within the organization, whether they are technically advanced, or the result of natural disasters.

Example of Threat Identification

Threat	What is the threat?
Target	Who is the target of the threat (individual, organizational unit, entire organization)?
Source of threat	Who is behind the threat?
Capacity of the source of threat	Describe the strengths, advantages, and capabilities of the source of threat that would contribute to the realization of the threat.
Prerequisites	What are the prerequisites for the threat to be realized?
Where	What are the physical and/or logical locations where the threat can be realized?
Our Capacity	What procedures and capacities do we have that could prevent the realization of the threat?
Our vulnerabilities	What deficiencies on our part could contribute to the realization of threats?

Once possible threats are identified, their impact on operations needs to be assessed, such as disruption or cessation of work, additional costs, material damage, legal liability, etc.

Finally, a good risk assessment also depends on a reasonable determination of the probability that a threat will be realized. While it's useful to consider all possible threats, it would be futile to spend resources protecting equipment from, say, a sandstorm if the servers are located in a temperate continental climate area.

Combining the impact of the threat and the probability of its realization results in the final risk assessment. At one end of the risk assessment scale, there will be a low probability of realizing a threat that will not significantly affect operations, while at the opposite end, there will be an imminent threat that could jeopardize the entire organization's operations.

Risk assessment thus becomes a priority list that the organization needs to address as soon as possible.

10.5.2. Security measures

Relevant provisions: *GDPR* – Article 25, Recitals 78 and 83; *PDPL* – Article 42.

After data classification and determining privileges and roles have been completed, the next step is to establish security measures. There are technical, organizational, personnel, and physical security measures. This section describes

technical measures. Commonly applied standard technical measures include access control, encryption, pseudonymisation, data anonymisation, and more.

Trusted resources

Specific standards for information security are prescribed, among which is ISO 27001, an international standard for information security. It requires organizations to identify risks to information security and select appropriate control measures for greater protection.¹



¹ ISO/IEC 27001 Information security management systems

10.5.2.1. Access control

An important aspect of data security in the information system is addressed through control of access to various sets of data, accomplished through privilege and role systems. This involves defining different roles in data processing for various groups of employees, business partners, and users. Some data sets may be visible to everyone, while others may only be accessible to specialized partners, and some might only be editable by employees with specific authorizations, and so forth. For instance, IT or sales personnel should not have access to employer-held documents related to legal disputes unless there is an objective reason. Access to dispute-related data should be limited to management, legal, and financial departments.

Roles are defined based on organizational needs and responsibilities, following the principle of least privilege. Each user account is granted access to only a specific part of the system to perform predefined tasks, with the information system automatically recording the time and location of each access. This system involves assigning user accounts and some form of ownership confirmation, such as a password, qualified certificate, or biometric information. Passwords are the most common authentication method and should be complex, not contain user-related data or natural language words. For secure management and storage of passwords, password managers are recommended. Besides storing credentials, they can generate passwords, making passwords even more secure. It is important for password managers to use default encryption. Additionally, as a second level of protection, alongside passwords, it is advisable to employ multi-factor authentication to further safeguard user accounts. Multi-factor authentication⁶² usually requires an additional code to be entered during login. This code can be received via SMS/email, through a physical key/USB, or via an application. When it comes to security, the latter two methods of obtaining the code are recommended.

⁶² PC Press, *Multi-factor authentication (MFA) via smartphones is becoming increasingly insecure*, 20. 3. 2023, <https://pcpress.rs/multifaktorska-autentifikacija-mfa-putem-smartphone-a-postaje-sve-nesigurnija/>. [in Serbian]

Trusted resources

Commonly recommended tools for managing passwords include *Bitwarden*,¹ which is open-source and encrypted, user-friendly, and offers synchronization across various devices. *KeePass* and *KeePassXC* are also recommended².

¹ Bitwarden, Password manager

² KeePass Password Safe



10.5.2.2. Encryption

Encryption or automatic ciphering of content is becoming a standard practice in safeguarding the security of information systems, specifically the data processed within these systems.⁶³ Local disk encryption pertains to physical devices where important data is stored as an additional method of protection, introducing a new level of controlled access. In the event of computer or disk theft, encryption acts as a substantial barrier against unauthorized access to data. There are several encryption options:

1. Full disk encryption, which encrypts the entire disk containing sensitive data to be safeguarded.
2. File-based encryption, where both the document's name and its contents are encrypted, while metadata (such as time of document modification or its size) remains readable.
3. Using encrypted communication channels for data transmission.

It is preferable for services used to provide encryption by default.

Practice

On September 13, 2018, the Regional Court in Würzburg issued a temporary injunction against a lawyer whose privacy policies on their website were not in compliance with GDPR, and whose communication contact form lacked encryption protection. The court, while explaining its decision, emphasized that both deficiencies constituted violations of GDPR provisions, and the lawyer faced a fine of 250,000 EUR if the obligation for compliance was not met.¹

¹ LG Würzburg, Beschluss 11 O 1741/18 UWG, Wettbewerbsrechtlicher Unterlassungsanspruch wegen der Nichteinhaltung der DSGVO



63 Kaspersky, *What is Data Encryption?*, <https://www.kaspersky.com/resource-center/definitions/encryption>.

10.5.2.3. Pseudonymisation, tokenisation, and anonymisation

Relevant provisions: *GDPR* – Articles 4, 25 and 32, Recitals 28 and 29; *PDPL* – Articles 4, 41 and 50.

Throughout the entire processing of personal data, if such data do not need to be stored in their original form, anonymisation, tokenisation, or pseudonymisation is recommended. Anonymisation involves an irreversible separation between data and the identity of the data subject. Pseudonymisation temporarily masks data, which can then be restored to their original form as needed, often with the help of a cipher, while tokenisation replaces personal data with tokens of similar value.

Example

Data	Pseudonymisation	Anonymisation
John Doe	PERSON 1	XXX XXX
John Roe	PERSON 2	XXX XXX
Jane Doe	PERSON 3	XXX XXX
John Doe	PERSON 1	XXX XXX

Option 1: Pseudonymisation

A method for protecting personal data, defined within the legal framework of personal data protection as “processing of personal data in such a way that it is no longer possible to attribute the personal data to a specific natural person without the use of additional information, provided that such additional information are kept separately and subject to technical and organisational measures, ensuring that the personal data are not attributed to an identified or identifiable natural person”. This method involves replacing identifiable data with a constant value, but it is not as effective as encryption, as the data remains in a readable format; it just needs to be located and linked. This means that an individual can still be identified through indirect or additional information used to mask the data.⁶⁴

Option 2: Tokenisation

A practice closely related to pseudonymisation, involving the replacement of personal data with tokens of similar value. Unlike pseudonymisation, tokenisation replaces data with non-sensitive values and maintains the length of the original values. Tokenisation and pseudonymisation are effective methods for protecting data during storage or transmission. However, they have limitations and can be vulnerable to attacks if enough data is decrypted, as the same tokens replace/decrypt the same values. Despite their vulnerability, these encryption methods are preferred under GDPR.

⁶⁴ Netokracija, *How to protect user's personal data by 'pseudonymization' and what this process represents?*, 7. 5. 2018, <https://www.netokracija.rs/pseudonimizacija-podataka-145217>. [in Serbian]

Option 3: Anonymisation

Transforming data by severing the link between information and individuals. If efficiently executed, anonymisation removes data and its processing from the scope of personal data protection, due to the circumstances that no personal data is involved in the processing activity. These methods are useful and highly applicable, especially for research and statistical purposes. Data controllers practically reduce the scope of data processing, carry out anonymisation, and delete unnecessary data to exit the scope of the PDPL and GDPR while still being able to achieve various business purposes of processing. The legal framework does not provide precise instructions regarding anonymisation, so data controllers must contextually analyse data processing activities to determine the suitability of their anonymisation methods.

Trusted resources

As we have witnessed numerous instances over the years of incomplete or improperly conducted anonymisation processes that resulted in the re-identification of individuals, the Spanish supervisory authority has prepared a concise document outlining the ten most common mistakes encountered by data controllers and processors during the anonymisation process.¹ Additionally, the Spanish supervisor has prepared a separate document specifically for data controllers who wish to employ hashing techniques in their personal data processing activities as a pseudonymisation tool.² These documents are freely available in English.

¹ 10 Misunderstandings Related to Anonymisation

² Introduction to the Hash Function as a Personal Data Pseudonymisation Technique



The Serbian Commissioner

When, in response to a request for access to information of public importance, a data controller provided documentation regarding complaints against police officers' conduct, they inadequately anonymised personal data (such as names, addresses, dates of birth, ID numbers). Consequently, personal data of these individuals became accessible to third parties. In doing so, the data controller violated provisions of the Personal Data Protection Law related to the application of appropriate technical, organisational, and personnel measures.

In the course of supervision, it was found that the data controller had merely shaded the personal data in the requested documentation, using a “new black marker pen”, and in one of the documents, an individual's ID number was not even shaded. The data beneath the marker trace remained visible.¹

¹ *Protection of personal data: Positions, opinions and practice of the Commissioner, publication no. 7, Belgrade, 2022. Case number: 072-04-49/2021-07, pp. 59-66 [in Serbian]*



10.5.2.4. Data loss prevention

Creating a backup is crucial when the need arises to recover lost data after a security crisis. Data backups enable the availability, one of the principles of the so-called CIA triad (Confidentiality, Integrity, and Availability). Sometimes, based on a backup, it is possible to determine the cause of a system failure through the reconstruction of security vulnerabilities or system errors, and the like.

Both external and internal storage of backups are recommended. External backup involves storing data copies on dedicated disks within secure vaults that are protected from potential mishaps (fireproof vaults). Internal backup entails storing database copies within the system, on different servers, or on a server specifically designed for this purpose.

D	1	2	3	4	5	6	7	1	2	3	4	5	6	7	1	2	3	4	5	6	7	1	2	3	4	5	6	7
W	1							2							3							4						
M	1																											
Y	...X 12																											

Mark	Description	Retention Period
D	Daily Backup	7 Days
W	Weekly Backup	1 Month
M	Monthly Backup	1 Year
Y	Yearly Backup	Unlimited

Figure 5: Backup copies

Servers should be backed up during the night or outside of working hours. Differential backups (backup of changes) should be performed every night, while full backups should be conducted once every seven days. Daily backups should be retained for one week, while weekly backups should be kept for one month. Monthly backups should be stored for one year.

Certainly, the retention of backup copies should not exceed the established period for retaining personal data. It is implied that these backup copies should be protected from all forms of physical harm. Keep in mind that deleted data may sometimes be irrecoverable. It is advisable to establish procedures for periodic testing of the backup restoration process.

Practice

After hackers gained access to a database containing approximately 165,000 pieces of personal data of Forenom company clients, which was stored on its infrastructure, the Finnish supervisory authority concluded that the data controller had violated the principles of minimization and storage limitation, and had failed to implement appropriate security measures to prevent the breach of personal data.¹ The supervisor held that the data controller should have implemented appropriate technical, organisational, and personnel measures to ensure that only data necessary for the purpose (responding to clients' damage compensation requests) were being processed. In the end, the supervisor stressed that the data controller had not assessed the potential risks associated with data retention, nor had taken adequate measures to prevent these risks, thereby breaching the GDPR.



¹ GDPR Hub, Tietosuojavaltuutetun toimisto (Finland) – 2206/171/20

10.6. Incident response

Relevant provisions: *GDPR* – Articles 33-34, 70, 83-84, Recitals 85-88; *PDPL* – Articles 52-53.

10.6.1. Incident management

The PDPL defines a personal data breach as a breach of the security of personal data that results in accidental or unlawful destruction, loss, alteration, unauthorised disclosure, or access to personal data that have been transmitted, stored, or otherwise processed. More serious breaches of personal data can have various negative consequences for the individuals whose data are compromised – material and non-material harm, loss of control over personal data, discrimination, reputational risk, identity theft, financial losses, various socio-economic consequences, and the like.

Guidelines

The question arises as to whether temporary loss of personal data constitutes a breach of such data. According to the Guidelines on Personal Data Breach Notification by Article 29 Working Party, accepted by the European Data Protection Board, temporary loss of personal data also qualifies as a data breach, since the GDPR mandates the implementation of measures to ensure the ongoing confidentiality, integrity, availability, and resilience of systems and services within which data is processed, as well as the ability to timely access data or restore data in the event of an incident.¹ Consequently, temporary loss is considered a breach of personal data.

¹ EDPB, Guidelines on Personal data breach notification under Regulation 2016/679, WP250 rev.01



In today's age of the internet and businesses heavily reliant on personal data, various breaches of personal data frequently occur, which in specific situations can have adverse consequences for a large number of individuals. Breaches of personal data can result from both external cyber and physical attacks, as well as errors within the organization of the data controller and processor. A breach of personal data may, for example, involve the theft of data by a third party who gains unauthorised access and transfers them to their servers or devices for later misuse toward their own objectives. Similarly, someone might steal data in physical form (for instance, from files in cabinets). However, a breach of personal data can also occur due to a mistake within the organisation itself – accidental data loss, sending data to the wrong person or in an insecure manner leading to their disclosure, loss of physical devices containing stored data (computers, phones, USB drives), accidental data deletion, and the like.

In most cases, the human factor is the reason for personal data breaches, making it the organisation's duty to prevent such incidents. To be prepared to respond appropriately in case of a breach, the organisation needs to make decisions about appropriate technical, organisational, and personnel measures to implement. The goal of these measures is first and foremost to minimise the possibility of breaches, and if a breach occurs, to enable the affected organisation to quickly detect the breach, decide whether to report it to the Commissioner and the individuals whose data is compromised, take steps to mitigate the consequences of the breach if possible, and prevent a recurrence of the breach, depending on the nature of the incident.

An organization looking to reduce the risks of breaches can take the following steps:

- Compile a risk assessment of security incidents to aid incident management, including prevention, reporting assessment, and measures for minimising consequences if an incident occurs.
- Educate employees on data handling practices to prevent incidents like loss, damage, unauthorised disclosure, and similar.

- Establish appropriate procedures and legal policies that enable employees to report incidents they observe adequately.
- Implement a role and access privilege system that controls data access for employees who objectively do not require access.
- Implement suitable technical measures that can significantly mitigate data breach consequences (for example, anonymisation or pseudonymisation).

When a specific employee within the data controller's organization becomes aware of a personal data breach, it is necessary to promptly notify their supervisor or the Data Protection Officer if appointed, or other individuals in accordance with the incident management policy if such a policy has been adopted.

Subsequently, it is essential for the relevant technical or designated personnel to immediately take all measures possible to mitigate the consequences of the breach (e.g., prevent further spread of the attack or data loss) if feasible in the specific case. Simultaneously, the responsible individual should assess all circumstances of the specific breach case, including questions about which data is compromised, which individuals are affected, how the breach occurred, the quantity of compromised data and individuals, as well as the likely risks that may arise as a result of the breach. This assessment aims to decide whether to inform the Commissioner and the individuals whose data has been compromised about the incident.

Trusted resources

In the process of managing information security incidents and personal data breaches, it is advisable to rely on the Guide for Incident Handling in Computer Systems Management.¹ **Phases of the incident response**, as defined by the Guide, include preparation, detection, containment/quarantine, investigation, remediation, and recovery. The dynamic relationship between these phases is emphasized, with each serving its purpose.



¹ NIST, Computer Security Incident Handling Guide (NIST SP 800-61)

- **Preparation** involves activities that enable the organisation to respond to an incident, including policies, tools, procedures, effective management, and communication plans. It is also important for affected groups to establish necessary controls for recovery and resumption of operations after the incident's discovery. Analysis of previous incidents is crucial for continuous improvement in this phase.
- **Detection** refers to identifying an incident through security tools or notifications from internal or external sources about a suspicious incident. This phase also includes initial incident classification and all initial notifications required by law or contract.
- **Containment** is a triage phase involving identifying, isolating, or otherwise mitigating the affected device or system, as well as informing affected parties about the incident. This phase encompasses sub-procedures for evidence seizure and handling, escalation, and incident communication.

- **Investigation** involves competent individuals within or outside the organisation determining the incident's priority, scope, risk, and root cause.²
- **Remediation** occurs post-incident and involves recovering affected systems, providing guidance to affected parties, coordinating, and conducting an analysis to confirm the threat has been addressed. Regulatory requirements and internal and external communications are determined by key stakeholders. Besides all formal reports, incident analysis concludes in this phase, as it can impact remediation and incident interpretation.
- **Recovery** involves analysing the incident and the applicability of existing procedures and policies, collecting metrics, analysing “lessons learned” for future incidents, and improving training.

² The international standard governing the field of digital evidence collection in the event of a cyber incident is ISO/IEC 27037:2012 Information technology – Security techniques – Guidelines for identification, collection, acquisition and preservation of digital evidence.

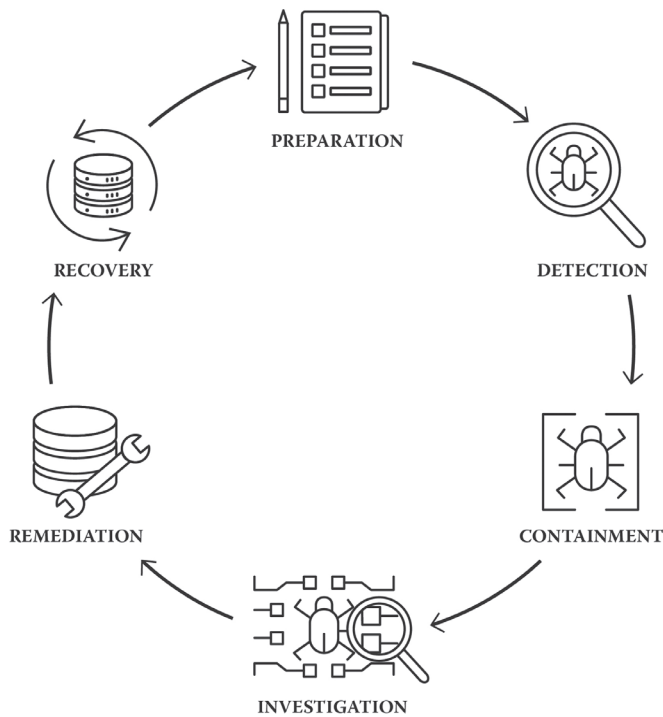


Figure 6: Stages of risk response

If in accordance with legal and other requirements, notification is necessary, the data controller must send such notifications in the prescribed form and within the specified timeframes. Ultimately, the data controller must document the occurred breach and take appropriate measures to prevent or minimise the possibility of similar breaches in the future.

Guidelines

The 2023 EDPB Guidelines on Personal Data Breach Notification provide clarifications on this process within the context of GDPR and offer suggestions for steps that data controllers and processors can take to fulfil their prescribed obligations.¹ The Guidelines also provide examples of various types of personal data breaches and recommendations on who should be notified in different situations.



¹ EDPB, Guidelines 9/2022 on personal data breach notification under GDPR, Version 2.0, 28. 3. 2023.

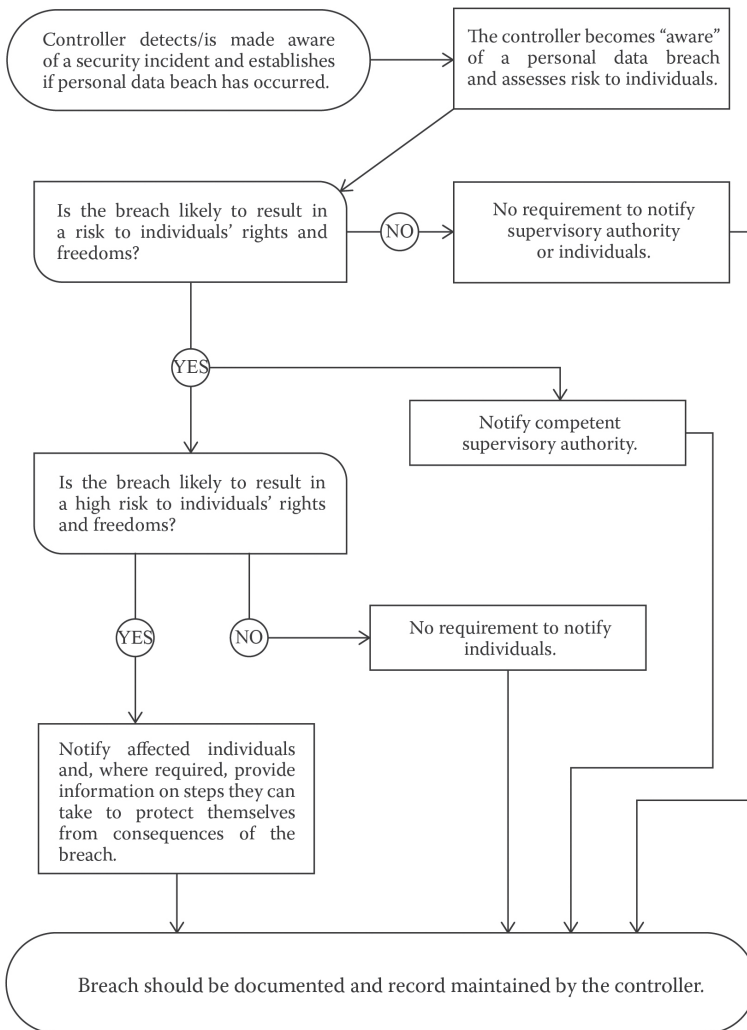


Figure 7: Flowchart showing notification requirements

10.6.2. Incident management policy

In order to assess the existence of a breach, conduct an internal investigation to define all necessary circumstances related to the breach and assess the risks, make decisions about breach notification, and send notifications within legal deadlines, it is highly useful for the data controller to adopt an incident management policy. This policy will regulate all these processes and designate responsible individuals to handle them.

This is especially crucial in large systems that process substantial amounts of personal data, as there are legal deadlines for breach notification. Having unified and clear procedures is necessary to assist the data controller in fulfilling their legal obligations.

Dilemmas

The Serbian Law on Information Security distinguishes the following categories of incidents that operators of ICT systems of special significance are obliged to report:

1. Incidents leading to a disruption of continuity or significant difficulties in performing tasks and providing services.
2. Incidents affecting a large number of service users or lasting for an extended period.
3. Incidents causing a disruption of continuity or difficulties in performing tasks and providing services that impact the operations and services of other operators of ICT systems of special significance or affect public safety.
4. Incidents causing a disruption of continuity or difficulties in performing tasks and providing services that have an impact on a larger part of the territory of the Republic of Serbia.
5. Incidents resulting in unauthorised access to protected data, the disclosure of which may jeopardize the rights and interests of the data subjects.
6. Incidents resulting from an incident in ICT systems of special significance.¹

The reporting procedure for these incidents is specifically regulated by information security laws and does not affect the obligations of the data controller in accordance with the legal framework for personal data protection. Therefore, in the event of an incident, an organization does not need to be burdened with understanding at least two different incident management frameworks. Through a previously prepared incident management policy that consolidates all relevant processes, the organization can focus on crisis response in accordance with the unified process.

¹ Law on Information Security ("Official Gazette of RS", no. 6/16, 94/17 and 77/19) [in Serbian]



10.6.3. Notifying the Commissioner

Relevant provisions: *GDPR* – Article 33, Recital 87; *PDPL* – Article 52.

The data controller is obliged to notify the Commissioner if they assess that a personal data breach may pose a risk to the rights and freedoms of individuals. The Commissioner must be informed without undue delay, or, if possible, within 72 hours of becoming aware of the breach. If the Commissioner is not informed within this timeframe, the data controller is required to provide reasons for the delay.

If a data breach occurs concerning personal data entrusted for processing to a data processor by the data controller, then the data processor is obligated to inform the data controller immediately upon becoming aware of the breach. Thus, the responsibility of notifying the Commissioner always rests with the controller, even if the breach pertains to data integrity being processed by the processor on behalf of the controller.

It is the controller's task to independently assess the seriousness of the risk to the rights and freedoms of individuals resulting from the breach, and based on this assessment, decide whether to report the incident or not. Naturally, the controller will need to conduct such an assessment for each individual breach. If the incident occurs at the processor's end, the processor will not be responsible for assessing the risks that may arise from the breach. Their task is to immediately inform the controller of the incident, and it is the controller's responsibility to assess the resulting risks and decide whether to inform the Commissioner and the affected individuals about the breach.

Example

When is incident reporting necessary?

In a hospital, critical health data of patients has been lost, which will lead to the postponement of certain surgeries and thereby pose serious risks to their health. Since such a breach of personal data directly endangers people's rights and freedoms, it is clear that the hospital, as the data controller, must promptly report such a breach to the Commissioner and the individuals whose data has been compromised.

When is incident reporting not necessary?

Within a media company, a power outage caused a temporary interruption in the operation of the system dedicated for sending the company's newsletter, making it impossible to send the newsletter as subscriber email addresses are temporarily unavailable. This situation will not pose risks to the rights and freedoms of individuals whose data is temporarily unavailable. Therefore, there is no obligation for the media company to report the incident to the Commissioner or the individuals whose data is unavailable.

The law specifies the information that must be included in the breach notification: a description of the nature of the personal data breach, types of data, approximate number of affected individuals and compromised data records, the name and contact information of the data protection officer (if designated),

or information on how to obtain data breach details by other means; a description of the potential consequences of the breach and a description of the measures taken by the controller to mitigate potential adverse effects.

The Commissioner has created a template for notifying of personal data breaches⁶⁵ within the Policy on the form and method of notifying the Commissioner of personal data breaches.⁶⁶ Data controllers can use this template when reporting personal data breaches. If, at the time of reporting an incident, a controller is unable to provide all the information required by law regarding the breach, they may provide it subsequently.

Ultimately, the law prescribes the duty of controllers to document each individual incident of personal data breach. This documentation should encompass all relevant facts about the breach, its consequences, and the measures taken to address them, enabling the Commissioner to determine whether the controller acted in accordance with the law.

The Commissioner has enacted the Policy on the form and method of maintaining internal records of violations of the Personal Data Protection Law and measures taken in the course of inspection.⁶⁷ This policy prescribes the template according to which the Commissioner's office maintains internal records of incidents – violations of the law that have occurred, and measures taken by the Commissioner during inspection in connection with the incident.

Trusted resources

The Spanish supervisory authority has developed a simple and free tool called Asesora Brecha, available in English as well, which serves to assess the obligation to notify the Commissioner about personal data breaches. It is important to note that after using the tool, the data entered into it is automatically deleted, so the Spanish supervisor cannot in any case access its contents. Please be aware that this tool is merely a decision-making aid and its outcome does not, under any circumstances, represent the opinion of the Spanish supervisor on a specific personal data breach.¹ The Spanish supervisor has also prepared an extensive guide on the obligation to notify about personal data breaches, freely available in English.²

¹ Asesora Brecha

² Guidelines on Personal Data Breach Notification



65 The template is available on the Commissioner's website: <https://shorturl.at/dnFMT>. [in Serbian]

66 Rulebook on the template of notification of personal data breach and the manner of notifying the Commissioner, for information of public importance and protection of personal data on personal data breach ("Official Gazette of the RS", number 40/19), <https://www.pravno-informacioni-sistem.rs/SlGlasnikPortal/eli/rep/sgrs/drugidrzavniorганиorganizacije/pravilnik/2019/40/1>. [in Serbian]

67 "Official Gazette of RS", number 40/19.

10.6.4. Notifying data subjects

Relevant provisions: *GDPR* – Article 34, Recitals 86 and 87; *PDPL* – Article 53.

In addition to notifying the Commissioner, the PDPL stipulates the obligation of the data controller to inform the data subjects in the event that such a breach could pose a high risk to their rights and freedoms. In this case, the data controller promptly informs the specific individual and is required to clearly and comprehensibly describe the nature of the data breach in the notification. The controller must also provide information about the contact person for data protection, describe potential consequences of the breach, and outline the proposed or taken measures to address the breach, including measures aimed at mitigating the harmful effects of the breach.

The controller will not be required to inform the affected individual in cases when:

- the data controller has implemented appropriate technical, organisational, and personnel protection measures regarding the compromised personal data, particularly if encryption or other measures have rendered the data unintelligible to unauthorised individuals;
- the data controller has subsequently taken measures to ensure that the data breach with a high risk to the rights and freedoms of the individual can no longer have consequences for that individual;
- notifying the affected individual would require a disproportionate amount of time and resources. In such cases, the data controller is obligated to provide the affected individual with notification through public means or other effective methods. If the data controller has not informed the affected individual about the data breach, and considering the possibility that the breach may pose a high risk, the Commissioner may order the data controller to do so or determine that the conditions for disproportionate effort have been met.

10.7. Data transfers

Relevant provisions: *GDPR* – Articles 44-50, Recitals 101-116; *PDPL* – Articles 63-66.

The PDPL sets the rules that controllers and processors must adhere to when transferring (exporting) personal data from Serbia to another country or international organization. The GDPR sets the rules for the transfer (export) of personal data outside the borders of the European Union.

Exporting personal data from Serbia occurs when a data controller or processor to whom PDPL applies (“data exporter”) transfers or otherwise makes personal data available to another data controller or processor located in another country, or when that data controller or processor is an international organization (“data importer”).

Therefore, data transfer is a broad concept within the context of the law and encompasses not only the physical or electronic transmission or sending of specific

personal data, but it can also involve making data available in other ways. For example, a transfer exists when a data controller or processor outside of Serbia is provided with a code that allows access to data in Serbia. Additionally, data transfer occurs when a data controller or processor in Serbia uses a server located outside of Serbia to store personal data. This is quite common nowadays, as numerous global companies provide cloud and hosting services with servers located in other countries. It's also possible that data exported from Serbia may travel through multiple jurisdictions.

Examples

Example 1

Jovana decided to travel to London via the Serbian travel agency X. Agency X collaborates with hotel Y in London, which provides accommodation for Jovana and other travellers. Agency X will email Jovana's information to hotel Y so that the hotel can reserve a room for her trip. The fact that agency X sent Jovana's personal data to hotel Y constitutes the transfer (export) of personal data outside of Serbia.

Example 2

Company X from Serbia has engaged company Y based in Germany to store Company X's data on its server located in France. The fact that the personal data processed by the Serbian company X as a data controller will be entrusted to the German company Y as a processor and will be stored outside the borders of Serbia constitutes the transfer (export) of personal data from Serbia.

Example 3

Company X from Serbia is part of a larger corporate group, and it shares an HR department with its sister companies in Canada and America. The HR department is within the Canadian company and has access to a shared server where the data of employees of Company X from Serbia is stored. The fact that the Canadian company has access to the data of employees from Serbia constitutes the transfer (export) of personal data from Serbia.

Guidelines

The EDPB has issued guidelines on the interplay between the rules of territorial scope (Article 3 of the GDPR) and the provisions regarding international transfers of personal data (Chapter V).¹ These Guidelines aim to clarify scenarios where the requirements for international transfers of personal data should be applied. To this end, three cumulative criteria have been identified to qualify processing actions as international transfers of personal data.

¹ EDPB, Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR, Version 2.0, 14. 2. 2023



1. A controller or a processor (“exporter”) is subject to the GDPR for the given processing.
2. The exporter discloses by transmission or otherwise makes personal data, subject to this processing, available to another controller, joint controller or processor (“importer”).
3. The importer is in a third country, irrespective of whether or not this importer is subject to the GDPR for the given processing under the general rules of territorial scope.

If all three criteria are met, it will be considered an international transfer of personal data, and Chapter V GDPR will apply. If the criteria are not met, the rules of Chapter V do not apply, but the data controller remains obliged to comply with other GDPR provisions and remains fully responsible for its processing activities, regardless of their location.

10.7.1. *General rule for transfers*

Relevant provisions: *GDPR* – Article 44; *PDPL* – Article 63.

According to the PDPL rules, any transfer of personal data from Serbia to another country or international organisation can only be carried out if the data controller and processor comply with PDPL. The primary goal is to ensure a level of protection for the individuals whose data is being transferred, as guaranteed by PDPL.

The PDPL provides multiple possibilities or situations where there is a legal basis for lawful data transfers.

10.7.2. *Transfers based on an adequate level of protection*

Relevantne odredbe: *GDPR*, član 45; *ZZPL*, član 64.

A universal legal basis applicable to all data controllers and processors is the export to foreign countries (or parts of the territory of one country) or international organisations where an adequate level of data protection has been established.

From the perspective of PDPL, an adequate level of protection is considered to exist in countries and international organizations that are members of the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, in countries or international organizations that the European Union has determined to provide an adequate level of protection, or with which Serbia has concluded an international agreement on the transfer of personal data. Practically, at this moment, data export from Serbia is permitted to all European Union member countries, as well as to other countries that are signatories to the Council of Europe Convention, and to all countries where data export from the European Union is allowed based on an adequacy decision made by the European Commission for each country individually. Adequacy decisions

have been made for the following countries: Andorra, Argentina, Canada (commercial organizations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Republic of Korea, Switzerland, United Kingdom, Uruguay.⁶⁸

Previously, the export of personal data from the EU to the United States was allowed under the Privacy Shield mechanism, where U.S. companies voluntarily certified with the U.S. Department of Commerce to enable the import of personal data from the EU. The idea was to verify and ensure that these data recipients would indeed provide an adequate level of protection for the data they import. Naturally, major U.S. technology companies like Google, Amazon, and the like were certified since such companies are the largest importers of personal data from the EU.

However, on July 16, 2020, the European Court of Justice issued ruling CJEU - 311/18, declaring the Privacy Shield invalid.⁶⁹ As a result, the export of personal data from the EU to the US has become much more complex. Even the so-called standard contractual clauses (one of the legal bases for data transfers, which will be discussed further) cannot be used as a mechanism for transferring personal data from the EU to the US if the US data importer is a company subject to US laws and engaged in mass surveillance of citizens. This situation arises due to the fact that US regulations require companies to share citizens' data (including EU citizens) with intelligence agencies in the US. These are mainly companies involved in electronic communications, including tech giants like Google, Meta (formerly Facebook), and the like. This does not mean that data will not be transferred from the EU to the US; data transfers are permitted under other legal bases. For example, transfers are allowed for the performance of a contract (such as booking a hotel in the US or making online purchases from a US seller), data can also be exported from the EU to the US based on consent, as well as other legal bases.

Practice

The French supervisory authority concluded that a French company engaged in online product sales violated Chapter 5 of the GDPR regulating international data transfers from the EU by using Google Analytics, leading to unlawful data transfers to Google, a company headquartered in the US.

Namely, visitor data from the website of the French company was transferred to the US through Google Analytics, as it was integrated into the website of the French company engaged in online sales. Google Analytics allowed user tracking by associating their identifier with session data initiated from their devices, and then transmitting that information to Google Analytics servers located in the US. The supervisor concluded that the combination of visitor identifiers with several other data points (such as visited web addresses, browser metadata, visit times, IP addresses) allowed for identification of visitors, thus constituting personal data, and that their transfer to the US occurred.

68 European Commission, Adequacy decisions, https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en.

69 CJEU, Judgment of the Court (Grand Chamber) In Case C-311/18, 16. 7. 2020, <https://noyb.eu/files/CJEU/judgment.pdf>.

The supervisor held that there was no legal basis for the transfer after CJEU ruling C-311/18 declared the Privacy Shield invalid. The supervisory authority determined that the standard contractual clauses concluded between the French company and Google LLC did not provide an adequate level of protection, as Google is an electronic service provider and subject to US surveillance laws.

At the time, the French supervisory authority decision was the second decision deeming the use of Google Analytics to be in violation of the GDPR. The first decision on this matter was issued by the Austrian supervisor.¹



¹ GDPR Hub, DSB (Austria) - 2021-0.586.257

In early 2022, the European Commission announced that it had reached the foundational framework with the United States regarding the transfer of data between the EU and the US.⁷⁰ The new legal framework is intended, among other things, to address the issues raised in the decision that invalidated the Privacy Shield mechanism and to signify the commitment of the US to implement reforms in its system that will strengthen the right to privacy and civil liberties, limit access of US intelligence agencies to EU citizens' data, and introduce new protection mechanisms that ensure surveillance measures are genuinely necessary and proportionate for national security, as well as to establish legal safeguards in the US system regarding personal data, including the creation of a court dedicated to data protection.

In October 2022, the President of the US signed an executive order that, together with regulations issued by the US Attorney General, implements the foundational framework agreement reached with the European Commission into US law. Based on this executive order, the European Commission is expected to prepare an adequacy decision, leading to the US being reinstated on the list of countries to which the transfer of personal data from the EU is allowed.

The collapse of the Privacy Shield mechanism has practical significance for the export of data from Serbia to the US, as the US is no longer on the list of countries with an adequacy decision by the European Commission under the condition that a specific company has certified itself under the Privacy Shield mechanism. A significant number of Serbian companies entrust data processing to various US technology companies, using their infrastructure for data storage (for example, servers of Amazon, Digital Ocean, and the like). Now that standard contractual clauses cannot always be used as a legal basis for transfers, Serbian companies exporting personal data to the US should conduct additional assessments to determine whether the transfer to a specific US company is permissible and whether that company adheres to standards that should provide the same level of protection to personal data as prescribed by PDPL. In practice, this is done by sending a questionnaire to

⁷⁰ European Commission, EU-U.S. Data Privacy Framework, 7. 10. 2022, https://ec.europa.eu/commission/presscorner/detail/en/qanda_22_6045.

the importing company that it needs to respond to. Of course, transfers are allowed based on legal grounds such as consent, contract performance, and the like.

Guidelines

The EDPB has issued Recommendations on measures that complement tools for international data transfers in order to ensure compliance with the level of personal data protection within the EU.¹ To provide support to exporters of personal data in the complex process of assessing third countries and identifying appropriate measures during data transfers, the EDPB has outlined six steps in these recommendations that need to be undertaken.

1. Mapping all transfers of personal data to third countries.
2. Verifying the legal basis for the transfer.
3. Assessing if there is anything in the law and/or practices in force of the third country that may impinge on the effectiveness of the appropriate legal basis in the context of a specific transfer (e.g. legislation is formally meeting EU standards but manifestly not applied/complied with in practice).
4. Identifying and adopting supplementary measures that are necessary to bring the level of protection of the data transferred up to the EU standard of essential equivalence if the assessment reveals that the third country legislation and/or practices impinge on the effectiveness of the legal basis chosen for the specific transfer.
5. Taking any formal procedural steps the adoption of supplementary measure may require, depending on the legal basis of the processing.
6. Re-evaluating at appropriate intervals the level of protection afforded to the personal data transferred to third countries and monitoring if there have been or there will be any developments that may affect it.

¹ EDPB, Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, Version 2.0, 18. 6. 2021.



Furthermore, PDPL provides a rule that the list of territories considered to provide an adequate level of protection, or for which the Government of Serbia has determined an adequate level of protection, should be published in the “Official Gazette”.⁷¹ If data is exported to territories with an adequate level of protection, controllers and processors do not need to take any additional steps – it is considered that an adequate level of protection has already been established for the entire territory where the data is being exported.

⁷¹ Decision on the list of countries, parts of their territories or one or more sectors of certain activities in those countries and international organizations in which it is considered that an adequate level of protection of personal data is ensured (“Official Gazette of RS”, number 55/19), <https://www.pravno-informacioni-sistem.rs/SlGlasnikPortal/eli/rep/sgrs/vlada/odluka/2019/55/2>. [in Serbian]

10.7.3. Transfer with appropriate safeguards

Relevant provisions: *GDPR* – Article 46; *PDPL* – Article 65.

If the data is exported to a foreign country, part of a territory, one or more specific activities of a foreign country, or to an international organization lacking the adequate level of personal data protection, the controller or processor exporting data from Serbia can do so only if they have implemented appropriate safeguards. The purpose of these safeguards is to ensure the feasibility of rights and effective legal protection for individuals whose data is being transferred (exported) from Serbia.

Therefore, unlike the data transfer based on an adequate level of protection, where it is sufficient for the specific country or international organization to be on the list of countries where data transfer is allowed, and data transfer to that country is thereby unrestricted, here the controller or processor must ensure appropriate measures for the protection of personal data.

The controller or processor ensures the feasibility of rights and legal protection for the individual to whom the data relates without specific approval from the Commissioner in one of the following manners provided by PDPL:

- By a legally binding act between government authorities;
- through standard contractual clauses provided by the Commissioner;
- by binding corporate rules;
- with an approved code of conduct;
- through certificates issued in accordance with the PDPL rules.

Additionally, if none of these mechanisms are applicable in a specific situation, controllers and processors can ensure appropriate protection measures based on the specific approval of the Commissioner for the particular case, as follows: (1) contractual provisions between the controller or processor and a controller, processor, or recipient in another country or international organization approved by the Commissioner; or (2) provisions inserted into an agreement between government authorities, which ensure effective and enforceable protection of the rights of the data subjects.

The simplest of these safeguards is the use of standard contractual clauses, often employed for data transfers. The reason for this is that standard contractual clauses are essentially a single contract, the draft of which is provided by the Commissioner, and they are signed in the written form as they are, without modifications, except for certain circumstances specific to the particular transfer, which are filled in at the designated places.

The Commissioner has adopted a Decision on the specification of standard contractual clauses, in which the content of standard contractual clauses to be signed between controllers and processors has been specified. These clauses can be used as a legal basis for transfers when a controller in Serbia intends to transfer personal data to a foreign processor.⁷²

⁷² Decision on establishing standard contractual clauses ("Official Gazette of RS", No. 5/2020), <http://www.pravno-informacioni-sistem.rs/SlGlasnikPortal/eli/rep/sgrs/drugidrzavniorganizacijedluka/2020/5/1>. [in Serbian]

Example

Company A from Serbia wants to engage Company B from Turkey, which provides hosting services, to store certain data on its infrastructure, including personal data. Since Turkey is not on the list of countries with an adequate level of protection, Company A will, in addition to the basic hosting agreement, sign standard contractual clauses with Company B from Turkey as a separate agreement or an annex to the basic hosting agreement. This will establish the appropriate legal basis for transferring data from Serbia to Turkey..

When using standard contractual clauses as the legal basis for transfers, a current issue in Serbian context is that the Commissioner has only adopted a model of standard contractual clauses that can be signed when there is a transfer between a controller and a processor. Situations involving data transfers between controllers or between processors are not yet regulated by separate models of standard contractual clauses. However, according to Serbian law, the Commissioner is the only authority empowered to issue such standard contractual clauses, as the law explicitly mandates the issuance of standard contractual clauses that govern the relationship between controllers and processors.

The Serbian Commissioner

Within their practice, the Commissioner has clarified certain aspects regarding the adoption of standard contractual clauses that they have developed.

- By agreeing on standard contractual clauses that comprehensively regulate the legal relationship between controllers and processors, appropriate protection measures can be ensured in cases where a controller or processor transfers personal data to another country, a part of its territory, or one or more sectors of specific activities within that country. Specific approval from the Commissioner is not required.¹
- Standard contractual clauses regulate the legal relationship between controllers and processors, not between processors and subprocessors. Therefore, they cannot be applied to regulate relationships between processors and subprocessors.²

¹ *Protection of personal data: Positions, opinions and practice of the Commissioner, publication no. 6, Belgrade, 2021. Case number: 073-14-681/2020-02, pp.122-123 [in Serbian]*

² *Ibid. Case number: 073-14-803/2020-02, pp. 123-125*



- If the decision is made to apply standard contractual clauses, the parties to the contract cannot modify their provisions.¹
- Standard contractual clauses are interpreted and applied in accordance with the laws of the Republic of Serbia (Article 14 of the Standard Contractual Clauses – Applicable Law). The parties to the contract cannot agree on the application of foreign law. When designating jurisdiction for dispute resolution, the parties may specify the jurisdiction of authorities/bodies of the Republic of Serbia²

¹ *Ibid.* Case number: 073-14-1517/2020-02, pp. 125–127

² *Protection of personal data: Positions, opinions and practice of the Commissioner, publication no. 7, Belgrade, 2022. Case number: 073-14-2175/2021-02, pp.164–165 [in Serbian]*



On the other hand, in 2021, the European Commission adopted modernized standard contractual clauses for use in situations where a controller or processor transfers data outside the European Union to a controller, processor, or subprocessor located outside the European Union.⁷³ Therefore, these situations are not limited to the transfer of data from a controller to a processor (as is currently the case with Serbian domestic standard contractual clauses) but cover a much broader spectrum of data transfers in terms of processing roles for which the transfer is carried out.

Binding corporate rules are another relatively common legal basis for data transfers, but they are used for transfers within a corporate group present in multiple jurisdictions. It is a legally binding document that needs to be approved by the Commissioner when exporting personal data from Serbia.

The Serbian Commissioner

The first Binding Corporate Rules in Serbia were approved in 2021 at the request of the company Ernst & Young d.o.o., as a legal basis for exporting personal data from Serbia within a corporate group.¹

¹ EY, Obavezujuća poslovna pravila (Republika Srbija), Politika za rukovaoca, 1. 8. 2021.



In situations where Binding Corporate Rules are used as a mechanism for transferring data from the Republic of Serbia to another country, a part of its territory, or one or more sectors of specific activities in that country, or to an international organization

⁷³ European Commission, Directorate-General for Justice and Consumers: *Standard contractual clauses for international transfers*, 4. 6. 2021, https://commission.europa.eu/publications/standard-contractual-clauses-international-transfers_en.

that does not provide an adequate level of personal data protection, such Binding Corporate Rules need to be submitted to the Commissioner for approval, regardless of whether they have been approved by a European supervisory authority. The Commissioner is not competent to grant approval for Binding Corporate Rules that do not regulate the transfer of personal data from the Republic of Serbia.²

² *Protection of personal data: Positions, opinions and practice of the Commissioner, publication no. 6, Belgrade, 2021. Case number: 073-14-682/2020-02, pp. 131-132 [in Serbian]*



It is expected that institutes such as certification and codes of conduct will soon become operational in Serbia.

Guidelines

In the field of data transfers, the EDPB has developed specific Guidelines on certification as a basis for data transfer¹ i Smernice o kodeksima postupanja kao osnovu za prenos podataka.² Ove smernice mogu biti od posebnog značaja kada se domaća praksa u ovoj oblasti bude razvijala.

¹ Guidelines 07/2022 on certification as a tool for transfers

² Guidelines 04/2021 on Codes of Conduct as tools for transfers



10.7.4. Transfers in specific situations

Relevant provisions: *GDPR* – Article 49; *PDPL* – Article 69.

The law explicitly lists specific situations in which the transfer is allowed if none of the mechanisms for implementing appropriate protective measures can be applied. These are instances where:

1. the data subject has explicitly consented to the transfer after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards;
2. the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request;
3. the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject;

4. the transfer is necessary for important reasons of public interest prescribed by the law of the Republic of Serbia, provided that the transfer of certain types of personal data is not restricted by the law;
5. the transfer is necessary for the establishment, exercise, or defence of legal claims;
6. the transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent;
7. the transfer is made from a public register which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, but only to the extent that the conditions laid down law for consultation are fulfilled in the particular case.

Additionally, if none of these conditions are met, the transfer of personal data may only be carried out if the following cumulative conditions are fulfilled:

1. the transfer is not repetitive,
2. concerns only a limited number of data subjects,
3. is necessary for the purposes of compelling legitimate interests pursued by the controller which are not overridden by the interests or rights and freedoms of the data subject, and
4. the controller has assessed all the circumstances surrounding the data transfer and has on the basis of that assessment provided suitable safeguards with regard to the protection of personal data.

The controller is obligated to inform the Commissioner about the data transfer on this basis, as well as to provide the data subject with information about the data transfer, including information about the specific legitimate interest pursued by the controller through such transfer.

Guidelines

For a better understanding of transfers in specific situations, it is useful to consider the relevant guidelines developed by the EDPB. The Guidelines aim to clarify situations in which a transfer is permitted even though none of the mechanisms for implementing appropriate safeguards can be applied, and they contain detailed explanations of each specific situation.¹



¹ EDPB, Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679

10.7.5. Data import into Serbia from the EU

All legal bases for data transfers provided by Serbian law (transfer based on an adequate level of protection – existence of an adequacy decision; transfer with the application of appropriate safeguards; transfer in special situations) follow the

logic of the GDPR. Therefore, the GDPR has practically the same rules when it comes to exporting data from the EU to other countries, including Serbia.

Since Serbia is not on the list of countries determined by the European Commission to have an adequate level of data protection (i.e., no adequacy decision has been made), the question arises as to which legal basis a Serbian company will use when importing personal data of EU citizens into Serbia.

Namely, a large number of companies in Serbia process the data of EU citizens as part of their business activities. This is most often the case with technology companies, which mainly operate on the internet – for example, they have an English-language website visited by global audience, including EU citizens, or they have an application on the App Store that can be purchased by EU citizens.

Of course, it doesn't have to be only technology companies; the import of data of EU citizens into Serbia can exist in various other circumstances. For example, when a Serbian company is part of a larger corporate group present in the EU, there may be a transfer of employee data from the EU company to the subsidiary company in Serbia.

Furthermore, if a Serbian company collaborates with an EU company based on a contract, and this collaboration involves the EU company sharing personal data of EU citizens with the Serbian company, once again there is an import of data of EU citizens into Serbia.

When data is being exported from the EU to another country that is not on the list of countries with an adequacy decision, such as Serbia, the most common and straightforward legal basis for the transfer used is the EU Standard Contractual Clauses. As noted, these are essentially draft contracts made by the European Commission and are signed as an annex to the main cooperation agreement or as a separate contract. The European Commission's Standard Contractual Clauses can be used in practically all roles in data processing – regardless of whether the Serbian data importer is a controller or processor, and regardless of whether the EU data exporter is a controller or processor. Therefore, they can be signed between two controllers, two processors, or between a controller and a processor.

Example

A German company X needs call centre services and engages a Serbian Company Y to provide these services in English in the EU market, based on a concluded agreement. During the provision of services, the Serbian company processes data of EU citizens, which involves the transfer of personal data from the EU to Serbia. In order for such a transfer to be legal, Company X and Company Y, in addition to the basic cooperation agreement, conclude standard contractual clauses between the controller and processor drafted by the European Commission.

Standard contractual clauses are the simplest and therefore the most common legal basis for exporting data from the EU to Serbia. However, they are not the only option. There are other legal bases, such as binding corporate rules, issued certificates, approved codes of conduct, etc. All of these legal bases represent transfers with appropriate safeguards. For example, if the Serbian company is part of a larger corporate group present in both the EU and Serbia, and thus involves the transfer of personal data from the EU to the Serbian subsidiary, the legal basis for such transfer could be binding corporate rules. This is a legally binding document that regulates the transfer of data within member companies of a corporate group and contains circumstances and rules regarding the protection of personal data that the corporate group members must adhere to, and it must be approved by the competent data protection authority.

10.8. Representative

Relevant provisions: *GDPR* – Articles 4 and 27; *PDPL* – Articles 4 and 44.

10.8.1. Representative of a foreign controller or processor in Serbia

The law stipulates that in certain situations of extraterritorial application of the Serbian PDPL to a foreign controller or processor, a so-called representative must be established in the Republic of Serbia.

The PDPL applies extraterritorially to foreign controllers and processors if they offer goods or services to citizens of the Republic of Serbia or monitor the activities of individuals when such activities are carried out within the territory of the Republic of Serbia.

The representative is a natural or legal person residing or having a registered office within the territory of the Republic of Serbia, authorised to represent the foreign controller or processor in relation to their obligations provided by the PDPL.

The purpose of the provision regarding the establishment of a representative in the Republic of Serbia for foreign controllers or processors who process the data of citizens of the Republic of Serbia in this manner is to ensure that Serbian Commissioner, or another person (for example, the person whose data is processed by the foreign controller or processor), can directly address the representative regarding all matters related to the processing of personal data. The obligation to appoint a representative has a clear logic, as it is much easier for the Commissioner or a citizen of Serbia to directly contact the representative in Serbia instead of the foreign company. The representative is obliged to cooperate with the Commissioner in the exercise of the Commissioner's legal powers, to respond to their questions within the scope of inspection supervision, to grant access to personal data processed by the entity that appointed them, etc.

Complaints, lawsuits, and other legal claims in accordance with the PDPL can be filed directly against foreign controllers or processors, regardless of whether that controller or processor has appointed their representative in Serbia.

Trusted resources

The Commissioner's website contains an updated list of foreign companies that have appointed a representative in Serbia.¹ The SHARE Foundation has also prepared a dedicated page with contact information for representatives of foreign companies in Serbia, whom citizens can contact to exercise their legal rights.² In most cases, the established representatives in Serbia are individual lawyers or law firms.

¹ Commissioner, Foreign companies that have appointed representatives in accordance with the Personal Data Protection Law, [in Serbian]

² Representatives



Example

A hotel in Budapest targets Serbian citizens for accommodation services by providing an option for the Serbian language on its website, employing a marketing strategy for Serbian citizens, and allowing payment in Serbian currency. Consequently, this constitutes a controller to whom the Serbian PDPL is applied extraterritorially. The hotel is obligated to appoint a representative in Serbia, as a controller that regularly offers goods and services and processes the data of Serbian citizens.

Example

The Meta Company enables Serbian citizens to create profiles on Facebook, offers Facebook in Serbian language, and it is evident that it regularly processes the data of Serbian citizens by targeting them and providing specific services. In this case, Meta is obliged to appoint a representative in Serbia.

However, the obligation for a foreign controller or processor to establish a representative in the Republic of Serbia will not exist if they occasionally process personal data and if processing does not involve special categories of personal data to a significant extent or data relating to criminal convictions and offenses, and it is unlikely to pose a risk to the rights and freedoms of individuals, considering the nature, circumstances, scope, and purpose of the processing.

Additionally, there is no obligation for controllers or processors that are foreign authorities to appoint a representative in the Republic of Serbia, even though the PDPL is applied extraterritorially to them.

Example

Company A from Norway is the parent company of Serbian Company B, which is engaged in providing and billing municipal waste management services. Serbian Company B processes data of its users in order to issue invoices to them. Occasionally, user data from Company B is shared with Company A from Norway, but this happens occasionally, for instance, when Serbian Company B has an issue with collecting payment from a specific user and sends certain data of that user in a report to Company A. This means that the processing of user data of Serbian citizens by the Norwegian Company A is sporadic, rare, and occurs in isolated cases. Therefore, the Norwegian company will not be obliged to appoint a representative in Serbia.

10.8.2. Representative of a Serbian controller or processor in the EU

Similar to the Serbian PDPL, the GDPR stipulates that controllers and processors outside the EU who 1) target EU citizens by offering goods and services to them, or 2) monitor their activities within the EU, must designate a representative in the EU. This is considering that GDPR has an extraterritorial application to such controllers and processors.

The rationale behind this obligation is to ensure that the rights of EU citizens concerning the processing of personal data are not compromised when being processed by entities outside the EU in a globalised world with a significant flow of data. By designating a representative, competent authorities in EU member states responsible for personal data protection, as well as the data subjects, are enabled to directly address the representatives.

Guidelines

Although GDPR in its Recital 80 stipulates that a representative is subject to enforcement proceedings in the event of a violation by the controller or processor who designated them, according to the EDPB Guidelines, the GDPR does not establish substantive liability of the representative in relation to the controllers or processors they represent in the EU.¹ The concept of a representative was introduced to establish a link and effective enforcement of GDPR towards controllers and processors outside the EU to whom GDPR apply extraterritorially. Supervisory authorities can initiate enforcement proceedings through the representative, including corrective measures and fines against the controller or processor. The representative can only be directly responsible for the breach of their own obligations (primarily record-keeping and providing information to supervisors).

¹ Guidelines 3/2018 on the territorial scope of the GDPR



Practice

The High Court of England and Wales held that controllers and processors outside the EU that appoint a representative in accordance with GDPR do not “outsource” liability for GDPR violations, meaning that the controller can be directly responsible only for their own obligations.¹

Namely, the data subject lodged a complaint against the American company World Compliance Inc. for processing and sharing their data, and subsequently initiated an appropriate violation proceeding against the representative of that American company in the United Kingdom (Lexisnexis risk solutions UK ltd).

The court ruled that the purpose of appointing a representative is to facilitate contact between data subjects and executive bodies and the controller who is not subject to the specific jurisdiction, and that representatives cannot be held liable on their behalf.



¹ GDPR Hub, EWHC (QB) - Sanso Rondon v LexisNexis Risk Solutions UK Ltd

Serbian controllers and processors to whom GDPR is applied extraterritorially must appoint their representative in the EU in writing. This practically means that:

- a Serbian controller or processor must assess whether GDPR is applied to them extraterritorially.
- a Serbian controller or processor must verify whether they are subject to the obligation to designate a representative, as there are certain exceptions to the prescribed GDPR requirement (cases where a Serbian controller or processor occasionally processes data of EU citizens, when they do not extensively process sensitive data or data related to criminal convictions, and when they are a public authority).
- if a Serbian controller or processor determines that they need to appoint a representative, they do so by issuing a written decision appointing a representative in the EU. Such a decision should include the name or business name of the representative and other identifying information such as address and contact details. To make the decision to appoint a representative, the Serbian entity and the future representative need to conclude an engagement agreement or agree on engagement through other means. Although GDPR does not set specific qualifications that the representative must meet, such as education or experience, representatives in the EU are usually individuals or companies with knowledge related to personal data protection, such as lawyers, consultants, etc. There is also the possibility of subscribing to this service for a specific period, and the fee is determined based on various parameters, such as the number of requests from data subjects, etc.

- it is recommended that the representative is appointed in the EU member state where a significant portion of the individuals whose data is processed by the foreign (in this case, Serbian) controller or processor are located. For instance, if the service provided by the Serbian entity is available in multiple EU countries and it's impossible to determine in which of these countries the largest number of individuals whose data the Serbian entity processes is located, then it is necessary to appoint a representative in one of those countries.

Example

Serbian Company A has developed a mobile application for practicing yoga. The application operates globally, and citizens of the EU can also purchase it by downloading the app from the App Store, paying a monthly subscription in EUR, and creating an account, which involves sharing certain personal data with the owner of the application, Serbian Company A.

Given that Serbian Company A regularly processes personal data of EU users and provides the application service, the Serbian company must appoint a representative in the EU.

Serbian Company A, which provides services to retail establishments, has engaged a shopping centre in Poland to analyse the behaviour of shopping centre visitors, specifically their movement through the shopping centre, using Wi-Fi trackers. This is done to provide suggestions to the Polish shopping centre on the order and floors to place specific retail stores.

Since Serbian Company A tracks the behaviour of people in the Polish shopping centre, which is in the EU, the Serbian company will need to appoint a representative in the EU.

10.8.3. Representative of a Serbian controller or processor in third countries

GDPR is not the only foreign law addressing personal data protection that requires companies operating in foreign markets and processing personal data of local citizens to appoint a local representative for data protection matters.

This is the case, for example, with the Chinese Personal Information Protection Law, which mandates that foreign companies processing data of Chinese citizens appoint a representative in China responsible for processing such data.⁷⁴ They are also required to submit the name and contact information of the representative to local authorities responsible for data protection. This obligation applies to Serbian companies offering services and products to Chinese citizens and monitoring their behaviour.

A similar obligation for foreign (including Serbian) companies to appoint a local representative is stipulated in the Law on Personal Data Protection of North Macedonia. Similar to GDPR and the Chinese Personal Information Protection Law, the North

⁷⁴ Article 53 of Chinese Personal Data Protection Law, enacted on 1. 11. 2021, http://en.npc.gov.cn.cdurl.cn/2021-12/29/c_694559_3.htm.

Macedonian law imposes this obligation on foreign companies offering goods and services to citizens of North Macedonia and monitoring their behaviour. The duties of a local representative of a foreign company under the North Macedonian law are similar to the obligations of representatives under both the Serbian PDPL and GDPR.

10.9. Allocation of roles in the organisation

Controllers and processors can be natural persons or organizations, legal entities, or government bodies. As established in the known case of Jehovah's Witnesses,⁷⁵ it is possible for individuals along with a religious organization to jointly act as controllers. However, in cases where data processing occurs within an organization, the assumption is that the controller will be the organization itself, rather than the individuals involved in the processing activities.

Dilemmas

Is it possible to consider an individual within an organization as a controller?

The Guidelines of Working Party 29 on the Concepts of Controller and Processor¹ and the EDPB Guidelines on the Concepts of Controller and Processor under the GDPR² stipulate that in cases of doubt, it should be assumed that in a specific case the controller is the organisation as such and not an individual within the organisation. In general, it should be presumed that the organization is responsible for the processing of personal data carried out by its employees within the scope of the organization's business domain. Employees with access to personal data should be considered individuals authorised by the controller or processor to access personal data (in the context of Article 29 of the GDPR or Article 46 of the Serbian PDPL). However, sometimes clear circumstances indicate that the individual should be considered the controller: it may occur that an employee decides to use personal data for their own purposes, thereby unlawfully exceeding the authority that they were given. In order to limit its liability in such cases, the organisation has a duty to implement appropriate technical, organizational, and personnel measures, including training and informing employees about handling personal data.

¹ Article 29 WP, Opinion 1/2010 on the concepts of 'controller' and 'processor', Adopted on 16 February 2010

² EDPB, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, Version 2.1, Adopted on 07 July 2021



Therefore, when organisations appoint a specific individual to be responsible for processing activities or ensuring compliance with the legal framework for personal data protection, the appointed individual will not be the controller.

⁷⁵ Jehovah's witnesses, C-25/17, https://gdprhub.eu/index.php?title=CJEU_-_C-25/17_-_Jehovan_todistajat.

Instead, they will act on behalf of the organisation, which retains the status of the controller and is responsible in case of breaches. In this case, the appointed individual may be accountable to the organisation for their actions and breach of duties in accordance with the law and internal policies.

10.9.1. Personal data protection management in organisations

In terms of organisations involved in personal data processing, the legal framework for personal data protection does not establish a duty of compliance with the law to a specific individual or entity within the controller or processor, but rather leaves it to each organisation to regulate through internal rules.

Trusted resources

The specialized EDPB platform is available to assist small and medium-sized enterprises within the EU in complying with the legal framework for personal data protection.¹ The Irish supervisory authority has also published a dedicated guide for small and medium-sized enterprises.²

¹ EDPB data protection guide for small business

² Guidance Note: GDPR Guidance for SMEs.



In practice, larger organizations often delegate individual personal data processing tasks to specific organisational units. This delegation is not only common but also desirable to establish accountability systems and ensure compliance with personal data protection requirements. If a particular department or organizational unit is operationally responsible for processing operations and compliance, it does not imply that this department or unit becomes a controller. Organisational units without separate legal personality lack the capacity to assume the role of a controller.

Dilemmas

Parent and subsidiary companies – who is the controller?

Business organisations typically consist of multiple organisational units. Additionally, large companies may have multiple physical business locations, often spanning across different countries. They can comprise a range of legal entities with different functions, with overall control often vested in a parent or holding company. In practice, such organisational structures can complicate the allocation of roles in the processing activity and create numerous dilemmas in regards to determining status of a controller, joint controller, processor, recipients, and third parties.

Multinational corporations usually encompass various legal entities, including management companies and subsidiaries. It is not uncommon for one of these affiliated legal entities to be authorised to make decisions regarding the processing of personal data on behalf of the entire business organisation. In such cases, this legal entity may be formally designated as the controller for the entire group. Although this determination of the controller role is not prohibited in any way, it is not definitive and will only be confirmed after factual analysis. Assigning the role of controller in a situation involving multiple interested parties in the processing activity cannot generally be subject to legal or organisational engineering; the entity that independently or jointly determines the purpose and manner of processing will be recognised as the (joint) controller, regardless of formally prescribed roles.

A particular question arises as to whether and under what conditions parent companies can be considered controllers in relation to the processing of personal data undertaken by their subsidiary companies. However, it is certain that control in terms of corporate law does not automatically confer controller status on the parent entity for the processing operations conducted by its subsidiary. However, if the parent company is involved in determining the purpose and manner of processing, it will likely be a controller or joint controller.

For organizations that are extensive and possess a complex organisational structure, the issue of “data protection management” is particularly significant in order to ensure clear accountability of the entity representing the organisation and specific functional responsibilities within the organisational structure, such as delegating other entities to act as representatives or points of contact for data subjects.

The Serbian Commissioner

The Commissioner deliberated on the matter whether, in the case of transferring the entire business from one legal entity, which, as a controller, processes a large amount of personal data within its activities, to another legal entity, the legitimacy of personal data processing for which consent has already been given is called into question. In other words, whether the legal entity to which the business is being transferred would need to seek consent again from the data subjects, or if it is sufficient to transparently inform them about the change of controller.

The Commissioner held that the consent for processing personal data given by a specific individual to one controller, after being informed about all essential aspects of the specific processing in accordance with the law, may serve as a legal basis for the specific processing only for that controller. Therefore, such consent cannot be considered a valid legal basis for processing by another controller. Consent as a legal basis for processing personal data cannot be transferred to another controller, nor can it be taken over from another controller. The Commissioner also stated that matters related to establishment, management, changes in status, changes in legal form, termination, and other issues of significance for the position of business entities,

and thereby legal succession in terms of assuming their rights and obligations, are regulated by the Company Law and other relevant regulations. In terms of seeking opinions on their application, the Commissioner referred to the Ministry of Economy.¹

¹ *Protection of personal data: Positions, opinions and practice of the Commissioner, publication no. 7, Belgrade, 2022. Case number: 073-14-2509/2021-02, pp. 171-174 [in Serbian]*



10.9.2. Management

Depending on the legal form, the responsibility for aligning business operations with regulations lies with the management: the CEO or the board of directors. Although GDPR does not regulate this issue in a specific manner, in European law, management responsibility varies with national liability provisions and can involve civil, administrative, and criminal liability.⁷⁶

However, it should be noted that in certain situations, members of the management may be responsible not only as “responsible persons” of the controller but also directly responsible as independent controllers.

Dilemmas

When can the role of a controller apply to members of management?

In a case decided by the Higher Regional Court of Dresden, the responsibility of management for unlawful processing of personal data was specifically examined.¹ After an individual applied for a membership in an association, the association's director ordered a private investigator to conduct a background check. The private investigation initiated in this regard revealed information about the individual's prior criminal convictions. The association's executive board was informed of these findings and, based on this information, rejected the membership application. The individual argued that the controller had violated Article 10 of the GDPR, due to the circumstances that the data regarding criminal convictions were not processed under official supervision, and demanded compensation for emotional distress in the total amount of EUR 21,000.

Deciding whether the amount of 5,000 EUR awarded by the trial court in damages for pain and suffering was appropriate, the Higher Regional Court of Dresden upheld the breach established by the trial court, deeming that the controller could have achieved the purpose by requiring the individual to voluntarily disclose this information or provide a certificate of non-conviction issued by the competent police authority.

¹ GDPR Hub, OLG Dresden - 4 U 1158/21.



The reasoning of the lower court was affirmed in that both the organisation and its directors can be deemed controllers. Considering that individuals or legal entities that independently or jointly decide on the purpose and means of processing personal data can be considered responsible controllers, the court concluded that employees and other engaged individuals cannot be held responsible due to the fact that they acted on the orders of superiors, but this cannot be applied to the director, as the director independently engaged a private investigator and did not act according to someone else's instructions.

This court decision is undoubtedly significant, but at the same time, it was the subject of a lot of criticism, especially regarding the lack of more detailed reasoning. However, if practice follows the court's standpoint in this case, management could potentially be more personally liable for violations of personal data protection in the future. This should not be interpreted to mean that directors will inevitably be liable as controllers, as they usually act in accordance with orders and internal policies. Their liability can only be established if they exceed their authority and independently or jointly decide on the purpose and means of processing personal data

Direct liability of management members regarding breaches of personal data protection may indirectly arise from fundamental principles of corporate law, such as the duty of care. This duty implies an obligation for management members to perform their duties conscientiously, in the best interest of the company, and with a high degree of care – the care of a diligent businessperson. Considering that managerial positions require specialized knowledge and experience, the care of a diligent businessperson entails behaviour resembling that of a reasonably prudent person possessing knowledge, skills, and expertise in business. A management member lacking expert knowledge in a particular area relevant to the business, such as personal data protection, may base their decisions on the opinions of sector experts. If harm arises as a result of a decision based on the opinion of a relevant expert, the manager will not be liable for the damage. Management members not only have a duty to ensure that the organisation complies with the legal framework for personal data protection but also have an obligation to ensure that this is adequately implemented by other competent individuals. Managers who, in the process of compliance, make decisions that result in, for example, a violation of individuals' rights, cannot excuse themselves based on their lack of knowledge in the field of personal data protection.

Although organisational units specialised for performing these tasks can be established within the organisation, or a data protection officer can be appointed, it appears that management cannot simply delegate their responsibility on this basis. It is important to emphasise that delegating responsibility to a data protection officer would represent a certain conflict of interest, given that the duty of this officer primarily involves overseeing compliance with personal data processing within the organisation itself, in order to prevent potential breaches of the law. Such an understanding is in line with the fundamental principles of the law of obligations, according to which an employer, or the legal entity where an employee was working at the time of caused harm, is liable for the damage caused by the employee in the

course of or in connection with their work. An exception will apply if it is proven that the employee acted as they should have under the given circumstances, which will be further discussed in the section on employees.

10.9.3. Data Protection Officer

Relevant provisions: GDPR – Articles 37-39, Recital 97; PDPL – Articles 55-58.

The Data Protection Officer (DPO) is a person with specialised qualifications, particularly expertise and experience in the field of personal data protection. This role is intended to serve as the main link between the organisation processing personal data and all data subjects, in terms of providing information and ensuring the realisation of legal rights. Additionally, the Data Protection Officer serves as the primary point of contact for collaboration between the organization and the Data Protection Authority. The general and fundamental task of this role is to ensure that the organisation processes personal data in accordance with the law.

The Serbian Commissioner

In response to the question of whether a Data Protection Officer working in a real estate agency needs a specific certificate or registration with the Data Protection Authority, the Commissioner held that the PDPL does not specify the type and level of professional qualifications that a Data Protection Officer must possess, nor does it require their appointment to be based on possessing a specific certificate. However, the appointed individual must be capable of fulfilling their obligations under the PDPL.¹

¹ *Protection of personal data: Positions, opinions and practice of the Commissioner, publication no. 8, Belgrade, 2023. Case number: 073-14-991/2022-02, pp. 71-73 [in Serbian]*



10.9.3.1. When is there an obligation to appoint a Data Protection Officer?

The PDPL establishes the obligation to appoint a Data Protection Officer for controllers and processors in the cases when:

- 1) the processing is carried out by a public authority or body, except for courts acting in their judicial capacity;
- 2) the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or
- 3) the core activities of the controller or the processor consist of processing of special categories of data pursuant to Article 17(1) or personal data relating to criminal convictions and offences referred to in Article 19 of the law, on a large scale.

This means that public authorities – including state authorities, territorial autonomy bodies, local self-government units, public enterprises, and other legal or natural persons exercising public powers – are required to appoint a Data Protection Officer. For instance, institutions such as the Health Insurance Fund, Pension and Disability Insurance Fund, ministries, public utility companies (water, heating, roads), as well as all others falling under the definition of public authorities according to the PDPL, are obligated to appoint a Data Protection Officer.

The question arises as to which controllers or processors' activities require regular and systematic monitoring of a large number of data subjects. This question holds practical significance, as the answer determines the obligation to appoint a Data Protection Officer. Consequently, there is a risk of legal penalties if a controller should have been appointed but hasn't been in accordance with the law. The PDPL does not provide specific examples of activities that constitute regular and systematic monitoring of data subjects.

Guidelines

According to the Guidelines of Article 29 Working Party on Data Protection Officers, confirmed by the EDPB, **regular monitoring** is ongoing or occurring at particular intervals for a particular period; recurring or repeated at fixed times; constantly or periodically taking place.¹ **Systematic monitoring** is occurring according to a system; is pre-arranged, organised or methodical; is taking place as part of a general plan for data collection; is carried out as part of a strategy.

The Guidelines provide that the obligation to appoint a Data Protection Officer also exists when it comes to an entity whose core, essential (not ancillary) activities involve the processing of special categories of data or data related to criminal convictions and offenses, on a large scale. Thus, it must be a core activity necessary for achieving the goals of the data-processing entity.

¹ Article 29 WP, Guidelines on Data Protection Officers ('DPOs') (wp243rev.01), as last revised and adopted on 5 April 2017, pp. 8-9



Examples of regular and systematic monitoring include telecommunications operations, data- and location tracking-based marketing, etc. Telecommunications operators, internet service providers, cable television service providers, banks, etc., are entities that would need to appoint Data Protection Officers.

Dilemmas

The PDPL does not specify the term “large scale” in the processing of personal data. The Guidelines of the Article 29 Working Party on Data Protection Officers state that it refers to processing that concerns a large number of data subjects and that the assessment takes into account the extent and nature of the processed data, the duration of processing, and the geographical extent of processing activity.

Examples of processing activities on a large scale may include insurance companies, hospitals, or healthcare centres regularly processing data of a significant number of patients – hence, such entities would need to appoint a Data Protection Officer. Conversely, if it's a small medical practice with only one doctor, it wouldn't be considered processing on a large scale, and such a practice would not need to appoint a Data Protection Officer, unless it chooses to do so voluntarily.

Therefore, not every controller or processor is obliged to appoint a Data Protection Officer, but nothing prevents them from doing so. Appointing a Data Protection Officer is highly beneficial for an organisation, primarily because it ensures comprehensive handling of personal data protection matters within the organisation, ensures lawful processing, identifies poor practices, educates employees, and more. In essence, the organisation will have greater confidence in compliance with its legal obligations regarding data processing if it has appointed a Data Protection Officer.

Controllers and processors that appoint a Data Protection Officer can do so through an internal decision, and in that case, they have to publish the contact details of the Data Protection Officer (e.g., on their website or through other appropriate means). As the Commissioner maintains a register of Data Protection Officers, the organisation that designates a Data Protection Officer must notify the Commissioner using the provided record form available on their website.⁷⁷

The PDPL allows for the possibility of appointing a joint Data Protection Officer and specifies that a group of economic entities can designate a joint DPO, provided that this officer is equally accessible to each group member. However, a single data-processing organisation, regardless of its size and complexity, can appoint only one DPO, not multiple individuals.

The Serbian Commissioner

In order to provide a systematic explanation of the rules concerning Data Protection Officers, the Commissioner has dedicated a special publication to this topic, freely available on their website.¹ Among other things, this publication clarifies several issues related to implementation.

¹ Commissioner, Frequently Asked Questions Regarding the Data Protection Officer, Version 1.0 of 12/31/2019 [in Serbian]



- The PDPL does not determine the form and type of document regarding the appointment of Data Protection Officers; it can be a job description, an individual act, or a contract. The PDPL also does not require controllers/processors to submit a “formal” decision to the Commissioner regarding the appointment of the DPO.

⁷⁷ Data Protection Officer records template, <https://shorturl.at/huwGV>. [in Serbian]

- Informing the Commissioner about a Data Protection Officer should include information about the controller/processor (name, address) and the Data Protection Officer (name, address, email, and phone number). The notice is submitted to the Commissioner in writing, in person, by paper mail, or email at licezazastitu@poverenik.rs. The PDPL does not prescribe a specific form for providing this information, so it can be done in a free form. Importantly, personal address or private phone number of the Data Protection Officer should not be disclosed.
- Controllers/processors are obliged to appoint only one Data Protection Officer and publish their contact details. However, this does not exclude the possibility of forming a team of data protection experts to support the designated Data Protection Officer for organisational or practical reasons. Moreover, the obligation to provide the Commissioner with contact details applies only to the appointed Data Protection Officer and not to any other individuals who assist this officer in their duties.
- Legal entities cannot be designated as Data Protection Officers.
- A Data Protection Officer can be an employee of the controller/processor or perform their tasks based on a contract, which does not necessarily need to be an encumbrance contract but must comply with labour and employment regulations, as well as the specific activities of the controller in question. There are no restrictions on designating a lawyer as a Data Protection Officer, but it cannot be a law firm since it's a legal entity.
- There are no barriers for a foreign citizen and/or a person without residence in the territory of the Republic of Serbia to be appointed as a Data Protection Officer if they can effectively perform tasks defined by the PDPL.
- The designation of a Data Protection Officer can be changed through an appropriate internal act of the controller/processor, which needs to be announced and promptly reported to the Commissioner, along with the contact details of the new Data Protection Officer for registration.
- A Data Protection Officer could perform other tasks and fulfil other responsibilities, but the controller/processor must ensure that the execution of these tasks and responsibilities does not lead to a conflict of interest for the Data Protection Officer.

10.9.3.2. Position of the data protection officer

Relevant provisions: *GDPR* – Article 38; *PDPL* – Article 57.

The Data Protection Officer can be employed within the organisation that appointed them, but it is not necessary; collaboration can also occur, for example, on a contractual basis.

In addition to appointing a DPO, it is essential to determine their position. To that end, the PDPL provides specific obligations:

- The controller and the processor shall ensure that the data protection officer is involved, properly and in a timely manner, in all issues which relate to the protection of personal data.
- The controller and processor shall support the data protection officer in performing legal tasks by providing resources necessary to carry out those tasks and access to personal data and processing operations, and to maintain their expert knowledge.
- Controllers and processors are required to ensure the independence of the DPO in performing their duties.

The law also regulates the relationship between data subjects and DPO's. The Data Protection Officer serves as a key point of contact for all data protection-related matters. Data subjects can address the DPO for questions regarding the processing of their data and the exercise of their rights prescribed by the law. Additionally, the Data Protection Officer is obligated to maintain the confidentiality of data obtained in the course of their duties.

Guidelines

The recommendations of Article 29 WP regarding the position of the Data Protection Officer emphasize the crucial importance of early involvement in all data protection processes. Furthermore, the Data Protection Officer should:

- participate regularly in meetings of senior and middle management;
- be present during decision-making processes related to data protection;
- be promptly consulted once a data breach has occurred.¹

¹ Article 29 WP, Guidelines on Data Protection Officers ('DPOs') (wp243rev.01), as last revised and adopted on 5 April 2017, pp. 13-14



The Data Protection Officer is accountable to the controller/processor for failing to fulfil their duties. The extent of their responsibility depends on whether they are an employee or perform duties based on an engagement contract outside of an employment relationship. However, the DPO is not liable for the obligations of controllers/processors stipulated by the PDPL, considering that their role concerning compliance with controller/processor actions is primarily advisory. Consequently, as a rule, they cannot be held responsible instead of the controller/processor for actions contrary to the provisions of the law.

10.9.3.3. Tasks of the data protection officer

Relevant provisions: *GDPR* – Article 39; *PDPL* – Article 58.

The law explicitly lists the duties of the Data Protection Officer:

- to inform and advise the controller or the processor and the employees who carry out processing of their legal obligations pursuant to data protection provisions;
- to monitor compliance with PDPL, other laws and policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits;
- to provide advice where requested as regards the data protection impact assessment and monitor its performance;
- to cooperate with the Commissioner, serve as a point of contact for cooperation with the Commissioner, and consult with them regarding processing matters, including notification and seeking opinions.

10.10. Employees

In the context of each processing of personal data by employees within the organisation's business domain, it can be assumed to occur under the organisation's control, making it the controller. Employees are generally not considered controllers but rather “individuals authorised by the controller or processor to access personal data”⁷⁸

Dilemmas

Who are “employees” for the purposes of the personal data protection legal framework?

Neither the law nor the GDPR specifically define employees, but within the definition of third parties, they refer to persons authorised to process personal data under the direct authority of the controller or processor. The EDPB Guidelines on the concepts of controller and processor note that “persons who, under the direct authority of the controller or processor, are authorised to process personal data” include not only employees but also persons otherwise engaged in a work relationship status very similar to employment.¹ According to Serbian labour regulations, this seems to encompass relationships based on contracts for temporary and occasional work, volunteering agreements, professional training agreements, temporary work transfer agreements, and agreements on rights and obligations of directors.

¹ EDPB, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, 7. 7. 2021



However, practice in Serbia also includes cases where individuals are engaged to perform specific tasks involving personal data processing based on service contracts, as well as engagements of individuals in the status of entrepreneurs for the same type of tasks. Such relationships, by their nature, differ from employment, possessing a higher level of autonomy. Thus, it remains uncertain whether such an engaged individual could qualify as the person authorised to process personal data under the direct authority of the controller or processor solely based on the fact that their engagement contract stipulates that the tasks are to be performed under the direct authority of the client. In the local context, when determining the existence of direct authority by the controller, the test of independence introduced by the Law on Personal Income Tax 2020 can be used.² Although this test is legally relevant exclusively for establishing the non-independence of an entrepreneur from the client within the scope of tax law, it provides nine relevant criteria that can also be considered when determining the existence of “direct authority”

The practical significance of assessing that direct authority does not exist in relation to a specific individual is that the individual cannot be considered an employee but a service provider. Accordingly, in the context of personal data protection, individuals who participate in data processing under orders, without direct authority, are to be treated as processors by the controllers.



² Law on personal income tax

Employees have a duty to respect the employer's instructions, internal procedures, as well as the broader legal framework within their work. While the relationship between employees and the employer should be based on mutual trust, violations of data protection laws by employees can lead to financial, operational, regulatory, reputational, and other costs for the employer.

Actions by employees in relation to personal data processing operation that result in the infringement of individuals' rights potentially make the employer liable for breaching the legal framework for personal data protection. Additionally, if damage occurs to property or as injury to individuals, liability regarding claims for compensation lies with the employer.⁷⁹ However, the employer can be relieved of liability if they can prove that the employee acted properly under the given circumstances

The liability of an employee is not governed by the legal framework for personal data protection but by labour law.⁸⁰ If an employee causes harm to a third party in connection with the performance of their work duties and breaches data protection, the employee will usually be held indirectly responsible. This is because

⁷⁹ Law on Obligations, Art. 170

⁸⁰ Labor Law, Article 163, https://www.paragraf.rs/propisi/zakon_o_radu.html. [in Serbian]

the employer will be obliged to compensate the third party for the damage, while having the right to seek reimbursement from the employee for the amount paid for the damage. The Law on Obligations allows for the possibility that the injured third party can directly claim compensation from the employee, but only if the employee caused the damage intentionally. However, in practice, it is more common for the injured party to approach the employer, who then internally resolves this relationship, considering that, according to the Labour Law, the employee will be obligated to reimburse the employer for the amount paid for the damage intentionally or through extreme negligence caused to a third party in the course of or in connection with work, which the employer has compensated for. The term “third party” can also refer to another employee at the same employer, not just an individual outside the employer's domain. This way, the responsibility of an individual who has access to the data of other employees and abuses their position can be determined.

The basis for the obligation to compensate for damage does not necessarily have to be the existence of the tortfeasor's criminal liability; it can also be their civil liability. Thus, the Serbian Supreme Court of Cassation has ruled that the absence of criminal liability of the defendant does not exempt the tortfeasor from civil liability for compensating the damage caused to another person.⁸¹

Dilemmas

Can an employer be relieved of liability for injuries caused by the actions of a malicious employee?

In a case before the Supreme Court of the United Kingdom, a question arose regarding the malicious behaviour of an employee in relation to the processing of personal data of employees within a supermarket chain.¹ The employee, a senior auditor, was responsible for transmitting the company's payroll data of around 126,000 employees to its external auditors. As a retaliation after recent disciplinary proceedings, he copied the data from his work laptop to a personal USB stick and then uploaded the personal data of 98,998 colleagues to a publicly-accessible file-sharing website under a fake account. He also sent this file anonymously to three UK newspapers purporting to be a concerned citizen who had found it online. The newspapers did not publish the data. However, the supermarket chain, as the data controller, became the target of legal claims by employees who suffered non-material and material damages due to the publication of their personal data, and who demanded compensation.



¹ Trilateral Research, Personal data protection breaches and employer liability, 22. 4. 2020

81 Judgment 204/2016, of February 23, 2017, <https://www.vk.sud.rs/sr-lat/prev-2042016-zakon-o-radu-gra%C4%91iansko-pravna-odgovornost-krivi%C4%8Dna-odgovornost-i-pravo-naknadu-%C5%A1tete>. [in Serbian]

The question posed before the court was whether an employer could be vicariously liable for data breaches caused by rogue employees, even where the employer had taken appropriate measures and reasonable care to comply with their data protection obligations. Contrary to the Court of Appeal, the Supreme Court found that the employer was not vicariously liable. Since the online disclosure of the data was not part of the employees' field of activities and was not an act which he was authorised to do, but rather a result of his personal vendetta, the employee's wrongdoing did not occur in the ordinary course of his employment. Accordingly, the employer was not vicariously liable.

An employee can become a data controller if, by exceeding the authorities they possess, they decide to process personal data that they have access to within the organisation for their own purposes. However, it is not entirely certain whether in this case the organisation as the initial data controller could absolve itself of responsibility towards third parties, even if it had previously implemented appropriate technical, organisational, and personnel measures, including training and informing employees about handling personal data. Nevertheless, a data controller who is able to demonstrate that timely and adequate organisational and personnel measures have been taken has the opportunity to reduce risks regarding reputational damage and legal liability, as well as to manage other challenges in business.

Trusted resources

As part of the SMEDATA project, a self-assessment and awareness-raising tool has been developed, recommending appropriate measures within the organisation based on relevant criteria, in order for small and medium-sized enterprises to build trust with their employees or clients, as well as internal mechanisms for their implementation.¹



¹ SMEDATA Self-Assessment and Awareness Tool

10.11. Organisational and personnel measures

Relevant provisions: *GDPR* – Articles 24 and 32; *PDPL* – Articles 41 and 50.

Relevant court decisions emphasise the importance of implementing appropriate preventive and reactive measures to mitigate the risks of employee misuse. These measures enable data controllers, acting as employers, to monitor, assess, and enhance the level of compliance with the legal framework for personal data protection, both within the organisation and in relation to external parties such as consumers and service providers. Depending on the size of the organisation and the scope of processing, data controllers are required to:

- ensure that employees are fully aware of their duties and contractual obligations regarding confidentiality;

- provide adequate training on data protection and regular data protection reminders;
- establish policies for identifying, reporting, and managing incidents related to personal data;
- establish mechanisms for employees and external parties to confidentially and securely raise concerns and complaints regarding data protection;
- establish roles and responsibilities for managing operations related to the processing of personal data;
- conduct regular audits.

Practice

The Romanian data protection authority has fined a leasing company 15,000 EUR for failure to implement appropriate measures, resulting in a data breach affecting 436 customers.¹ Namely, the leasing company organised a competition on Facebook to attract potential clients, but inadvertently posted a document that granted access to the data of hundreds of clients. Following an investigation, the competent authority found that the leasing company had not implemented adequate technical and organisational measures.



¹ GDPR Hub, ANSPDCP - Fine against Proleasing Motors SRL

The Danish data protection authority has imposed a fine on a vehicle insurance sales company.² The company created a portal that allowed clients access to all documents related to their case, including those for which access had not been authorised. Around 340 documents submitted by other parties in the process, witnesses and staff, contained personal data such as contact information, witness statements, payment details, and other personal information. After conducting an investigation, the Danish authority determined that the data controller company lacked an appropriate access authorisation system and had not conducted necessary and effective testing to identify the error that enabled access to the documents.



² GDPR Hub, Datatilsynet (Denmark) - 2021-441-10244

Data controllers and processors should divide responsibilities between themselves, require individuals within the organisation who have access to personal data to undergo specific training and education, establish internal policies defining disciplinary measures for employees who breach rules of handling personal

data, and more. Authorised individuals within data controller and processor organisations who access data should do so in accordance with internal rules and instructions, use specific technical measures such as access codes, or, if the data is in physical form, ensure certain individuals have keys to unlock safes where the data is stored, and so on. Additionally, one organisational measure could involve prohibiting employees from accessing business data containing personal data from personal computers and copying such data onto personal computers. If such data is stored on USB drives, a mandatory measure could be the use of access codes on the USB, as the loss of an unprotected USB could compromise the stored data.

These organisational and personnel measures primarily apply to employees within data controller and processor organisations, but they should also apply to all other individuals who have access to this data, such as external consultants and others.

Aligning business processes with the legal framework for personal data protection is not a goal but an ongoing process. Initial compliance is just the first step, but it does not mean that the work of the data controller or processor ends there. As circumstances and facts related to personal data processing change, previously adopted legal policies, procedures, and documents need to be adjusted. Additionally, once-implemented organisational and personnel measures can become ineffective as technology develops, necessitating the replacement of these measures with others that are more suitable and appropriate.

10.12. Continuous internal education

One way for an organisation to remain compliant with the PDPL is to ensure that employees are continuously educated regarding the protection of personal data. In order for employees to understand and apply internal procedures and policies related to the protection of personal data, continuous education is necessary. Since almost anyone working in a specific organisation comes into contact with personal data, it is desirable for all employees to undergo training on personal data protection. If this is not feasible, the priority is to educate employees who are most involved in the processing of personal data in their roles (for example, financial, legal, HR departments) and those who handle customer relations (such as sales, marketing/PR departments, event organization departments, etc.).

Employees who are educated in the field of personal data protection, even if the education involves understanding only the most basic concepts, will help the organisation avoid breaches of the data it processes and sanctions for unlawful processing.

While the law does not explicitly prescribe an obligation for data controllers and processors to educate their employees on personal data protection, employees without basic knowledge on this topic can lead to violations of the law.

Practice

The Romanian supervisor issued 100,000 EUR fine against a bank for unlawful disclosure of personal data and inadequate education of its employees that were sharing certain personal data of a bank client among themselves using their business emails.¹ One of the employees took a photo of the email containing the data with their phone and shared the photo on WhatsApp. Eventually, the client's personal data ended up on Facebook. The leaked data belonged to the client and a few employees and included their names, email addresses, business phone numbers, job titles, business addresses, and other information.

The supervisor deemed that the data sharing violated the principles of integrity and confidentiality set by the GDPR and demonstrated the inefficiency of the data controller (the bank) in educating its employees about personal data protection. In other words, the data controller had not taken sufficient measures to ensure that its employees processed data in accordance with the data controller's requirements.



¹ GDPR Hub, ANSPDCP - *Fine against Banca Transilvania SA*

10.13. Service providers

Modern organisations are typically unable to independently perform all functions necessary for their operations. Small and medium-sized enterprises, especially at their start, face significant capacity limitations and are forced to hire third parties as service providers for various business functions. Large corporations also often opt for restructuring processes that involve the engagement of external service providers for specific areas of business (outsourcing). For instance, organisations of all types frequently hire IT companies to perform certain services such as network development and maintenance, storage systems, database management, and the like. In these cases, it is highly likely that IT companies will have access to personal data processed by organisations, such as employee and client data, and therefore, the contractual relationship with them must include provisions regarding personal data protection.

10.13.1. Software services

If an organisation orders customised software to meet its needs or purchases a license for an existing software solution, the first step is to determine whether personal data will be collected and processed within the software application. If this is the case, the organisation is obliged to consider its relationship with the software provider, the company engaged in software development and maintenance, and to regulate the relationship in accordance with personal data protection rules.

When the software used by an organisation involves processing personal data (collecting, storing, analysing data, or performing other processing operations),

it should be developed in compliance with the PDPL/ GDPR, which practically means that it should protect users' personal data and their right to privacy. This implies that in the course of the software development process, attention is given to incorporating certain measures to safeguard the security of personal data. It is particularly important to implement the principles of privacy by design and by default, as well as individual technical, organisational, and personnel measures, which include, among others:

- ensuring the processing of minimal data (the principle of minimization);
- enabling pseudonymisation and encryption of personal data, applying other technical measures throughout the processing, and allowing the controller to enhance security measures (the principles of integrity and confidentiality);
- providing the ability to manage privileges and roles and implement other organisational and personnel measures;
- offering the ability to control how data is processed, access it, delete it, etc., in order to fulfil individuals' rights. Additionally, software applications should be developed to inform data subjects that their data will be collected and processed and enable them to provide informed consent for processing where required, to withdraw it easily, etc.;
- enabling the right to data portability from the developed software application to another data controller or software application (right to data portability).

It is particularly significant to establish whether, in a specific case, a software development and maintenance company holds a role in the processing of personal data. If the software provider is involved in processing operations due to circumstances such as the software application being hosted on their infrastructure, storing personal data, managing processing tasks on client orders, and similar actions, then this software provider will have the status of a data processor.

When software is handed over to the organisation to install on its own infrastructure and to independently manage processing operations, the software provider likely will not have any interaction with the data processed by such software and will not have a role in accordance with the legal framework for personal data protection. In this case, it is important to include in the basic software procurement agreement that the software provider ensures the implementation of the principles of privacy by design and by default, as well as adequate technical, organisational, and personnel measures for that type of software.

10.13.2. Storage and maintenance services

Companies that provide data storage services, including hosting and cloud computing services, in line with the legal framework for personal data protection, qualify as data processors given that operations related to data storage and making personal data accessible constitute processing. Similar reasoning applies to companies maintaining IT infrastructure on behalf of other organisations

or providing regular and emergency software maintenance services – these companies, in fulfilling their duties, will often have the right to access client's personal data, which constitutes a processing activity and designates them as data processors.

In these cases, IT companies hold the role of data processors, and therefore, the organisation as the data controller is required, among other things, to:

- conclude a data processing agreement defining the responsibilities of the data controller and data processor regarding processing;
- verify if the IT services company engages sub-processors and, if so, request the data processor to demonstrate regulated relationships with them in accordance with the data processing agreement;
- demand that the data processor implements adequate technical, organisational, and personnel measures within their organisation;
- require the data processor to establish internal policies regarding informing the data controller in case of a breach of personal data under processing, as well as demonstrate the capacity to take measures to minimize the negative effects of such a breach.

10.13.3. E-commerce services

If an organisation is engaged in e-commerce, depending on the size of the business, it may process significant amounts of personal data as a data controller. For instance, this could include data necessary for setting up a user account for individuals wishing to make online purchases, data regarding physical addresses for delivery or if the organisation hires a third party as a courier service, financial data used for product payments, data on online behaviour and visitor preferences on the website (via cookies), and the like.

If the organisation employs third-party services to manage orders and payments, it is essential to ensure that the services of such third parties and the tools used by their applications are in compliance with the PDPL / GDPR. Furthermore, companies involved in e-commerce often entrust the physical delivery of goods to courier services. Whenever an e-commerce data controller engages third parties for specific services (payment, delivery, etc.), it's necessary to ensure appropriate contracts are in place (typically data processing agreements between controller and processor). If the business involves processing a substantial amount of personal data, the organisation should consider appointing a Data Protection Officer.

10.13.4. Professional management and consulting services

When an organisation engages accounting services providers, tax consultancy, financial advisory, and similar entities, the question arises regarding the role these assume within the legal framework of personal data protection. The qualification of these entities determines the distribution of roles concerning the processing of personal data and legal obligations in relation to the data subjects.

Guidelines

In accordance with the Opinion of Article 29 Data Protection Working Party on the concepts of controller and processor, the qualification of an accountant in terms of their role in data processing depends on the context.¹ In a situation where an accounting agency provides services to clients based on general instructions (“please file taxes for my company”), the accounting agency will then be considered a data controller. However, when a company engages an accounting agency and provides detailed instructions for conducting auditing services, such an agency will act as a data processor due to the detailed instructions it follows and the limited scope of services provided in accordance with the client’s request. If the hired accounting agency uncovers any unlawfulness or misuse during the auditing process, it will have a legal obligation to report it. In this case, it becomes a data controller as it has a professional obligation to act independently as a controller.



¹ Article 29 Data Protection Working Party, *Opinion 1/2010 on the concepts of ‘controller’ and ‘processor’*, 16. 2. 2010

According to the Guide of the UK supervisory authority ICO, when a company engages an accountant to maintain their books, the accountant is a controller in relation to the personal data in the accounts. This is because accountants providing professional services work under a range of professional obligations that oblige them to take responsibility for the personal data they process (for example, the accountant may be required to report the detected malpractice and in doing so, an accountant would not be acting on the client’s instructions but in line with their own professional obligations and therefore as a controller in his own right).⁸² It seems that a similar principle applies to other providers of professional services as well.

The Serbian Commissioner

If an auditing and accounting company operates independently and autonomously in providing services for which it is hired, and if it in any way determines the purpose or manner of processing, or if the purpose or manner of processing is regulated by law, then that company would be considered a data controller in relation to the processing of personal data. On the other hand, if such company acts according to client instructions and processes data while providing services to the client in accordance with a contract concluded with the client, thereby fulfilling its contractual or legal obligation, then that company is considered a data processor for that specific processing.¹



¹ *Protection of personal data: Positions, opinions and practice of the Commissioner, publication no. 6, Belgrade, 2021. Case number: 073-14-2406/2019-02* [in Serbian]

82 ICO, What are ‘controllers’ and ‘processors’?, <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/controllers-and-processors/what-are-controllers-and-processors/>

Lawyers processing personal data of their clients typically act as data controllers, as they independently decide on the manner of processing in the client's interest as part of client representation.

For instance, when you hire a lawyer with a general instruction to handle your divorce, establish a company for you, or represent you in a dispute, the lawyer will decide how to process your data (determine the purpose and manner of processing) – thus, they will be a data controller in relation to the personal data of their client. Additionally, lawyers have certain professional obligations that may involve processing client data (cooperating with relevant authorities, police, courts, etc.), so they may also act as data controllers in this context. On the other hand, a lawyer can be a data processor when the client provides clear and precise instructions to process data on behalf of the client, so that the lawyer has no control over the data and does not determine the purpose and manner of processing. For example, a client engages a lawyer solely to review a draft contract with an individual user and asks the lawyer to process the user's personal data solely for the purpose of reviewing the draft contract, after which the client requests the lawyer to delete that contract from their computer or internal network.

The Serbian Commissioner

Considering that providing legal assistance in line with the Serbian Legal Profession Act encompasses various activities within the legal profession, such as providing oral and written legal advice and opinions, representing and defending natural and legal persons, as well as performing other legal assistance tasks on behalf of and for the account of domestic or foreign natural or legal persons, the Commissioner has taken the position that the capacity in which a lawyer operates in a specific case of personal data processing depends on the specific service for which the lawyer is engaged to provide legal assistance and can only be determined after establishing the relevant circumstances of the specific case. When a lawyer processes personal data of their employees or clients, they have the role of a data controller in relation to that data. Additionally, a lawyer is usually an independent data controller when processing personal data of third parties while representing them before courts or other authorities, taking into account the autonomy and independence of the legal profession as a service. In terms of other forms of legal assistance, the possibility cannot be excluded that a lawyer may act as a joint data controller or data processor in relation to a specific data processing activity.¹

¹ *Protection of personal data: Positions, opinions and practice of the Commissioner, publication no. 6, Belgrade, 2021. Case number: 073-14-1921/2019-02, pp. 56-58 [in Serbian]*



10.14. Cooperation with the Commissioner

Relevant provisions: *GDPR* – Article 31, Recitals 124-138; *PDPL* – Article 49.

Cooperation with the Serbian Commissioner and European supervisory authorities in the exercise of their powers is a duty of data controllers, data processors, and their potential representatives. The Commissioner oversees the

application and enforcement of the Serbian Personal Data Protection Law by data controllers, legal entities, and individuals through the Supervision department, i.e., authorised personnel of the Commissioner. Authorised personnel of the Commissioner contact data controllers through their representatives or legal representatives. The most common form of communication between the Commissioner and data controllers is through contact between authorized personnel of the Commissioner and the designated data protection officer of the data controller,⁸³ if such an officer is appointed. Otherwise, representatives of the data controller are often individuals from the administrative-legal department of the data controller or hired externally (e.g., qualified lawyer, IT specialist, etc.).

Controllers and processors should strive to establish the best possible cooperation with the Commissioner's office, consult them when needed, and keep track of the Commissioner's website and review their opinions and decisions, as it will be of great assistance in the process of compliance with the law, as well as in the monitoring and demonstration of compliance.⁸⁴

Cooperation between data controllers, data processors, and the Commissioner may involve a range of obligations established by the legal framework for personal data protection.

Examples of duties of data controllers and data processors toward the Commissioner		
Duty	Requirement	Deadline
Making processing records available	Upon request	No deadline, as soon as possible
Notification of personal data breach with all available information about the incident	If the breach is likely to result in a risk to the rights and freedoms of individuals	Within 72 hours of becoming aware
Seeking the Commissioner's opinion regarding personal data processing, including providing the Commissioner with additional information relevant for decision-making and all available information about assessed risks	If the impact assessment indicates that the intended processing activities would result in a high risk to the individuals' rights and freedoms without risk-mitigating measures	Prior to commencing the processing activities
Notification of appointment of the data protection officer and provision of DPO's contact details	Appointment of the data protection officer	Immediately after appointment
Consulting with the Commissioner on matters related to new forms of self-regulation (codes of conduct, certification, binding corporate rules)	Establishment of new forms of self-regulation	Prior to establishing new forms of self-regulation

83 Personal Data Protection Law, Articles 56–58

84 The Commissioner's website: www.poverenik.rs. [in Serbian]

Thus, there are regular and extraordinary situations in which the controller contacts the Commissioner.

Regular situations are those in which the controller fills in the checklist provided by the Commissioner according to the regular supervision plan, as well as in the case when the controller wishes to perform a self-assessment and fill out the checklist themselves,⁸⁵ or voluntarily calls for supervision in case they have any doubts regarding their compliance with the PDPL. Additionally, data controllers contact the Commissioner by registering via email for training sessions periodically organized by the Commissioner's office.

Extraordinary situations arise when the Commissioner becomes aware that the data controller potentially committed a violation (through complaints of citizens, publicly available sources, notification of a personal data breach submitted by the data controller themselves as provided by Article 52 of the PDPL). In extraordinary situations, prior to conducting an extraordinary on-site inspection, the Commissioner gathers information related to potential irregularities concerning the processing of personal data. If suspicions persist, the Commissioner communicates with the controller through correspondence, seeking clarification on the reported allegations, inquiring whether specific personal data processing is being conducted in a certain manner, requesting details about the legal basis for processing (PDPL, Article 12), and the purpose of processing. If doubts persist that processing is being conducted in a manner contrary to the law, an extraordinary inspection is initiated. Authorised Commissioner's personnel conduct an on-site inspection to establish facts, identify irregularities, and determine corrective actions, if applicable. In cases where there is a minimal risk to the rights and freedoms of individuals in relation to the processing of personal data, the Commissioner issues a warning, pointing out the irregularity and providing a deadline for the data controller to address it. However, if the processing is conducted without a legal basis, a decision on temporary or permanent restriction of data processing by the data controller is issued by the Commissioner.

Data subjects have the right to file a complaint with the Commissioner if they believe that the processing of their personal data is not in accordance with the law. The exercise of the right to file a complaint does not prevent the data subject from initiating other administrative or judicial proceedings. The Commissioner is obligated to inform the complainant about the progress and results of the complaint procedure, as well as their right to initiate administrative proceedings against the Commissioner's decision within 30 days of receiving the decision. Therefore, data subjects have the right to initiate administrative proceedings against a decision by the Commissioner concerning them, and initiating administrative proceedings does not affect their right to initiate other legal protection proceedings.

85 Commissioner, Checklists, <https://rb.gy/6xseg> [in Serbian]

11. Citizens' rights

Following the model of GDPR, the PDPL defines a range of rights that data subjects have, with the obligation of the controller to ensure their enforcement. If the data controller does not comply with these rights or fails to respond lawfully to requests for their realization, data subjects have various legal remedies and recourse. First and foremost, these include the right to file a complaint with the Commissioner and the right to sue in court.

The realisation of these rights in practice can lead to the transformation of entire business models of certain data controllers, especially those whose operations are primarily based on the processing of personal data (like technology and telecommunications companies, internet-based companies, etc.).

As for processors, they are obliged to assist the data controller in realising the rights of data subjects, such as implementing appropriate technical and organisational measures, resources, and means, to the extent these activities are under their control within the scope of data processing entrusted to them by the data controller.

Trusted resources

The SHARE Foundation has prepared a publication dedicated to the rights of data subjects: "My Data, My Rights". This publication is particularly useful for citizens unsure how to exercise their rights, providing concrete advice and guidelines, and it is freely accessible.¹

¹ Guide to GDPR and personal data protection "My data, my rights" (D. Krivokapić et al., SHARE foundation, 2018) [in Serbian]



11.1. Exercising rights and Transparency

Relevant provisions: *GDPR* – Articles 12-14, Recitals 58-62; *PDPL* – Article 21.

The procedure and deadlines for exercising all rights are regulated by the provisions of the law, and they are the same regardless of the type of request for exercising rights. In order for this process to go smoothly and be completed within the designated deadlines, a recommendation for controllers is to have

internal rules and procedures ready in advance for how their employees should handle requests for exercising any of the rights. The controller can make a request form publicly available (for example, on their website), which citizens can use to exercise their legal rights.

The Serbian Commissioner

In one of their decisions, the Commissioner has explained the details of the procedure for exercising individuals' rights.¹ A request to exercise rights related to the processing of personal data is addressed to the controller, i.e., the natural or legal person, or the authority that processes the data. The controller is obliged to respond to the request within 30 days from receiving the request. This deadline can be extended for additional 60 days if necessary, taking into account the complexity and number of requests. The controller must inform the data subject about the extension of the deadline and the reasons for such extension within 30 days from receiving the request.

¹ *Protection of personal data: Positions, opinions and practice of the Commissioner, publication no. 6, Belgrade, 2021. Case number: 073-14-1980/2020-02, pp. 78-79 [in Serbian]*



If the controller does not comply with the request of the data subject, they are obligated to inform that individual promptly, and at the latest within 30 days from the date of receiving the request, about the reasons for non-compliance, as well as the right to file a complaint with the Commissioner or a lawsuit in court. Therefore, if the controller, within the legally prescribed deadline, does not comply with the request of the individual to exercise rights related to the processing of personal data, or if, upon receiving information, the individual believes that the processing of their data has been contrary to the law, that individual can file a complaint with the Commissioner or a lawsuit in court.

The Commissioner has drafted and published on their website a text of the request form for exercising rights related to the processing of personal data, as well as a special form for requesting rights related to the performed access that citizens can also use to exercise their rights.² Complaints are submitted to the Commissioner in writing, directly or by paper mail, and can also be submitted as a scanned copy of the complaint to the email address: pritzba@poverenik.rs.

² Forms are available on the Commissioner's website [in Serbian]



The controller is obligated to provide all prescribed information to the data subject in a concise, transparent, understandable, and easily accessible manner, using clear and simple words, especially when it concerns information intended for a minor. The form and manner in which the information will be

provided depend on the specific circumstances. The PDPL in this regard is not exclusive, mentioning both written and electronic forms, as well as the possibility of providing information orally (provided that the identity of the individual is clearly established). However, the rule is that information must be provided electronically (if possible) when the individual has submitted the request in that manner, unless the requester asks for the information to be provided in a different way.

Exercising rights related to the processing of data concerning a minor belongs to the child's legal representative, i.e., the parents when exercising parental rights jointly, or to a single parent to whom the child has been entrusted for sole care by a court decision.

The fundamental rule is that the controller provides information free of charge. However, if an individual's requests are vexatious and clearly unfounded, especially if they are repetitive, the controller has the right to refuse them or to charge for processing the request, where the burden of proving that the request is unfounded and excessive rests on the controller.

The Serbian Commissioner

Is it possible to stipulate in a bank's internal policy, pertaining to the processing of personal data, that unfounded and excessive requests may be charged or refused, especially if they are frequently repeated? The Commissioner has taken the stance that if an individual's request is obviously unfounded or excessive, particularly if the same request is repeatedly made, the controller may: 1) charge necessary administrative costs for providing the information or processing the request; 2) refuse to act on the request. Such provisions in the controller's internal policy are not contrary to the PDPL rules.¹

¹ *Protection of personal data: Positions, opinions and practice of the Commissioner, publication no. 6, Belgrade, 2021. Case number: 073-14-1199/2020-02, pp. 79-80 [in Serbian]*



11.2. Right to information

Relevant provisions: *GDPR* – Articles 13-14, Recitals 11, 39, 57-60, 63-64, 73 and 166; *PDPL* – Articles 22-24.

The right to information is a derivative of the transparency principle. The law explicitly lists the information that the data controller must provide to the individual before even starting the processing. The list of mandatory information is found in Articles 22 and 23 of the law and varies depending on whether personal data is collected directly from the data subject or from a third party.

Information to be provided	Personal data are collected from the data subject	Personal data are collected from third parties
Purpose of processing	✓	✓
Legal basis for processing	✓	✓
Identity of the controller	✓	✓
Contact details of the controller	✓	✓
Contact details of the data protection officer (if appointed)	✓	✓
Recipients of the personal data (or categories of recipients)	✓	✓
Transfer of data to third countries	✓	✓
The legitimate interests (if specified as a legal basis) pursued by the controller or by a third party	✓	
Types of data being processed		✓

The PDPL also requires the controller to provide additional information to ensure fair and transparent processing. This obligation again depends on the source from which the personal data was collected.

Information to be provided	Personal data are collected from the data subject	Personal data are collected from third parties
Retention period	✓	✓
Rights of the data subject to access, rectify, and erase, as well as rights to restrict processing, object to processing, and to data portability	✓	✓
Right of the data subject to withdraw consent	✓	✓
Right of the data subject to lodge a complaint with the Commissioner	✓	✓
Existence of automated decision-making, including profiling, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.	✓	✓
Existence of legitimate interest of the controller or a third party if specified as a legal basis		✓
Source of personal data and, if necessary, whether the data originates from publicly available sources		✓

The law does not prescribe how the controller ensures the right to information, leaving it up to the controller to determine the most appropriate means. In practice, the simplest way to exercise the right to information is through a privacy policy or a data processing notice, which should contain all processing-related details as prescribed by the law.⁸⁶ Such external privacy policy should be written in simple language, avoiding legal jargon, understandable to an average reader. When writing a privacy policy, a balance should be struck between the requirement for the document to be concise (as an overly lengthy document may be skipped) and the obligation to include all information mandated by the law.

Trusted resources

The SHARE Foundation has prepared a tool for creating simple privacy policies. Answer a series of questions, and based on your responses, the privacy policy generator will create a draft containing the necessary elements as per the PDPL.¹



¹ Privacy Policy Generator [in Serbian]

Companies typically publish their privacy policies online, on their websites. However, the data controller can make the privacy policy available in various other ways. For example, if the controller wishes to inform their employees internally about the data being processed, they can do so by posting the privacy policy on a notice board, sending it via email, making it available on the intranet, or using another suitable method. The level of transparency and the extent of content in writing the privacy policy are at the discretion of the controller. However, it is recommended to be as open, relevant, and clear as possible, considering the average data subject. The controller should always keep in mind the need to provide information in a manner that the data subject understands the scope and effects of such processing, so that the processing does not come as a surprise to them.

Guidelines

The Article 29 Working Party issued Guidelines on Transparency, which have been endorsed by its successor, the EDPB. These Guidelines provide detailed recommendations to controllers regarding aspects to consider when fulfilling the right to information.¹



¹ EC - Article 29, *Guidelines on Transparency under Regulation 2016/679 (wp260rev.01)*, 22. 8. 2018.

86 A free tool that can help controllers draft their privacy policy in line with the new personal data protection rules: SHARE Foundation, Personal Data Toolkit, <https://gdpr.mojipodaci.rs/home>. [in Serbian]

One of the complex issues in this context is finding the right balance between the requirement for information about relevant processing to be complete (so that no important information is concealed) and providing that information in a clear and concise manner (instead of long and incomprehensible privacy policies). The proposed resolution to this tension is the “layered approach”, which involves providing a summary in the first layer – consolidated information about key processing aspects, such as purpose, controller's identity, and data subjects' rights – and allowing the data subject in the second layer to read more detailed information about specific processing segments of particular interest. The technical solution for such an approach should be user-friendly, clear, and intuitive, rather than misleading and complicating users' access to desired information.

Dilemmas

What is the difference between good and bad transparency practices?

Bad and non-transparent practice:

“We may use some of your personal data to develop new services and conduct research.”

It is unclear which specific new services are meant and what kind of research is involved. Additionally, the phrase “we may use” creates ambiguity as to whether the data will actually be processed for these purposes, as well as which specific categories of data will be processed.

Good and transparent practice:

“We will collect and process data about products you have purchased through our website in order to send you email suggestions for similar discounted products that we believe might interest you.”

In this case, it is clear which types of data will be processed and that direct marketing for specific products will be conducted based on the individual's profile, involving data processing for this purpose.

What is the significance of a consent to a privacy policy?

Companies' websites often provide an option to visitors to consent to the privacy policy by clicking a designated button. However, such consent holds no legal weight. A privacy policy represents the manifestation of the controller's obligation to inform the data subject about data processing, regardless of whether the individual has consented to this method of notification. What matters is that the data subject is informed about the processing-related circumstances; consent is not a requirement. Some companies might believe that securing consent to the privacy policy makes them safer. However, such consent holds no legal significance and should not be confused with consent as a legal basis for processing, which must meet a set of legal criteria to be legally valid.

The law provides for certain situations in which the data controller is not required to inform the individual about processing. These are situations in which the individual is already aware of processing information, or if providing such information would be impossible or require a disproportionate amount of time and resources, as well as in other exceptions defined by law.

Once published, a privacy policy (or other manifestation of the right to information) needs to be regularly updated to fully reflect the processing-related circumstances as they change.

Practice

The French supervisor imposed fine of 50 million EUR on Google following a complaint for violations of citizens' rights on multiple grounds. The complaint was filed on behalf of users by two organizations, "None Of Your Business" (NOYB) and "La Quadrature du Net" (LQDN), with LQDN representing 10,000 citizens. After an investigation, it was found that Google had violated multiple rights of its users, particularly the right to information. It was assessed that the information was not easily accessible on Google's website as it was scattered across various locations, presented incoherently and non-transparently, and certain information was unclear or incomplete. Due to these reasons, the consent that was intended to be the legal basis for processing was not lawful, as one of the fundamental conditions for valid consent is that it must be sufficiently informed, meaning that the individual must clearly understand what they are consenting to based on the available information.¹



¹ GDPR Hub, CNIL (France) - SAN-2019-001

The Dutch supervisory authority fined TikTok Inc. 750,000 EUR for making its privacy policy available exclusively in English to Dutch users, many of whom are children under the age of 16, thereby violating their right to information. Despite the fact that the process of giving consent when creating TikTok accounts was in Dutch, the supervisor held that from mid-2018 to mid-2020, the privacy policy was only available in English. The data controller did not take into account the characteristics of its audience and did not provide information in an understandable manner.²



² GDPR Hub, AP (The Netherlands) - TikTok

11.3. Right of access

Relevant provisions: *GDPR* – Articles 15, 16 and 20, Recitals 59, 63, 64 and 68; *PDPL* – Articles 26-28.

The right of access is a fundamental right of individuals whose data is processed, enabling them to understand how and why their data is processed and to verify whether their data is being processed lawfully. The data subject have the right to demand from the controller:

1. confirmation as to whether or not personal data concerning them are being processed,
2. access to the personal data,
3. a copy of the data, and
4. the right to receive certain information about the processing at any time, which largely overlaps with the information that the data controller must disclose without a specific request before commencing processing, as part of the right to information (including information about the purpose of processing, types of processed data, recipients of the data if any, retention periods, the right to rectify incomplete or inaccurate data, etc.).

A specific component of this right is the right to a copy: the data controller is obliged to provide the data subject, upon request, with a copy of the data being processed, either electronically or in paper format. In this case, the data controller may request a fee for the necessary costs of producing additional copies, if such costs exist. The data controller should also ensure that the exercise of the right to receive a copy does not compromise the rights and freedoms of other individuals (such as intellectual property rights or business secrets).⁸⁷

The Serbian Commissioner

A complainant submitted a request to a banking institution to exercise their rights regarding the processing of personal data, seeking copies of data related to a previously concluded loan agreement, along with supporting documentation. This included the loan repayment plan, analytical cards for the relevant loan agreement's debits and credits, analytical cards for potentially calculated and charged penalty interest, as well as analytical cards for fees and commissions. In response to the request, the bank provided the complainant with a letter stating that, in accordance with the stance of the National Bank of Serbia and current regulations, the bank is only obligated to provide documentation for active loan agreements, and no such obligation exists for liquidated credits.

⁸⁷ In 2016, the SHARE Foundation conducted research on the processing of geolocation data by electronic communications operators, with a proposal on how service users can obtain a copy of this type of their data from the operator; *Who's allowed to know where you were last summer*, 16. 6. 2016, <https://resursi.sharefoundation.info/sr/resource/share-istrazuje-ko-sme-da-zna-gde-ste-bili-proslog-leta/> [in Serbian]

The National Bank of Serbia's interpretation of the provisions of the Law on Protection of Financial Services Users and the Personal Data Protection Law led to the conclusion that not providing contractual documentation that the client had already received from the Bank when concluding the loan agreement does not contradict the client's right to be informed, since the client was obligated to diligently safeguard their copy of the contractual documentation. Accordingly, for liquidated credits where the contract is no longer in effect, the bank is not obligated to provide the contractual documentation.

The Commissioner found the complaint valid because the bank did not provide the complainant with a copy of the requested data related to them, which the bank undoubtedly continues to process in its data collections, as there are no justifiable reasons to limit this right under Article 40 of the law. The bank's assertion that the National Bank of Serbia's stance on providing copies of contracts according to the Law on Protection of Financial Services Users pertains only to existing contractual relationships and not to terminated contracts, and that the bank had already provided the complainant with her copy of contractual documentation upon contract conclusion, was not relevant to the Commissioner's decision. This is because the individual whose data is being processed has the right to request a copy of the data related to them from the data controller, regardless of whether a copy of the same data can be obtained through another legal basis or whether it involves an active business relationship or not. Additionally, the Commissioner emphasized that the individual whose data is being processed is not obligated to specify the purpose for which they need the data or to provide evidence for it. Finally, the Commissioner ordered the bank to provide the complainant with a copy of the documentation containing her data related to the loan agreement, along with supporting documentation, within eight days, ensuring the protection of third-party data before providing the information.¹

¹ *Protection of personal data: Positions, opinions and practice of the Commissioner, publication no. 7, Belgrade, 2022. Case number: 072-16-1129/2021-6, pp. 98-101 [in Serbian]*



In case the data controller from whom an individual requests the right of access has a data processor that holds personal data, or processes data on behalf of the data controller, and the data controller does not have direct access to the data (for example, data is stored on the processor's IT infrastructure), then the data controller is authorised to request the necessary information from the data processor and, if necessary, the data controller can ask the processor to provide a copy of the data.

Guidelines

The EDPB guidelines on the right of access outline how data controllers should proceed when receiving a request for access to personal data from the data subjects.¹

¹ EDPB, Guidelines 01/2022 on data subject rights – Right of access



Specifically, if it is not explicitly stated which data the individual is requesting access to, the request should be understood as encompassing all personal data that the data controller processes about that specific individual. In cases where the data controller processes large amounts of data, the data controller may ask the data subject to specify the scope of the request. Upon receiving an access request, the data controller will need to search through its IT and physical systems (such as physical files) to locate the requested data, prepare it, and provide it to the data subject.

The data controller should provide the data and other relevant information about the processing in a concise, transparent, understandable, and easily accessible manner, using simple and clear language. If the requested data is encrypted, the data controller should provide an explanation to ensure that the provided data makes sense to the data subject. The controller may deliver the information, for instance, via email, so that the data subject can easily retrieve it.

Practice

A question arose before a Dutch court regarding the extent to which Uber is obligated to provide its drivers with access to data used for calculating earnings, assigning jobs, and suspending drivers.¹ In deciding the case, the court had to consider various categories of personal data and assess for which categories Uber must enable the right of access. These categories included driver profiles, user comments, start and end locations of service, individual driver ratings assigned by users, pricing systems, and more. The significance of this decision lies primarily in enhancing the understanding of the scope and categories of personal data processed within “sharing economy” platforms and finding ways to grant drivers access to specific data categories without compromising the rights of service users.²

¹ GDPR Hub, Rb. Amsterdam - C/13/687315 / HA RK 20-207

² Dutch court rules on data transparency for Uber and Ola drivers



The Serbian Commissioner

The data subject filed a complaint against a healthcare institution for a breach of the right of access to data, stating that the data controller did not fully comply with the request by failing to provide a copy of a decision made by the director of the healthcare institution regarding its employees. The Commissioner found the complaint to be unfounded as the director’s decision does not constitute personal data,

while in exercising the right related to the processing of personal data, a data subject can only access data that pertains to them.¹

¹ *Protection of personal data: Positions, opinions and practice of the Commissioner, publication no. 6, Belgrade, 2021. Case number: 072-16-705/2020-06, pp. 49–50 [in Serbian]*



11.4. Right to rectification and completion

Relevant provisions: *GDPR* – Articles 16 and 19, Recitals 59 and 65; *PDPL* – Articles 29 and 33.

The right to rectification and completion is directly related to the principle of accuracy. Every data subject has an unconditional right to rectify inaccurate and to complete incomplete personal data. This right is particularly important because once personal data are collected, their accuracy is often not maintained, which can pose significant practical problems and lead to consequences for the data subject. Controllers might make decisions based on inaccurate or incomplete information (for example, a competent government authority might decide to lower or discontinue social benefits due to inaccuracies in data exchange between government agencies). As a rule, it is up to the individual to prove that certain data are inaccurate or incomplete, and to do so, it is necessary for the controller to grant them access.

Upon receiving a request for rectification and completion, the controller is obligated to inform all recipients of the data about the changes that arise from the request, unless it is impossible or would require excessive time and resources.

Example

An individual applies for a loan from a bank, but the credit bureau does not have updated information about their current employment and the fact that they now have higher income than before. This could result in the bank rejecting their loan application. If the information about their current employment had been updated, the bank would have approved the loan request.

Practice

The Spanish supervisor fined a bank 25,000 EUR for significantly delaying the processing of a request for rectification of personal data. Three years after the data subject informed the bank about the change of their address, the bank was still using the old one. The data subject requested the correction of the address on two occasions. In the first response to the request, the bank asked the individual to submit the request via a specific email address, while in the second response, it requested additional information to enable the change. Finally, the bank informed the individual that the request had been forwarded to a specialised department for implementation.

As it turned out that the request had not been fully addressed, the individual initiated proceedings with the Spanish supervisory authority. The supervisor determined that the address had not yet been corrected in all documents related to the data subject and imposed a monetary fine on the bank, taking into account the time that had passed since the submission of the request for rectification of personal data.¹



¹ GDPR Hub, AEPD (Spain) – PS-00183-2022

11.5. Right to erasure

Relevant provisions: *GDPR* – Articles 17-19, Recitals 59, 65-67 and 73; *PDPL* – Article 30.

The data controller is obliged to erase personal data without undue delay in the following cases:

- the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed, i.e., the purpose has been achieved or has ceased;
- the data subject withdraws consent on which the processing is based, and there is no other legal basis for processing;
- the data subject objects to the processing and there are no legitimate grounds for the processing overriding the interests, rights, and freedoms of the data subject, or the data subject objects to the processing for direct marketing purposes when the cessation of processing is mandatory;
- the personal data have been unlawfully processed, meaning there was never a legal basis for processing;
- the personal data have to be erased for compliance with legal obligations to which the controller is subject;
- the data were collected from a child in connection with the use of information society services based on the child's consent. Special protection for data collected from children is crucial, especially in the online environment, as such data can be easily exploited. This applies even when the individual is no longer a child but was a child at the time of giving consent, as they may not have been fully aware of the potential risks of data processing at the time of consenting

To strengthen the right to erasure primarily in the online environment, and generally, if the data controller has publicly disclosed personal data, their obligation is also to take all reasonable measures in accordance with available technologies to

inform other data controllers processing such data about the request for deletion of all copies of this data and provide directions or electronic links to this data.

Guidelines

According to the Guide issued by the UK supervisory authority ICO, if a valid erasure request is received and no exemption applies, the data controller have to take steps to ensure erasure from backup systems they possess, which will depend on the technical means available to the controller. It may be that the erasure request can be instantly fulfilled in respect of live systems, but that the data will remain within the backup environment for a certain period of time until it is overwritten. The controller have to be clear with data subjects as to what will happen to their data when their erasure request is fulfilled, including in respect of backup systems. The even if the data cannot be immediately overwritten, the key issue is to put the backup data “beyond use”.



¹ ICO, *UK GDPR guidance and resources - Right to erasure*

There are certain exceptions to this right, when the data controller does not have to comply with the erasure request, which include exercising the right to freedom of expression, complying with legal obligations of the data controller, exercising public health interest, archiving in the public interest, processing for scientific and statistical purposes, as well as for establishment, exercise, or defence of legal claims, etc.

Example

An employee's contract expires, and they send a request for erasure of their personal data to their former employer. However, the employer is legally obliged by the Serbian law regulating labour records to permanently retain a range of personal data of its employees, even after the termination of the employment. Therefore, the employer as the data controller has the right to reject the erasure request because it has a legal obligation to continue processing, which is one of the exceptions to the right to erasure.

During the COVID-19 pandemic, an individual is hospitalised, and the hospital collects certain data about their health status in order to provide adequate health-care. Upon discharge from the hospital, the data subject submits a request to the hospital for the erasure of their health data. However, the hospital has the right to refuse the request because processing such data is necessary for the public health interest, such as protecting against serious cross-border health threats to the population, in this case, the containment of the pandemic.

The Serbian Commissioner

When deciding on a request for the removal of links from the search engine indexing system (“right to be forgotten”), it is necessary to determine in each specific case whether the right to freedom of expression and information outweighs the right to the protection of personal data of the individual concerned.¹ In the specific case, the Commissioner determined that the links, for which removal is requested by the application, lead to newspaper articles containing personal data of the complainant, but in the form of information about their actions as a director of a joint-stock company owned by the Republic of Serbia, a position the complainant still holds, as well as about the business operations of that company, including information related to the budget and spending of the company, the procedure for conducting public procurement and employment in the company, as well as basic information from the complainant's biography and information related to the declaration of assets to the Anti-Corruption Agency by the complainant, which is a legal requirement.

¹ *Protection of personal data: Positions, opinions and practice of the Commissioner, publication no. 6, Belgrade, 2021. Case number: 072-16-1827/2020-06, pp. 92-94 [in Serbian]*



Since the complainant holds a public position and plays a role in public life, and given that the information concerns matters of public interest, such as their actions as a director and the operation of the company, they are inevitably and consciously subject to scrutiny, both by journalists and the general public. Therefore, their right to data protection is narrower compared to other individuals. Considering that the complainant's role in public life, the original content being published for journalistic purposes, the accuracy of the data in the newspaper articles to which the links lead has not been proven to be false, nor has it been proven that the complainant has suffered harm; also, that the data does not concern criminal offenses or special categories of data, and the photographs published in the articles are not biometric data since they were not obtained through special technical processing; and that the complainant is not a minor; and no other criterion exists by which the right to data protection of the complainant could outweigh the right to freedom of expression and information – pursuant to these findings, the Commissioner held that, in this specific case, the public interest in accessing information about the complainant outweighs their right to data protection, and therefore, removing the mentioned links would constitute a disproportionate restriction on the right to freedom of expression.

A data subject lodged a complaint with the Commissioner against their former employer - the data controller, due to a violation of the right to erasure of their email address, as it is personalised and includes their last name. In their response to the complaint, the employer, among other things, emphasised that the mentioned data is not personal data; that the complainant was in an employment relationship with the employer until October 2020 and while employed, used an official email address owned by the data controller; that access to the official email address of the complainant is necessary for the employer to timely fulfil its contractual obligations to business partners

and in accordance with the contract, and to achieve its legitimate interests; that the employer never sent correspondence from the mentioned email address or engaged in any misuse, and that the processing is limited to access in compliance with the principles of processing and in accordance with Article 12 of the Personal Data Protection Law. The Commissioner held that an email address through which an individual is identified or identifiable, directly or indirectly, as in this case, constitutes personal data of that individual. As the employer accesses and retains the official email address of the complainant, they engage in data processing activities. Therefore, since it is an official email address opened and used for the purpose of fulfilling the complainant's obligations related to their engagement with the employer, there is no longer a contractual relationship as the legal basis for processing after the termination of the employment relationship, and the purpose for which the official email address of the complainant was opened has been fulfilled.

In making this decision, the Commissioner considered the employer's claims that they process the email address in question based on a legitimate interest to prevent the harm caused by the complainant's actions. However, the Commissioner found that the conditions for the application of legitimate interest as the legal basis for data processing were not met in this specific case, as the employer did not document or present to the Commissioner a legitimate interest that outweighs the complainant's right to data protection. Processing the complainant's data to prevent harm to the company where the complainant was employed, as indicated by the employer, is not necessary in this specific case, as the employer has other legal means to protect their rights and interests. Therefore, since there is no longer a legal basis for processing the complainant's personal data, specifically, the official email address containing their last name and initial, and the purpose for which the data was processed has been fulfilled, the Commissioner found that the conditions for erasing personal data have been met and ordered the employer to delete the official email address within eight days.²

² *Protection of personal data: Positions, opinions and practice of the Commissioner, publication no. 7, Belgrade, 2022. Case number: 072-16-110/2021-6, pp 82-84 [in Serbia]*



Practice

The Danish supervisory authority rejected the complaint regarding a denied erasure request, as the controller's legitimate interest in retaining the data outweighed the interests of the data subject.¹ The controller was an online platform for selling second-hand goods. The data subject had a blocked user account on the platform and requested the data controller to erase their personal data.

¹ GDPR Hub, Datatilsynet (Denmark) – 2021-31-5439



The data controller refused the request as it had received three independent complaints about the same data subject from other buyers. In order to prevent fraud, the data controller claimed that it needed to retain the personal data of the owner of the blocked account to identify newly opened accounts by the same individual. The lodged complaint with the Danish supervisor was then rejected.

The right to erasure and the right to object were considered by the Court of Justice in the Manni case.² An Italian citizen requested the national commercial register (established in accordance with EU regulations) to erase data, which were about 10 years old at that time, indicating that the data subject had been the manager of a company that had gone bankrupt. The CJEU balanced the individual's right to erasure against the public's right to know, which was protected by the establishment of the commercial register accessible to all interested third parties. In the final conclusion, the Court gave precedence to the right of the public to know, but left the possibility for national regulations to provide rules that after a certain period of time, this public right could be limited, or to comply with the right to object to certain types of data processing. Additionally, the Court did not consider the claims of the Italian citizen that their current job was affected by the fact that all potential clients had access to the disputed information, as a relevant circumstance for the right to erasure and the right to object. In other words, the rights and interests of the individual requesting erasure must be of such nature that they protect more significant values that outweigh the rights of third parties to have access to the disputed information.³

² GDPR Hub, CJEU – C-398/15 – Salvatore Manni

³ EUR-Lex, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce v Salvatore Manni*, 9. 3. 2017



11.6. Right to restriction of processing

Relevant provisions: GDPR – Article 18, Recital 67; PDPL – Article 31.

Situations in which a data subject can exercise the right to restrict the processing of their personal data by the controller are as follows:

- the accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy of the personal data;

- the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead;
- the controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise, or defence of legal claims;
- the data subject has objected to processing pending the verification whether the legitimate grounds of the controller override those of the data subject.

The right to restrict processing provides the individual with the ability to limit how the controller uses their data and serves as an alternative to the right to erasure of data. Therefore, in situations where an individual does not want to erase data (as it is needed for another purpose), they can make this request to the controller. In most cases, controllers will not have to restrict processing indefinitely but only for a specified period.

Since processing can also involve data erasure, it should be emphasised that suspending processing halts nearly all activities related to personal data, including the prohibition of deletion. Logically, in this case, the only permitted processing activity is retention, and the data must not be used or processed in other ways.

If processing is restricted, those data can only be further processed based on the consent of the data subject, unless it involves data retention for the purpose of establishment, exercise, or defence of a legal claim, or for the protection of the rights of others, or for reasons of a significant public interest.

Guidelines

According to the British ICO's Guide, there's a number of different methods that could be used to restrict data, such as temporarily moving the data to another processing system, making the data unavailable to users, or temporarily removing published data from a website.¹

Controllers who receive a request to restrict processing have to consider how they store personal data that they no longer need to process but the individual has requested restriction, effectively requesting that they do not erase the data. If the controllers are using an automated filing system, they need to use technical measures to ensure that any further processing cannot take place and that the data cannot be changed whilst the restriction is in place. They should also note on their system that the processing of this data has been restricted.

If the controller has disclosed the personal data in question to others, they must contact each recipient and inform them of the restriction of the personal data, unless this proves impossible or involves disproportionate effort.

¹ ICO, *UK GDPR guidance and resources - Right to restrict processing*



Practice

The Greek supervisory authority ordered three mobile network operators to suspend (restrict) processing involving the destruction of data related to phone numbers until the supervisor makes a final decision in the case.¹ The data subject received two text messages on their mobile phone, which were intended to lead them to click on hyperlinks through which spyware was installed. The individual submitted requests for the access and restriction of processing against the three controllers – mobile network operators. The supervisor initiated its inspection in relation to this case. One of the controllers responded to the request by providing a copy of the data and stating that critical personal data had already been extracted and provided to the supervisor, and therefore, they cannot be destroyed. The individual lodged a complaint with the supervisor.

The supervisor explained that traffic and location data were generated during the sending of the text messages, and when they relate to a natural person, they are personal data. Also, the deletion or destruction of data constitutes a processing activity. The supervisor has the right to issue a temporary measure and order a complete or partial restriction of processing, in accordance with other relevant Greek national law. Data such as location and traffic data are retained for a period of 12 months, after which they are automatically destroyed, except those for which legal access is provided. Accordingly, the disputed text messages would be destroyed after the expiration of this period. Due to the ongoing inspection, the supervisor prevented the deletion and destruction of this data (restricted processing) until the investigation is completed or a final decision is made.



¹ GDPR Hub, *HDPA (Greece)* - 3/2022

11.7. Right to data portability

Relevant provisions: *GDPR* – Article 20; *PDPL* – Article 36.

The goal of the right to data portability is to enhance the control that individuals have over their personal data and enable data subjects to access their data, reuse it for other purposes through different services, migrate, and transfer data from one online environment to another in a secure manner without negatively affecting the possibility of reusing that data.

In a way, it is an extension of the right of access, as it requires the controller, upon request of the data subject, to provide personal data in a structured, commonly used, and machine-readable format, and the data subject has the right to transmit it to another controller, without hindrance.

The controller must fulfil this request only if the following conditions are cumulatively met: (1) processing is based on consent or on a contract; and (2) the processing is carried out by automated means.

The controller may also be required to directly transmit the data to another controller when such a process is technically feasible.

This right gains particular significance in the online service environment, where an individual has various accounts or profiles, from social media to content streaming services to applications processing sensitive data such as health information (various training and fitness applications). In all these cases, by exercising the right to data portability, a data subject would have the right to request that their data be transferred, for example, to a new social media or a competing platform. In this case, the controller transmitting the data is not responsible for the processing carried out by the data subjects or another controller receiving personal data. Data portability should enable the reuse of personal data if a copy of the data can be transferred in a defined format, hence controllers are encouraged to use interoperable formats to facilitate data transfer between them. For instance, companies within the same industry can create interoperable formats specific to their sector to facilitate easier data transfer.

Example

A data subject has been using the running app X for several years, which tracks their progress, statistics, etc. In the meantime, a more efficient and better running app Y becomes available on the market, and the data subject wishes to switch but doesn't want to lose their progress and statistics. In this sense, the data subject can approach the app X controller to transfer their personal data to the app Y controller and continue where they left off with their statistics.

Similar to the right to copy of data, the PDPL regulates that exercising this right must not adversely affect the rights and freedoms of other individuals.

Guidelines

The UK's ICO explains in its Guide what data transfer in a structured, commonly used, and electronically readable format means. "Structured data" refers to software's ability to extract specific elements of the data. An example of a structured format is a spreadsheet, where the data is organised into rows and columns. In practice, some of the personal data processed will already be in structured form. "Commonly used" means that the format chosen by the controller should be widely used. "Machine-readable" means that the data is in a format that can be automatically read and processed by a computer, allowing software applications to easily identify and extract specific data.



¹ ICO, *A guide to individual rights - Right to data portability*

Practice

A complaint was filed with the Belgian supervisory authority by the data subject who had repeatedly unsuccessfully approached a controller with a request to exercise their right to data portability in the context of switching to a new health insurance fund. The supervisory authority took the stance that three cumulative conditions must be met to exercise this right:

1. The data processing must be based on the consent of the data subject or must be part of the performance of a contract.
2. The processed personal data must be obtained directly from the data subject. Derived or indirectly obtained data fall outside the scope of the right to data portability.
3. The processing is carried out using automated procedures.

The supervisory authority rejected the request and concluded that the data processing conducted by the mutual insurance company is part of a legal obligation incumbent on the controller, i.e., the processing is an extension of a legal obligation rather than contract performance, explicitly excluding it from the right to data portability. Therefore, the first of the cumulative conditions was not met. Furthermore, it was determined that the individual's file also contained, among other things, personal data related to insurance, which are derived data. Hence, the second condition was also not met in this case.¹



¹ GDPR Hub, APD/GBA (Belgium) - 45/2023

11.8. Right to object

Relevant provisions: *GDPR* – Article 21, Recitals 69 and 70; *PDPL* – Article 37.

This right tests legitimate interest or the performance of tasks in the public interest as legal grounds for processing, and it provides the data subject with the opportunity to object to these processing bases.

Upon receiving such request, the controller is obligated to cease the processing of data unless it can demonstrate that there are legal reasons for processing that outweigh the interests, rights, or freedoms of the data subject, or are related to establishment, exercise, or defence of a legal claim.

However, the right to object is absolute when data is processed for the purpose of direct marketing, including profiling. The data subject has the right to object to the processing of their data for this purpose at any time, and the controller must immediately cease such processing, as the controller's interest in conducting direct marketing can never be deemed more important and outweighing the interests, rights, and freedoms of the data subject. Therefore, controllers who send promotional emails or text messages or otherwise contact individuals for the purpose of carrying out marketing activities must provide a mechanism for

complete cessation of such practices as soon as the individual makes such a request (for example, by including an unsubscribe link at the end of an email or similar).

Practice

The Romanian supervisor fined the company Sephora in Romania with 2,000 EUR because it continued to send marketing messages via SMS to an individual after the data subject objected to processing for direct marketing purposes.¹ Even though the individual received confirmation from the controller that processing would stop, they continued to receive promotional messages, after which they contacted the Romanian supervisor. Upon determining that Sephora had continued sending messages despite the objection, the supervisor imposed a financial penalty on the company.



¹ GDPR Hub, ANSPDCP (Romania) – *Fine against Sephora Cosmetics România SA*

The controller is obligated, at the latest when establishing the first communication, to clearly and explicitly inform the data subject that they have the right to object, and this information must be separate from other information provided by the controller. The objection can be made verbally or in writing. In the use of information society services, the data subject has the right to submit an objection through automated means, in accordance with the technical specifications for using the services. Therefore, this pertains to services provided remotely, in an online environment.

11.9. Right to legal remedy

Relevant provisions: *GDPR* – Articles 77-82, Recitals 141-147; *PDPL* – Article 82.

Right to legal remedy entails the possibility of lodging a complaint with a supervisory authority. One of the primary tasks of the Commissioner is to address complaints from data subjects, determine whether a violation of the law has occurred, and inform the complainant about the progress and outcomes of the process. To simplify the filing of complaints, the Commissioner prescribes a complaint form and enables its submission electronically, without excluding other means of communication.

The data subject has the right to lodge a complaint with the Commissioner if they believe that the processing of their personal data is not in accordance with the law. The exercise of the right to lodge a complaint does not prevent the data subject from initiating other administrative or judicial proceedings. In the process of handling complaints, the provisions of the law regulating inspection oversight shall be applied, specifically in the section related to acting on petitions. The Commissioner is obligated to inform the complainant about the progress and outcomes of the complaint process, as well as their right to initiate administrative litigation against the Commissioner's decision within 30 days from the day of receiving the

decision. Therefore, the individual has the right to initiate administrative litigation against the Commissioner's decision concerning them, and initiating such litigation does not affect their right to initiate other forms of legal protection.

Although the right to complain is already guaranteed by the law, if personal data is collected directly from the data subject, the controller or processor has an obligation to provide information about the right to legal remedy, namely the right to lodge a complaint with the Commissioner.

The Serbian Commissioner

A complaint is premature if it is submitted before the expiration of the 30-day period within which the controller was obligated to address the request.

The formality of the complaint is a prerequisite for a substantive decision on the complaint. Specifically, when, for formal reasons, the merits of the complaint cannot be examined, or when it cannot be determined whether there has been a violation of the Personal Data Protection Law by the data controller to the detriment of the complainant, the complaint is dismissed as irregular.

If there is no request submitted based on the Personal Data Protection Law, the complaint is dismissed as irregular.¹

¹ *Protection of personal data: Positions, opinions and practice of the Commissioner, publication no. 6, Belgrade, 2021, pp. 24-28 [in Serbian]*



11.10. Rights regarding automated decisions and profiling

Relevant provisions: *GDPR* – Article 22, Recitals 68, 70-72; *PDPL* – Article 39.

As the processing of personal data increasingly takes place in a digital environment, new European and Serbian regulations recognise responsibility even in situations where machines independently handle personal data, along with complementary rights of individuals. Automated processing of personal data has always been a subject of controversies.

Profiling encompasses three situations: creation of a profile, decision making based on the created profile, and solely automated decision making. Profiling can be performed for various reasons. In the second case, a specific individual makes a decision based on a profile created solely through automated means, while in the last case, the decision itself is made automatically, without any human involvement in the evaluation and verification of the decision. Therefore, automated decision making represents a process using technical means without any human involvement in decision making or its verification.

These data are often sensitive, thus enjoying additional protection. Rights traditionally associated with personal data must be in effect when it comes to automated processing as well, including informed consent, access, rectifying, or

deletion, and all prescribed principles of processing. An individual whose data is used in automated data processing must have the opportunity to express their opinion regarding a specific decision and to seek legal remedies if they believe the decision is not lawful or accurate. For instance, if an insurance company uses an algorithm to decide the amount of an insurance premium, the data subject must be informed, have the chance to express their opinion, potentially challenge the decision, and request a human review of the decision made by the algorithm.

The application of the results of automatic data processing cannot be avoided in three cases: when a decision is made based on a specific law allowing automatic data processing, when automatic data processing is necessary for the conclusion and execution of a legal relationship between the data subject and the controller, and when explicit consent for automated processing has been given by the data subject. For example, in cases of performing certain socially significant tasks aimed at national security and public health protection, automated processing of personal data will be allowed, provided there is a prior specific justification based on legitimate expectations. Furthermore, in the case of announcing a job vacancy with a large number of applicants, the employer has the right to use special software to select a shortlist of candidates based on predefined criteria. It will be considered that candidates have implicitly given consent to automated data processing by applying, as their intention is to enter into an employment relationship with the employer.

Guidelines

The Article 29 Working party issued Guidelines on automated decision-making and profiling holding the view that the rights of individuals apply regardless of whether the individual has actively exercised those rights. In other words, for automated individual decision-making and profiling to be permissible, one of the three stated conditions must be met.¹ As a result, controllers are not recommended to initiate processing involving automated individual decision-making and profiling without meeting the conditions in all cases where decisions produce legal effects or can significantly affect the individual's position.

¹ EC – Article29, *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 (wp251rev.01)*, 22. 8. 2018



When it comes to automated data processing, particular attention should be paid to respecting all prescribed standards of personal data protection – lawfulness, fairness, transparency, purpose limitation, data minimization, accuracy, and data retention periods.

The principle of transparency can be challenged not only because data subjects are unaware of the methods and purposes of processing, but also because they may struggle to understand complex techniques used for profiling and automated decision-making. In this sense, it is essential to provide clear, transparent, easily accessible, and

comprehensible information about the processing of personal data. The Guidelines on transparency by the Article 29 Working Party can also be helpful in this regard.⁸⁸

Special rights that exist in cases of automated processing allow individuals to retain control over their data when only machines and software are involved in their processing. The PDPL provides that the individual has the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning them or significantly affects their position (except in clearly defined exceptions). The legal effects must be substantial, affecting fundamental rights such as the right to assembly and association, voting rights, and the like. Additionally, decisions with legal consequences should include decisions that can lead to contract termination, denial of legally guaranteed assistance, refusal of visas, entry into a country, etc. Decisions that can significantly affect someone's position are those with lasting consequences, capable of leading to discrimination, or influencing an individual's choices and behaviour. Such decisions can impact access to healthcare, credit assessment, labour rights, or the right to education.⁸⁹

Furthermore, the controller is obliged to implement appropriate measures to protect the rights, freedoms, and legitimate interests of individuals. The minimum of these rights includes the right to ensure the involvement of a human under the controller's authority in decision-making, the right of the data subject to express their opinion regarding the decision, and finally, the right of the data subject to contest the decision before an authorised person of the controller.

Automated decisions cannot be based on special categories of personal data, apart from exceptional situations provided for by the law.

Guidelines

According to the proposed regulation of the European Union establishing harmonised rules on artificial intelligence (Artificial Intelligence Act, AI Act), certain artificial intelligence systems will be prohibited.¹ Specifically, the proposed regulation distinguishes four types of risks that may arise from the application of artificial intelligence: unacceptable, high, limited, and low or minimal risk. The proposed list of prohibited practices so far encompasses all artificial intelligence systems whose use is deemed an unacceptable risk as it goes against EU values, such as the protection of fundamental human rights.

¹ Review of all documents created in the process of negotiations on the future law, <https://artificialintelligenceact.eu/documents/>



88 EC – Article 29, *Guidelines on Transparency under Regulation 2016/679 (wp260rev.01)*, 22. 8. 2018, <https://ec.europa.eu/newsroom/article29/items/622227/en>.

89 EC – Article 29, *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 (wp251rev.01)*, 22. 8. 2018, <https://ec.europa.eu/newsroom/article29/items/612053/en>.

The prohibitions relate to practices with the potential to manipulate through the use of subliminal techniques that operate at the subconscious level or exploit specific vulnerable groups, such as children or persons with disabilities, in a way that may cause harm to them or others. Other manipulative practices that impact individuals and that artificial intelligence systems could facilitate are covered by regulations on personal data protection, consumer protection, and digital services that ensure proper informing of individuals and free decision-making regarding profiling, as well as other practices that could influence human behaviour.

11.11. Restriction of rights

Relevant provisions: *GDPR* – Article 23, Recital 73; *PDPL* – Article 40.

Following the model of the GDPR, the PDPL contains rules specifying circumstances under which certain rights can be restricted. This is possible only if such limitations respect the essence of the fundamental rights and freedoms and constitute a necessary and proportionate measure in a democratic society to safeguard: (1) national security, (2) defence, (3) public security, (4) the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security, (5) other important objectives of general public interest, (6) the protection of judicial independence and judicial proceedings, (7) the prevention, investigation, detection and prosecution of breaches of ethics for regulated professions, (8) a monitoring, inspection, or regulatory function connected, even occasionally, to the exercise of official authority, (9) the protection of the data subject or the rights and freedoms of others, (10) the enforcement of civil law claims.

Although the PDPL does not explicitly state that restrictions can only be introduced through specific laws, as specified in Article 23 of the GDPR, it seems that the same principle should apply in Serbian context as well, in accordance with Article 42 of the Constitution of the Republic of Serbia, which stipulates that the collection, retention, processing, and use of personal data shall be regulated by law.

11.12. Citizen requests

The controller should establish procedures and internal rules to promptly respond to the request of the data subject no later than within 30 days of receiving the request, with the possibility of extending this period to 60 days in certain situations (in cases where the requests are exceptionally complex or the controller has received a large number of requests, requiring more time for response).

Whether a request is deemed complex depends on the circumstances of the case and the technical, personnel, and other capabilities of the controller, as what may be complex for one does not necessarily mean it is complex for another controller. For instance, a request may be considered complex if there are technical difficulties

in accessing the required data, or if it involves sensitive data with confidentiality obligations, or if it requires locating data within files containing a vast amount of information, and similar scenarios.

In order to respond to the request, controllers may require identification from the data subject to ensure that personal data of one person is not sent to another. It would be acceptable for them to ask necessary questions to determine if the requester is the data subject whose information the controller processes. However, controllers should exercise strict proportionality, meaning they should only ask as many questions as necessary to establish the identity of the requester for the purpose of successfully responding to the request, and only when the identity of the requester is unknown to the controller. For example, controllers should not request formal identification documents from the data subject if it is not necessary, or if there is an alternative way to establish the identity (such as using a username and password associated with the account on the controller's website or similar means).

Additionally, the controller should have the option to seek clarification from the requester in certain situations – for example, to precisely specify the data to which the request pertains if the controller processes a large volume of data about the requester and the request does not clearly define the exact data being requested.

The fundamental rule is that the controller cannot charge for responding to a request related to the exercise of the data subject's rights; however, there are exceptions. If the request is unfounded, excessive, or repetitive, the controller may charge necessary administrative costs for processing the request (such as costs of copying, postage, equipment like disks, USB drives, etc.) or may refuse to comply with the request. If the controller deems it necessary to charge a fee, they should inform the data subject immediately, so that they are aware of what to expect.

12. Typical situations

Responsibility for complying is one of the core principles of personal data processing. The controller must assess whether the processing of personal data they are conducting is lawful, determine the methods by which they will comply with their legal obligations (which PDPL also largely regulates in principle), and, ultimately, provide evidence that the first two points have been carried out. Processors also have their share of responsibilities, particularly in terms of implementing organisational and technical measures, but often also assisting the controller in all processing matters entrusted to them.

The benefit of this approach lies in providing controllers and processors with a significant margin of freedom to organise their processing operations and align them with legal requirements. Often, there is not just one precise way to achieve compliance with the law, especially in terms of providing evidence of compliance. On the other hand, this task can be challenging for many. The PDPL is written in legal jargon, which is sometimes unclear even to legal professionals without specific knowledge in this field.

Analysing typical situations in which controllers and processors may find themselves will help better understand the legal provisions through everyday experience. Various business processes, observed from the perspective of collecting and processing personal data, can be broken down according to various legal requirements. They are exposed to one of the possible methods of compliance in each typical situation. Addressing all items and various questions that controllers and processors have to answer in order to comply with the law, provides a clearer picture of the lawfulness of a specific processing, and then whether all obligations under the PDPL have been fulfilled.

The selected situations are only examples of typical processing operations in practice, and they do not represent instructions to follow if a controller or processor finds themselves in a similar situation. As illustrations, they also do not represent the unique nor complete method of compliance. For a precise analysis of a specific case, it would be necessary to take into account all its circumstances and specifics.

12.1. Recruitment process

Name of the characteristic (typical) data processing activity

Recruitment process

Description of the characteristic personal data processing situation

A human resources department has developed multiple methods for advertising open positions for which new employees are being recruited. Candidates can

apply directly through the controller's website. Additionally, they can apply via the LinkedIn application by sending a direct message to the HR employee who posted the vacant position on that social media. Furthermore, for specific positions, job ads are posted on employment websites, and in such cases, applications are sent to the email address indicated in the ad.

For certain high-level positions, the employer may engage a recruitment (headhunting) agency.

Mapping of business processes and data flows:

Data collection method

Data is collected directly from individuals, job applicants. For suitable positions, data is also collected from the headhunting agency.

Location and method of storing personal data

Regardless of how the candidate submitted their job application, all data is stored on a shared drive of the human resources department on the Google Workspace platform.

Is the processing internal, or are external service providers (processors) involved in the data processing?

Data from job applications are stored on the Google Workspace platform, which places Google in the role of a data processor.

Who manages the personal data processing activity (department and responsible person)?

The HR department manages the data processing activity. After the initial stages of selection with a shortlist of candidates, managers from the relevant departments where the position is open become involved in the process.

Who has or can have access to the data and under what conditions?

There is a recruitment team within the HR department. Only persons employed in this team have access to job applicants data. All employees within the recruitment team have access to the shared drive, are authorised to post positions on the LinkedIn platform, and one person is responsible for managing the email account of the recruitment department. There is a written internal procedure outlining how data from received applications are stored, used, and deleted, depending on how the application was submitted or received.

Furthermore, there is a recruitment procedure policy that governs the selection rounds. According to this policy, only applications that have passed the appropriate rounds are sent to relevant managers, which also depends on the specific position being filled.

Roles allocation according to PDPL

Data controller

Employer

Joint controllers

For certain positions, a headhunting agency may be involved.

Data processors

Google LLC.

Categories of external data recipients (third parties to whom data is externally transferred)

n/a

Data processing

Processing purpose

Conducting the selection process for hiring new employees for open positions.

Legal basis

Data is collected for the purpose of entering into an employment contract, making the conclusion and performance of a contract with the data subject a legal basis for processing. Candidates who have not passed the selection process can give consent to retain their data for the next three years, to potentially be contacted if a similar position opens.

Categories of data subjects

Job applicants.

Types of personal data processed

Data from resumes submitted, interview notes. Depending on the position, candidates may be tested for English language proficiency or take a test in their field of expertise, with the employer retaining the test results.

Types of special categories of personal data processed

Sensitive data is not processed at this stage of the new employee intake.

Type of processing actions

Collection, storage, categorisation (classification by type of position), search, deletion.

Retention period – deletion deadline and method

Data of candidates who did not pass the selection process are deleted immediately after concluding a contract with the selected candidate(s). Data of individuals who have consented to data retention for potential future selections are deleted after three years.

The deletion deadline (which is defined here, for example, at three years) should be determined considering the purpose of data processing – which means determining after how long the data is likely to become “outdated”, i.e., irrelevant for filling a specific position (among other reasons, due to changes in circumstances and the biography of the specific candidate during that period).

Minimisation

The employer collects only data that is relevant to the specific position. Candidates whose positions do not require it, as well as candidates in the initial stages of selection, are not tested.

Technical and organisational measures

Technical measures primarily relate to standard practices applied to all employees using business computers and HR software, which includes, among other things, using appropriate credentials to access data within the shared drive.

Organisational measures include a structured system of roles and privileges in accordance with the task distribution within the HR sector (not all HR employees have access to candidate data, only those employees working on selection tasks, i.e., in the recruitment team). As part of internal procedures, there is a rule that resumes are not printed except for interview purposes, and all printed resumes are destroyed as soon as the need for their use ceases. Written form candidate tests are destroyed, only the test results for relevant employees are retained.

Citizens' rights

- Notice of processing (right to information) – Candidates must be informed in advance of all information required by the PDPL, including the data retention period. Depending on the method of receiving job applications, it is necessary to find an optimal way to make this information available to interested parties. Prior to publishing the appropriate notice on their website, a good practice is to provide a link to the webpage where the notice is available in all job advertisements or to provide it to candidates during initial communication (e.g., for candidates who applied directly through the LinkedIn platform).
- Right of access and copy

- Right of rectification
- Under certain conditions, the right to erasure and the right to restriction of processing

Other obligations

Data transfer

Third countries data transfer

Since the data is stored on the Google Workspace platform, it is considered transferred (exported) to countries where the corresponding Google servers are located.

Legal basis for data transfer abroad

Considering that the processor exports the data and offers its processor services as a standardized service, in practice, the controller is dependent on the legal basis provided by Google, in case the data is stored in countries that are considered inadequate under the PDPL.

If the controller determines that the proposed legal basis is not appropriate (for example, if Google relies on inadequate standard contractual clauses), they must discontinue the use of these Google services.

Personal data protection impact assessment

n/a

Privacy by design and by default

The principles of privacy by design and by default are reflected in the predefined rules of candidate selection (in the initial stages of selection, only resumes are collected, followed by data from interviews and tests), which adhere to the fundamental principles of data processing and other obligations under the PDPL.

Documentation

In relation to this processing, the employer – controller must have/maintain, at a minimum:

- A record of processing activities
- Contract with the processor (which should be identified and available on the appropriate Google website)
- Documented basis for data export and inadequate countries (which should be identified and available on the appropriate Google website)
- Policy on the implementation of the selection process
- Notice for job candidates

12.2. Required personnel records

Name of the characteristic (typical) data processing activity

Required personnel records

Description of the characteristic personal data processing situation

An employer with a small number of employees, apart from the required personnel records, in accordance with labour laws, does not process additional personal data of employees (no time tracking, access control, performance monitoring, video surveillance, distribution of gifts to employees' children for New Year, Christmas, and the like).

Mapping of business processes and data flows:

Data collection method

Data is collected directly from individuals, i.e., employees.

Location and method of storing personal data

For each employee, a personnel file is created in paper format, which is kept in separate folders in the office of the person responsible for finance and legal matters.

All electronic personnel files and accompanying documentation for each employee are stored on the computer of the person responsible for finance and legal matters.

Relevant data is stored in the software of an external accounting agency for the purpose of salary and other employee payment processing.

Is the processing internal, or are external service providers (processors) involved in the data processing?

Since the accounting is outsourced, the accounting agency is provided with the necessary data for salary and other income calculations, as well as for other accounting services if needed, through the software provided by the accounting agency itself.

Who manages the personal data processing activity (department and responsible person)?

The processing of data is managed by individuals responsible for finance and legal matters, as the controller does not have a separate human resources department.

Who has or can have access to the data and under what conditions?

The individual responsible for finance has access to all data. As needed, the director of the controller also has access to the data. The accounting agency has access to data related to salary calculations, other income, and, if necessary, other accounting matters.

Roles allocation according to PDPL

Data controller

Employer

Joint controllers

None.

Data processors

External accounting agency.

Categories of external data recipients (third parties to whom data is externally transferred)

Relevant state authorities, depending on the purpose of sharing, in accordance with applicable regulations (social security, tax administration).

Upon request and with the consent of the employees, certain data can be shared with banks for obtaining loans and using other banking services.

Data processing

Processing purpose

Maintaining required personnel records for all employees, in accordance with mandatory labour and other applicable regulations.

Legal basis

Employee data is processed based on relevant regulations, such as the Labour Law, Law on Records in the Field of Labour, regulations governing taxes and social security.

Due to the nature of this record-keeping, data is also processed for the conclusion and execution of employment contracts. However, if there is processing of certain data necessary for the execution of employment contracts that is not regulated by laws, it must be specifically identified and separated during data mapping (for example, recording of working hours may be maintained to fulfil employee obligations under the employment contract, but this is not a mandatory processing operation according to positive laws).

Categories of data subjects

All employees. For employees whose family members have dependant health insurance, the employer also processes certain data about those individuals in accordance with applicable regulations.

Types of personal data processed

Within this record-keeping, only data of employees for whom collection is mandatory according to positive laws are processed. All data collected for other (though somewhat related) purposes are treated within their own specific processing operations.

Types of special categories of personal data processed

In labour relationships, it is possible to process, in accordance with regulations: (i) data on employees' religious beliefs (for the purpose of obtaining days off for religious holidays according to the Law on State and Other Holidays in the Republic of Serbia), (ii) health data (for the purpose of regulating sick leave), and (iii) data on union membership (if relevant to the specific employer).

Type of processing actions

Collection, storage, labelling, categorisation, structuring, access, use, sharing, searching, deletion.

Retention period – deletion deadline and method

Labour laws prescribe certain retention periods for specific data, primarily the Law on Records in the Field of Labour. For data without a defined retention period by appropriate regulations, the employer should establish internal rules regarding when specific data from personnel files are deleted. The responsible person ensures that all necessary data is periodically deleted if in electronic form, or appropriately destroyed (shredded) if in paper form.

Minimisation

Within personnel record-keeping, only data that is necessary to be collected for the controller, as an employer, to fulfil its obligations according to labour regulations, is processed.

Technical and organisational measures

Since data is processed in both electronic and paper form, appropriate measures need to be established for both processing methods.

Regarding data processing in paper, it is necessary to ensure limited access to data, i.e., personnel files, typically by keeping them locked in special cabinets or by providing locking mechanisms and restricted access to the room where the files are stored.

For electronic format, since documents are stored on an employee's computer, standard computer protection measures need to be implemented (access passwords, antivirus protection, policies for use of business computers). As data resides on a single computer, it is particularly important to ensure that the computer is used exclusively for business purposes and remains within the employer's premises.

Given the increased risk of accidental data destruction and loss, adequate and regular data backup needs to be ensured.

As data is externally shared with the accounting agency through their software, the sharing process needs to be arranged with the agency. The agency must guarantee appropriate protection measures through a data processing agreement, and the controller must ensure measures on their end (primarily limiting access to the software to necessary personnel, in this case, the person responsible for finance and legal matters, possibly the director, and using the software only in accordance with instructions from the agency).

Citizens' rights

- Notice of processing (right to information) – information about personnel record-keeping is typically included within the notifications for employees (where employees are provided with information about other potential processing activities), hence, there's no need for a separate notification for this processing activity.
- Right of access and copy (also regulated by the Labour Law)
- Right of rectification
- Under certain conditions, the right to erasure and the right to restriction of processing

Other obligations

Data transfer

Third countries data transfer

Data is not transferred outside the country.

Legal basis for data transfer abroad

n/a

Personal data protection impact assessment

n/a

Privacy by design and by default

The principle of privacy by design and by default is reflected in the strict compliance with conditions for data collection for the purpose of fulfilling the legal obligations that the controller has as an employer.

Documentation

In relation to this processing, the employer – controller must have/maintain, at a minimum:

- A record of processing activities
- Contract with the processor (specifically regulating the use of software provided by the processor – external accounting agency)
- Notice for employees

12.3. Video surveillance of employees

Name of the characteristic (typical) data processing activity

Video surveillance of employees

Description of the characteristic personal data processing situation

The employer has installed cameras within the production facility where hazardous machinery is operated, with the aim of monitoring whether employees adhere to prescribed safety measures and workplace protection regulations. Employees found to have violated the measures through video surveillance may face dismissal following a disciplinary process.

Mapping of business processes and data flows:

Data collection method

Data is collected directly from data subjects, i.e., employees, using video surveillance equipment.

Location and method of storing personal data

Data, or recordings that can identify employees, are stored on servers maintained by the employer.

Is the processing internal, or are external service providers (processors) involved in the data processing?

An external service provider is engaged for the maintenance of the video surveillance system, who does not have direct access to the recordings (as it is not necessary for providing their services), but may be granted access if needed for maintenance and technical support purposes.

Who manages the personal data processing activity (department and responsible person)?

The employer has a security department that manages this process. Its users include the security and workplace protection (SWP) department and the HR department.

Who has or can have access to the data and under what conditions?

Employees in the security department are responsible for monitoring the recordings and reporting incidents, granting them daily access, particularly live

access. Upon request, the SWP department and/or the HR department can be given access to the recordings, which would occur in cases of suspected incidents. If an incident is confirmed and a disciplinary process is initiated, other authorised employees, such as the immediate supervisor of the employee involved or the employer's director (depending on the severity of the incident), can also access the recordings. This entire process is regulated by a procedure within the employer's decision on establishing video surveillance.

According to the processing agreement, the processor - service provider - may also have access to the data.

Depending on the case, or specific incident, access may also be granted to relevant state authorities (inspections, courts).

Roles allocation according to PDPL

Data controller

Employer

Joint controllers

None.

Data processors

External service provider for maintenance and technical support.

Categories of external data recipients (third parties to whom data is externally transferred)

As necessary, relevant state authorities and inspections.

Data processing

Processing purpose

The purpose is to monitor compliance with workplace safety and health regulations. Recordings must not be used for any other purposes (e.g., time tracking, performance assessment, etc.), as that would go against the principle of purpose limitation.⁹⁰ According to the Commissioner's opinion, if video surveillance is exclusively aimed at monitoring regular activities and behaviour of employees during working hours for the assessment of employee performance, such processing of personal data is not allowed (indiscriminate surveillance).⁹¹

90 *Protection of personal data: Positions, opinions and practice of the Commissioner, publication no. 7, Belgrade, 2022*, p. 19, https://www.poverenik.rs/images/stories/dokumentacija-nova/Publikacije/7PublikacijaZZPL/ZZPLPublikacija_7.pdf. [in Serbian]

91 *Protection of personal data: Positions, opinions and practice of the Commissioner, publication no. 4, Belgrade, 2019*, p. 23, <https://www.poverenik.rs/images/stories/dokumentacija-nova/Publikacije/Publikacija4ZZPL/4PublikacijaZZPL.pdf>. [in Serbian]

Employees have a right to privacy in the workplace, and any intrusion through video surveillance must be justified. In other words, the purpose of processing must be lawful and permissible, which in this case is demonstrated by the values provided by video surveillance (protection of life and physical integrity, as well as the employer's production process). According to the case law of the European Court of Human Rights, employers can use video surveillance in specific circumstances to protect against theft or fraud by employees.⁹²

Legal basis

The only legal basis available to the employer is legitimate interest, wherein a balancing test must be conducted to demonstrate that in the specific case, the employer's interests as the controller outweigh the interests of the employees.

Employee consent cannot be the legal basis for this processing, as the conditions for free and voluntary consent cannot be met.

Categories of data subjects

Employees working in or present in the production facility.

Types of personal data processed

Recordings that can identify employees.

Types of special categories of personal data processed

n/a

Type of processing actions

Collection, storage, labelling (categorisation based on time and location of recording), searching, copying, deletion.

Retention period – deletion deadline and method

Data is deleted after 30 days. In the event of an incident, recordings may be retained for a longer period, but not beyond the legal statute of limitations.

Minimisation

The angle and number of cameras must be such that they capture only what is relevant to workplace safety and health regulations. To ensure better protection of employee privacy in the workplace, the number and angle of cameras must cover risky areas and actions, fulfilling the purpose (using video surveillance and other

⁹² ECHR, *Case of López Ribalda and others v. Spain*, 17. 10. 2019, [https://hudoc.echr.coe.int/fre#%22itemid%22:\[%22001-197098%22\]](https://hudoc.echr.coe.int/fre#%22itemid%22:[%22001-197098%22]).

evidentiary means) without unnecessarily intruding into employees' privacy (for example, by not continuously capturing their faces, but rather machine operations).

Technical and organisational measures

Technical measures, involving equipment and software used, may include automatic archiving of video materials within specified timeframes, as well as implementing access control to the recordings themselves, both in real-time and for later reviewing. Organisational measures primarily encompass a well-defined system of roles and privileges in accordance with the employer's decision on establishing video surveillance, as well as a confidentiality obligation for all employees accessing the recordings.

Citizens' rights

- Notice of processing (right to information) – employees have to be informed in advance of the purpose and consequences of the processing. It's best to provide this information in a separate notice that is easily accessible, as this concerns a specific processing that doesn't apply to all employees.
- Right of access and copy
- Right to object
- Under certain conditions, the right to erasure and the right to restriction of processing (if the legitimate interest is overturned as the legal basis based on the right to object)

Other obligations

Data transfer

Third countries data transfer

The employer's management is located in Austria, so it's possible to access the data from Austria. Such access is considered a transfer of data outside of Serbia.

Legal basis for data transfer abroad

Austria is considered a country with an adequate level of protection, where data transfer is free (as a signatory to the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data).

Personal data protection impact assessment

It is necessary to conduct a data protection impact assessment in accordance with the Commissioner's Decision on the list of types of personal data processing actions for which a data protection impact assessment must be conducted and to seek the Commissioner's opinion (Official Gazette of the Republic of Serbia, No. 45/19), according to Article 2(7) of the Decision.

Privacy by design and by default

The principles of privacy by design and by default must be respected due to the process's logic, as it's necessary to determine the number and angle of cameras in advance in line with the principles of purpose limitation and data minimisation.

Documentation

In relation to this processing, the employer – controller must have/maintain, at a minimum:

- A record of processing activities
- Contract with the processor
- Policy on the implementation of video surveillance
- Data protection impact assessment
- Grounds for legitimate interest (as a standalone document or within the impact assessment)
- Notice for employees

12.4. Employee productivity monitoring

Name of the characteristic (typical) data processing activity

Employee productivity monitoring

Description of the characteristic personal data processing situation

The controller provides online customer support services for various clients, which are business entities. Employees at the controller are assigned to positions where they interact with end customers of specific controller's clients. For communication purposes and providing customer support, employees use appropriate software – chat applications, either provided by the controller or by the client, depending on the case. For the purpose of assessing employee performance, the employer has the right to access metadata collected through the use of the relevant chat application (collected by the application itself), and under specific conditions, access to the content of the communication.

Mapping of business processes and data flows:

Data collection method

Data is collected from individuals, i.e., employees, based on their behaviour – the use of appropriate equipment, namely, work-related application.

Location and method of storing personal data

Data is stored on the controller's servers, as well as on the servers of controller clients for whose end customers the employees provide customer support services or with the processors of these clients.

Is the processing internal, or are external service providers (processors) involved in the data processing?

The chat application used by the controller is maintained and technically supported by an externally engaged service provider who developed the application upon the controller's request.

Client applications are also typically maintained by various external service providers for various purposes, depending on the specific application (all of whom are considered processors if their service involves any interaction with personal data, including passive storage or hosting of such data).

Who manages the personal data processing activity (department and responsible person)?

The data is used for monitoring employee performance, and the relevant data concerning assigned goals, as well as communication content (for monitoring work quality and resolving incident situations), are primarily managed by the immediate supervisor of the specific employee.

Who has or can have access to the data and under what conditions?

The processing operation primarily involves employees of the controller. Data about work performance and communication content can be accessed by the appropriate supervising manager of that employee. Specific data can also be accessed by persons from the HR department for the purpose of employment contract execution, monitoring of personal development plans for employees, potential disciplinary proceedings, as well as by persons from the finance department for calculating compensation based on work performance (bonuses).

In executing a commercial agreement between the controller and their client, specific data necessary for that purpose can be accessed by authorised persons on the client's side (in accordance with the agreement between the client and the controller), using a specific role and privilege system.

For certain clients, instead of granting access to the application, specialised performance reports containing personal data may be sent.

Roles allocation according to PDPL

Data controller

Employer

Joint controllers

The clients of the controller for whose customers support services are provided.

Data processors

IT service providers who maintain applications used for monitoring work performance and providing technical support, both for the controller and their clients.

Categories of external data recipients (third parties to whom data is externally transferred)

Data may be shared externally in the event of a legal dispute where it is necessary to provide access to either metadata or communication content.

Data processing

Processing purpose

Monitoring employee work performance to determine: (i) whether they have achieved the specified goals within their customer support tasks, (ii) whether they provide customer support in accordance with communication rules with end consumers (monitoring work quality), as well as (iii) tracking whether any complaints from end consumers about the employee's performance are justified (in case of incidents or alleged inappropriate communication with the consumer).

An additional complementary purpose is the execution of contracts that the controller has concluded with their clients.

Legal basis

All relevant data is processed for the execution of the employment contract that the employee has entered into with the employer, which comprehensively regulates the required work performance of the employee in their position.

Sharing data with clients is based on the legitimate interest of the controller in executing the contract with their clients.

Categories of data subjects

Employees working in customer support.

Types of personal data processed

Metadata regarding use of the chat application as a work tool by the employees, as well as the content of their communication with end consumers.

Depending on the case, the types of data collected and processed by the employer may differ from the data shared with the client.

Types of special categories of personal data processed

n/a

Type of processing actions

Collection, storage, structuring, comparison, access, use, sharing, search, encryption, deletion.

Communication content data is generally not monitored, except in two cases: occasionally through random sampling to monitor the quality of work by the controller, or in the event of reporting an incident.

Retention period – deletion deadline and method

All data is deleted in accordance with the statutes of limitations that pertain to labour disputes.

Minimisation

Only the necessary data is collected for the purpose of assessing the performance of a specific employee, depending on the specific client for whom the employee works. This is regulated by the employment contract of the employee or the contract with the respective client.

The application used by the controller has the option to select which types of (meta)data will be tracked, collected, and stored. Client applications are evaluated on a case-by-case basis and are not used if they collect more data than necessary.

In addition to data from the relevant application, the controller does not utilise any other data generated from the business computer provided to the employee for performance tracking.

Technical and organisational measures

The controller's application is provided by a hired service provider in accordance with standard technical security measures for this type of software. Since data is retained for a period after use before deletion, encryption is enabled at regular intervals after the end of relevant accounting periods.

Specific protection measures have been established for data sharing with clients, including measures for secure data transmission.

All those accessing the data are assigned with appropriate rights according to a predetermined system of roles and privileges. Access logs of employee data (metadata and communication content) are also maintained.

Protection measures are specifically governed by contracts with each client, as required and depending on the specific case.

Citizens' rights

- Notice of processing (right to information) – given the specific purpose and method of processing employee personal data, it is recommended to prepare a separate notice about this processing operation. In addition to the mandatory elements of information outlined in the PDPL, employees should also be informed about potential consequences (such as qualifying for bonuses, salary reductions, or potential disciplinary proceedings due to incidents or inappropriate communication with end consumers).
- Right of access and copy
- Right to object (for processing based on legitimate interest)

- Under certain conditions, the right to erasure and the right to restriction of processing (if the legitimate interest as the legal basis is invalidated due to an objection)

Other obligations

Data transfer

Third countries data transfer

Since a large number of employees (or other engaged individuals) of the controller's processor, who maintain its chat application, access data from India, it is considered that the data has been transferred to India.

Data can be transferred to any country where the controller's client or its processors are located.

Legal basis for data transfer abroad

Depending on the case. Standard contractual clauses prepared by the Data Protection Commissioner can be concluded with the controller's processor. If data is transferred to countries that are considered inadequate under the PDPL, an appropriate legal basis must be established, such as codes of conduct, certificates, or special approval from the Commissioner (since there are no standard contractual clauses under the PDPL concluded between two controllers). Before sharing data with clients, the controller must verify and collect evidence that all the client's processors have appropriate legal bases to access data from inadequate countries in case the client's application is used.

Personal data protection impact assessment

It is necessary to conduct a data protection impact assessment in accordance with the Commissioner's Decision on the list of types of personal data processing actions for which a data protection impact assessment must be conducted and to seek the Commissioner's opinion (Official Gazette of the Republic of Serbia, No. 45/19), according to Article 2(7) of the Decision.

Privacy by design and by default

The principle of privacy by design and by default must be strictly adhered to, especially in the initial phases of developing the chat application where employee data is collected and stored. It is important to ensure that the application only collects relevant data and provides the controller with the option to customise the type and retention period of data for each employee individually (to avoid collecting more data than necessary for their respective roles).

The same applies to client applications. If a client requests the use of an application that does not comply with the principle of embedded and default privacy and/or other processing principles, the controller must reject such a request to avoid violating its obligations under the PDPL.

Documentation

In relation to this processing, the employer – controller must have/maintain, at a minimum:

- A record of processing activities
- Contract with the client on joint data processing
- Contract with the processor
- Data protection impact assessment
- Grounds for legitimate interest (as a separate document or within the impact assessment)
- Special notice for employees

12.5. Direct marketing

Name of the characteristic (typical) data processing activity

Direct marketing and conducting promotional activities

Description of the characteristic personal data processing situation

The controller engages in the sale of sports equipment through its extensive retail network and also operates an online store. It is based in Serbia but has a presence in all markets across the region. The controller collaborates with partners such as gyms, sports clubs, hiking societies, and similar organisations, offering special benefits to their members for purchasing products. Marketing and promotional campaigns are conducted through email, text messages, paper mail to physical addresses, as well as targeted advertising to visitors of the online store on their website. The controller also partners with sports clubs that organise training sessions, competitions, and camps for children, and the website has a dedicated section for kids and youth.

Mapping of business processes and data flows:

Data collection method

Depending on the method of conducting promotional activities, data is collected either directly from data subjects who provide their contact information to the controller or through online tracking technologies such as cookies. If data is collected from individuals under the age of 15, their parents or guardians provide the information.

Location and method of storing personal data

Data is stored on the internal server of the controller in Serbia. Contact data (names, email and physical addresses, and phone numbers), depending on the type of promotional campaigns, are also stored by marketing department employees in various Excel spreadsheets on their business computers. Data collected through tracking technologies is stored within the platform on which the online store is hosted.

Is the processing internal, or are external service providers (processors) involved in the data processing?

The entire marketing team is employed by the controller. Processors are only IT service providers, such as the provider of the platform hosting the online store.

Who manages the personal data processing activity (department and responsible person)?

The marketing department of the controller.

Who has or can have access to the data and under what conditions?

The marketing department does not share personal data with anyone within the organisation. The director of marketing has access to all data, and other employees have access based on their involvement in specific promotional campaigns. The director of the controller may also be granted access to the data as needed for their duties, upon request to the director of marketing.

Roles allocation according to PDPL

Data controller

The company engaged in the sale of sports equipment.

Joint controllers

For certain promotional actions, the controller can collaborate with some of its partners, in which case they have the role of joint controllers. The exact allocation of rights and obligations for each specific agreement is determined according to the needs and circumstances of the particular campaign.

For certain online tracking technologies, joint controllers may also be companies whose cookies or trackers the controller has placed on its website (third-party cookies). In this sense, the circumstances that the EU Court of Justice addressed in the Fashion ID case are relevant (see chapter 7.1).

Data processors

The provider of the platform hosting the online store, other IT service providers.

Categories of external data recipients (third parties to whom data is externally transferred)

Data is not shared with third parties.

All partners with whom data is shared, or from whom data is received as part of joint promotional campaigns, are considered joint controllers on that basis.

Data processing

Processing purpose

The purpose of processing is to conduct promotional activities, depending on the type of promotional/marketing campaign. Before initiating any marketing activity, the controller determines the specific goal – promoting a specific product, sending newsletters, informing consumers about the opening of a new retail store, seasonal discounts, etc. Promotional messages directed at children primarily involve various types of event notifications and are not directly aimed at advertising products.

Legal basis

The legal basis is the consent of individuals to receive promotional messages from the controller. This consent is given by actively indicating the desire to receive promotional messages during online purchases, registration, newsletter sign-up, or by providing contact information in retail stores. Regardless of how consent is given, the controller retains evidence that consent has been provided. The same individual may provide separate consents for different types of promotions or opt for only some of them (via text messages, email and physical addresses, only for discounts, or for a specific type of product). Consent also applies to the possibility of receiving messages about joint campaigns with partners. If the data concerns minors under 15 years of age, consent is given by parents or guardians whose children have participated in events organised by the controller.

Consent for online targeted advertising is given within a pop-up window on the controller's website, where individuals can indicate their consent to receive promotional offers through this method. The pop-up window leads to a section of the privacy policy where the process of such advertising is clearly explained, as well as how to withdraw the given consent. Targeted advertising is not conducted on the website segment intended for children and youth, as the controller has assessed that valid consent cannot be obtained in their case, given the inability to determine the age of website visitors and explain to children what obtaining consent from them entails.

Regardless of the market in which activities are conducted (in Serbia or in countries in the region), the same rules for obtaining valid consent apply as in Serbia.

Categories of data subjects

Customers and potential customers of the controller's and partners' products, and visitors to the online store.

Types of personal data processed

Contact data (name, email, phone number, physical address) is collected depending on the type of promotional activities. Unique identifiers and other electronic data collected and used depending on online tracking technologies.

Types of special categories of personal data processed

n/a

Type of processing actions

Collection, access, viewing, use, sharing, analysis, deletion.

Retention period – deletion deadline and method

Since the legal basis for processing is consent, all data is deleted when consent is withdrawn.

Minimisation

Within the stated purposes, only contact data is collected (each data point used for its specific purpose) and electronic data for online tracking.

Technical and organisational measures

Although the processed data is generally non-sensitive, the volume of data controlled necessitates appropriate protective measures. In addition to regular technical computer, server, and platform protection measures for the online store, specific organisational measures have been implemented. These measures apply both within the marketing department, where data access is assigned based on roles and privileges, and within the broader organisation of the controller, ensuring that data is not accessed by anyone from other organisational parts.

Similar measures are required from joint controllers - partners in joint marketing campaigns.

Citizens' rights

- Notice of processing (right to information) – privacy policy, with a special emphasis on the cookie policy
- Right of access and copy
- Right of rectification
- Right to withdraw consent and erasure
- Right to restriction of processing

Other obligations

Data transfer

Third countries data transfer

Considering the global presence of the provider of the platform hosting the online store, data located there can be stored on various servers worldwide.

Legal basis for data transfer abroad

Within the data processing agreement by the provider, if data is stored outside the territory of the European Union, EU Standard Contractual Clauses have been concluded in accordance with EDBP recommendations on measures complementing tools for international data transfers.

Personal data protection impact assessment

In principle, not necessary, but it may be if targeted advertising is carried out in an innovative or intrusive manner.

Privacy by design and by default

Privacy by design and by default are emphasised when deciding how the pop-up window for giving consent to targeted advertising will be presented. It must be developed in line with the principles of fairness and transparency, and must not include design elements that would lead website visitors to reflexively give their consent without reading or understanding what they are consenting to (“dark patterns”). Given that there is a section of the website promoting events and products for children, a special analysis is needed for this segment to elevate default privacy to the highest level, especially in the context of targeted advertising.

Documentation

In relation to this processing, the employer – controller must have/maintain, at a minimum:

- A record of processing activities – within the scope of this processing, it is of utmost importance that all specific purposes within which data is processed for promotional purposes are clearly separated in the records of processing activities, i.e., all different processing operations, according to an appropriate criterion (e.g., type of campaign, communication channel, standalone campaigns or campaigns conducted with partners, etc.). Once all specific processing operations have been listed within the records, the controller needs to ensure that valid and appropriate consent has been obtained for each of them, and that the processing is in line with other principles.
- Contracts with Processors (accompanied by relevant contracts with sub-processors)
 - Contracts of Joint Controllers for each specific campaign
 - Privacy Policy
 - Policies detailing the procedure for exercising the rights of data subjects and the procedure in case of data security breaches (optional but recommended)

12.6. Mobile application

Name of the characteristic (typical) data processing activity

Mobile application for online banking

Description of the characteristic personal data processing situation

For the purpose of online banking, the bank has developed a mobile application for smartphones. In addition to the data related to the execution of contracts and services provided by the bank within the application (accounts, cards, transactions), for which the mobile application serves as an additional means of processing, the application itself collects and processes certain personal data (phone access, location, camera). These processing operations are specific to the mobile application, i.e., the method of conducting transactions, and are neither present nor relevant to other methods (online banking via a computer browser, transactions performed and services provided in the bank).

Mapping of business processes and data flows:

Data collection method

Data is collected indirectly from data subjects, i.e., through the use of the phone, based on the functionality, settings, and permissions on the individual's mobile phone.

Location and method of storing personal data

Data is stored on the controller's servers.

Is the processing internal, or are external service providers (processors) involved in the data processing?

The mobile application was developed by the bank's own IT team. However, from time to time, the bank hires external service providers who may or may not have access to personal data in their performance. However, if there is a possibility for such access (thus, occasionally or even rarely), that service provider is considered a data processor.

Who manages the personal data processing activity (department and responsible person)?

The IT department within the bank manages the process. In terms of the application, roles are clearly divided among superior administrators, administrators, and users involved in technical support tasks.

Who has or can have access to the data and under what conditions?

Except for the IT team, no one has access to the data, except in the case of an incident when access may be granted to relevant individuals who require access for incident response. There is an internal procedure for this within a specific document (policy).

Roles allocation according to PDPLData controller

Bank.

Joint controllers

n/a

Data processors

IT service providers maintaining applications used for online banking and providing technical support both to the controller and its clients.

Categories of external data recipients (third parties to whom data is externally transferred)

Data is not shared with anyone.

Data processingProcessing purpose

The purpose of processing is to enable all functionalities of the mobile application.

Legal basis

The legal basis is the execution of contracts with bank clients who have chosen to use the bank's services through the mobile application.

Categories of data subjects

Clients who have chosen to use the bank's services through the mobile application.

Types of personal data processed

The type of data processed is determined by the functionalities provided by the mobile application. In this regard, there are data that are mandatory for processing as the application cannot function without them, and there are data for which processing is optional. Within the permissions on their phone, users can specify which permissions for accessing certain functionalities they do not wish to grant, thus preventing the processing of relevant data. The data in question are considered personal data as they all relate to a unique user of the mobile application who is a bank client.

For example, camera access may be relevant if the application has facial recognition technology for user authentication, or if the application allows video calls with bank representatives, or if attaching a photo within the application is necessary for a specific service. Location access may be necessary for locating the nearest ATM or branch.

Types of special categories of personal data processed

n/a

Type of processing actions

Collection, access, viewing, use, search, encryption, deletion.

Even though the bank does not retrieve certain data from the user's phone to enable certain functionalities, the fact that it accesses and uses the data for the application's operation qualifies as data processing.

Retention period – deletion deadline and method

The collected data is retained depending on the specific functionality it serves.

Minimisation

Only the data necessary for the application's function are processed as mandatory. If user consent is required for access, they are prompted each time with an explanation of how and for what purpose such access authorisation will be used. All optional accesses can be disabled at any time.

Technical and organisational measures

The application is developed in accordance with the highest security standards applicable in the banking industry. Appropriate encryption methods are applied during data transmission and storage.

Access to data by the bank and possibly external technical support is regulated by an internal act / policy which regulates in detail the issues related to the possible violation of personal data and the management of security incidents. All employees, depending on their position, have regular training and case simulations in which they test the resilience of their systems and procedures.

Citizens' rights

- Notice of processing (right to information) – since this involves specific data processing situationally linked only to the mobile application, a separate notice should be prepared for these specific processes, or a specific section related to this processing context should be highlighted within the general notice; considering that applications are generally downloaded from authorised platforms (such as Google Play, Apple Store), the notice should be easily downloadable from the platform itself and accessible within the application (once installed), as well as readily available on the bank's website.
- Right of access and copy

- Under certain conditions, the right to erasure and the right to restriction of processing

Other obligations

Data transfer

Third countries data transfer

Data is not transferred to third countries. From the controller's perspective, using the application by a client abroad is not considered data transfer to third countries.

Legal basis for data transfer abroad

n/a

Personal data protection impact assessment

DPIA is required in accordance with the Decision of the Commissioner on the list of types of personal data processing operations for which an assessment of the impact on personal data protection must be carried out and an opinion of the Commissioner obtained ("Official Gazette of RS", No. 45/19), particularly if new technology is used for application development or if location tracking is involved.

Privacy by design and by default

Given the sensitivity of the processing at hand and the heightened risks due to the nature and manner of data processing, privacy by design and by default is of utmost importance. Alongside the highest technical standards concerning security and protective measures, attention must be given to minimisation, technical solutions for optimal user notification, retention periods, and ways in which users can exercise their rights. In this regard, during application development, consultation with legal experts is necessary to identify specific legal requirements from the perspective of data protection.

Documentation

In relation to this processing, the employer – controller must have/maintain, at a minimum:

- A record of processing activities
- Contract with processor
- Data protection impact assessment
- Internal policies (or acts) regulating data access, authorizations within the application, incident procedure
- Separate notice for bank clients using the mobile application or distinct information highlighted within the general notice

12.7. Online shop and loyalty program

Name of the characteristic (typical) data processing activity

Customer database, registered users, and loyalty program of the online shop

Description of the characteristic personal data processing situation

The controller is a fruit and vegetable producer and owner of an online shop. Part of the shop's assortment comes from the controller's own production, but goods from other producers are also offered. Customers have the option to make purchases as "guests" without registration, to register and create a profile/account on the store's website, and to enrol in the loyalty program. The loyalty program is agreed upon with all producers and sellers, based on their agreement outlined in a commercial contract or a joint data management agreement. An external agency is engaged to administer the loyalty program, which also handles certain marketing and PR activities on behalf of the controller. The store offers the option of online payment through an external service provider. The online shop is built on the infrastructure or platform of a global service provider for such software.

Mapping of business processes and data flows:

Data collection method

Guest shoppers enter the necessary data for the purchase themselves. Registered users who have also enrolled in the loyalty program, their purchase history and collected points are processed and stored, reflecting their activities within the online shop.

Location and method of storing personal data

Data about guests and registered customers are stored within the platform and backed up on the controller's servers hosted by a hosting provider. Loyalty program participant data is also backed up on agency servers, which are hosted by another hosting provider.

Is the processing internal, or are external service providers (processors) involved in the data processing?

While the management of the loyalty program is entirely entrusted to an agency with expert marketing knowledge, the agency holds the position of a processor. It processes data only based on written instructions from the controller or based on criteria established and defined in the marketing services agreement and data processing agreement. The controllers retain full control over all processing activities and can terminate the contract with the agency and request data deletion at any time. The processors include the hosting provider and the platform provider on which the online store is built.

Who manages the personal data processing activity (department and responsible person)?

The sales department at the controller independently manages the data of customers who are not part of the loyalty program. Data from the loyalty program is effectively processed with the involvement of the marketing agency.

Who has or can have access to the data and under what conditions?

The controller's sales department shares relevant data with the finance department regarding completed payments and the complaints department, and when necessary, with the controller's IT support department. The agency accesses data related to the loyalty program through assigned access rights on the appropriate segment of the online platform.

Roles allocation according to PDPL

Data controller

The owner of the online store is the controller for all processing activities. An external payment service provider holds the role of a controller within the service it provides to both customers and the seller (controller).

Joint controllers

For the loyalty program, all sellers who have concluded relevant agreements for participation in the program are joint controllers.

Data processors

For the loyalty program, the marketing agency acts as a processor. The agency's hosting provider is a sub-processor. The controller's hosting provider and the platform provider on which the store is built are processors for all data.

Categories of external data recipients (third parties to whom data is externally transferred)

Delivery data is shared with courier services responsible for specific product deliveries.

Data processing

Processing purpose

The purpose of processing guest customer data is to fulfil purchase agreements (payment, delivery). Registration's purpose is to provide regular customers who have registered with a more efficient purchasing experience through their user accounts and access to all their transactions and communications conducted

through the platform. Registered users can also voluntarily select favourite products to receive notifications about. The purpose of registration for the loyalty program is participation in the program and utilisation of the benefits it offers.

Legal basis

The legal basis for all the mentioned purposes is the execution of contracts with customers. If customer data is used for any other purposes, such as sending marketing messages, handling complaints, and similar activities, a different legal basis must be established, typically being legitimate interest (for complaints) or consent (for marketing messages). If data is retained after the contract expires, a separate legal basis must be defined, usually legitimate interest for the purpose of pursuing or defending legal claims.

Categories of data subjects

Buyers, whether as guests or registered users.

Types of personal data processed

For guest customers, the platform requires input of name, delivery addresses, email addresses, and contact phone numbers (optional). Registered customers can define a username and password within their account, optionally providing multiple delivery addresses. Within their account, they can access their transaction history, placed but unrealised orders, as well as favourite products. Through their profile, users can directly contact customer and IT support via messages, as well as file complaints, with access to the complaint history. Within the loyalty program, users are assigned an identification number used in each purchase. Data about accumulated and spent points, as well as other benefits received, are stored.

All customers and users are given the option to voluntarily sign up to receive promotional information (via phone or email).

Types of special categories of personal data processed

n/a

Type of processing actions

Collection, access, viewing, usage, sharing, deletion, retention, encryption, anonymisation.

Any data analysis from the customer database, registered users, or loyalty program participants for business analysis or marketing activities would not be possible under the contract execution legal basis and purpose. However, it might be possible, subject to other conditions including transparency, that data could be anonymised based on legitimate interest as the legal basis, for the purpose of conducting analysis on such data (which no longer holds the quality of personal data).

Retention period – deletion deadline and method

All data is generally retained for 10 years, which is the legal statute of limitations period. Data about guest customers, completed transactions, and inactive or deleted accounts are stored in encrypted form for two years.

Minimisation

All data not necessary for the execution of contracts (depending on the type of contract or service provided) is provided voluntarily.

Technical and organisational measures

Technical measures have been provided by the platform service provider, which were confirmed by the controller's IT department before entering into the service and data processing agreements. A secure connection for agency access to the data has been established. None of the joint controllers have direct access to the data since it is not required for executing the commercial agreement. Access is provided as needed through a mechanism regulated in the joint controller agreement. Encrypted data is stored with special protection measures, and access is limited to a small number of individuals within the controller's organisation.

Citizens' Rights

- Notice of processing (right to information) – privacy policy published on the online store's website
- Right of rectification
- Right of access and copy
- Right to data portability
- Under certain conditions, the right to erasure and the right to restriction of processing
- In cases where the legal basis is legitimate interest – the right to object

Other obligations

Data transfer

Third countries data transfer

Given the global presence of the platform provider hosting the online store, data may be stored on various servers worldwide. Under the processing agreement with the provider (concluded upon access by platform users, such as the controller), it is stipulated that user data from EU member states is stored within the EU or in a country from the EU's list of adequacy, while certain data stored in EU countries can exceptionally be accessed from specific Asian countries for the purpose of providing technical support.

Legal basis for data transfer abroad

EU member states are considered countries with an adequate level of protection (as signatories of the Council of Europe Convention for the Protection of Individuals

with regard to Automatic Processing of Personal Data), as well as countries on the EU's list of adequate countries. Any further transfer of data from the EU to Asian countries is governed by appropriate EU standard contractual clauses.

Personal data protection impact assessment

n/a

Privacy by design and by default

Since the online store is built on an existing platform, when customising it to the controller's needs, special attention is required to ensure that all functionalities, online data entry forms, available options, etc., are set up to collect only the necessary data within required fields. Customers must not be prompted to provide more data than the minimum required. It is necessary to clearly indicate which data is optional, and if provided, for what purposes it will be used. This is particularly important within the loyalty program, where customers must not be coerced into revealing more about themselves through any offer of benefits. Registered users should also be provided with greater control over their data within their accounts in a clear (user-friendly) and transparent manner.

Documentation

In relation to this processing, the employer – controller must have/maintain, at a minimum:

- A record of processing activities
- Contracts with processors (accompanied by appropriate contracts with sub-processors)
- Joint controller agreement
- Privacy policy for all categories of customers, with a recommendation for a separate privacy policy for the loyalty program
- Policy that details the procedure for exercising the rights of data subjects and the process in case of a data breach (optional but recommended)

12.8. Big data

Name of the characteristic (typical) data processing activity

Processing data for training for analysis and online content optimisation algorithm

Description of the characteristic personal data processing situation

The company has developed a tool that analyses the behaviour of website visitors interacting with specific written content (media, scientific institutions, news portals) based on various parameters, depending on the users' interests within the

application. The analysis is performed on extensive behavioural data collected from the website with the aim of content optimisation, without the intention to directly profile or target website visitors based on their behaviour. The analysis is conducted using appropriate algorithms and artificial intelligence. The company sells the tool to its clients, offering various functionalities depending on the client's interests (there are standard “service packages” that can be further customised upon special order). Thus, the company is generally acting as a processor, while clients assume the role of controllers. The following analysis is conducted from the company's perspective as a processor, with appropriate notes related to the controller.

Mapping of business processes and data flows:

Data collection method

Data is collected directly from data subjects based on their behaviour on the website (depending on the enabled functionalities of the tool, specific aspects of this behaviour data can be collected, for example, data related to user registration may be analysed, though not necessarily).

Location and method of storing personal data

The processor backs up the data on Amazon Cloud.

Is the processing internal, or are external service providers (processors) involved in the data processing?

In addition to Amazon, the company has hired various service providers in the development and maintenance of the tool, who are affiliated with the company (part of a common group of companies). These providers are assigned different tasks such as client communication, technical maintenance, etc., under an external engagement principle (service agreements have been signed with all of them). This positions them as sub-processors.

Who manages the personal data processing activity (department and responsible person)?

Different organisational units manage the data processing operation at the processor's end, depending on the phase of the entire data processing operation, the type of client, and similar factors. The entire operation is thoroughly documented in records of processing activities, from the data collection phase to deletion or anonymisation.

Who has or can have access to the data and under what conditions?

Access to data at the processor is provided according to a role and privilege system, documented in the form of an authorisation distribution matrix, depending on the data processing phase, responsibilities, and the position of the individuals who have access to the data.

Roles allocation according to PDPL

Data controller

In principle, the controller will be the client who purchased a specific version of the tool or a package with predefined functionalities from the company that created it.

Joint controllers

The tool has specific functionalities that, when integrated into a specific tool package, place the company that created it in a joint controller position with the client, as the data is also used for the further development of the tool itself, i.e., for machine learning.

Data processors

From the company's perspective, Amazon and other external service providers have the status of subprocessors.

Categories of external data recipients (third parties to whom data is externally transferred)

Since the data is processed on behalf of and for the account of the controller, there are no external data recipients. The company guarantees not to share data with anyone where it has a joint controller role.

Data processing

Processing purpose

The purpose of processing is to provide content analysis and optimisation services. Since the intention is not to perform profiling or targeting of individuals whose data is processed, any use of data for such purposes would be considered incompatible.

Legal basis

The legal basis is determined by the controller. In principle, this could be legitimate interests or consent, depending on specific functionalities. The company's task is to provide a technical solution for obtaining such consent at the request of the controller, in cases where consent is the legal basis.

Categories of data subjects

Individuals who visit the websites of the controller's clients, i.e., the company's clients.

Types of personal data processed

Depending on the functionalities, it could be any form of behaviour on the controller's website.

Although the tool does not identify website visitors (nor does the controller have an interest in knowing their identity), the collected data qualifies as personal data if it would be possible to uniquely distinguish a site visitor at any stage of processing.

If the analysis were performed on data that has been collected and promptly and fully anonymised, such processing would not involve the processing of personal data.

Types of special categories of personal data processed

n/a

Type of processing actions

Collection, structuring, analysis, encryption, deletion, anonymisation.

Retention period – deletion deadline and method

The company should enable clients to determine the retention period themselves.

Where the company is a joint controller, data is retained for a maximum of six months, which is the period during which the necessary analysis is conducted. It is predetermined which data is permanently deleted and which is anonymised after the expiration of the relevant deadlines.

Minimisation

Depending on the specific service package offered by the tool, only the necessary data for the functionalities included in the package are collected.

Technical and organisational measures

The processor has implemented appropriate data encryption and anonymisation measures.

Citizens' rights

- Notice of processing (right to information) – the controller is obligated to inform visitors to its website, which utilises the tool for analysis, in the most effective way possible, and to obtain consent if necessary. In this case, a layered approach to notification can be beneficial, where clear information about the tool's usage is provided in the first step, for example, in a pop-up window, along with the option for visitors to read more as required according to GDPR rules in the second step.
- Right of access and copy
- Right to object
- Under certain conditions, the right to erasure and the right to restriction of processing (if legitimate interest as a legal basis has been overruled due to an objection)

Other obligations

Data transfer

Third countries data transfer

For data transfers, it would be necessary to clearly identify all transfers that occur within the controller-processor, and within processor-subprocessors relationships.

Legal basis for data transfer abroad

Each of these transfers, which often occur in a connected chain, must have an appropriate legal basis depending on the role of the data exporter and the country to which the transfer is made.

Personal data protection impact assessment

The impact assessment is the responsibility of the controller. To determine whether it is mandatory to carry out an impact assessment based on the purchased functionalities, the controller must take into account the Decision of the Commissioner for Information of Public Importance and Personal Data Protection on the list of types of personal data processing operations for which an impact assessment on the protection of personal data must be conducted.

Privacy by design and by default

Although the company that developed the tool acts as the controller, the tool is sold as a product that must comply with all legal requirements. From the processor's perspective, this often means enabling the controller to customise the application's operation according to their needs so that it functions in accordance with the rules. For example, it is not the processor's role to determine the data retention period or legal basis, as these decisions are not inherent to the nature of such a tool; rather, the tool should enable the controller to make such decisions.

Documentation

In relation to this processing, the employer – controller must have/maintain, at a minimum:

- A record of processing activities
- Data processing agreement with the controller
- Data processing agreements with subprocessors
- Joint processing agreements where it has that role with the client
- Legal basis for data transfers, where applicable

13. Pecial cases of processing

13.1. Freedom of expression and information

To a large extent, the law does not apply to processing carried out for the purpose of journalistic research and the dissemination of information in the media, as well as for scientific, artistic, or literary expression, provided that, in each specific case, the limitations of the application of the PDPL are necessary to protect the freedom of expression and information. In this way, the law prioritizes freedom of expression and information over strict personal data protection. Specifically, in these situations, the provisions of the PDPL relating to: (1) processing principles; (2) rights of data subjects; (3) controllers, processors, and joint controllers, as well as their obligations; (4) transfer of personal data to other countries and international organisations; (5) other special cases of processing, will not be applicable.

Following the example of the GDPR, Serbian legislator has provided a significant exemption from strict data protection rules, considering the conflict between two fundamental rights: freedom of expression and information on one hand, and the right to privacy on the other. Whenever this conflict tilts in favour of freedom of speech and public interest, specific activities will be exempt from the obligations of personal data protection.

Trusted resources

The suspension of certain rules within the practices of media organizations is a topic thoroughly explored by the SHARE Foundation's *Guide for Media: Personal Data Protection and Journalistic Exception*.¹

¹ Adamović, J. et al., 2018, *Media Guide: Privacy and the Journalist Exemption*, SHARE Foundation. [in Serbian]



The exemption from specific provisions of the law applies during concrete activities aimed at journalistic research and the dissemination of information in the media, as well as scientific, artistic, or literary expression. After the specific activity is concluded, all data that are no longer necessary should be deleted or anonymised.⁹³

⁹³ *Ibid.*, p. 42.

Practice

One of the first cases of GDPR abuse occurred in Romania in November 2018. The investigative journalism project RISE from Romania published several documents containing personal data of a prominent politician and associated persons.¹ Immediately after the publication on the research project's Facebook page, the Romanian DPA intervened and issued an order to provide all information related to this case, including their sources, threatening with a 650 EUR fine for each day of delay, up to a maximum amount of 20 million EUR.²

The Romanian Personal Data Protection Law includes a provision regarding the processing of personal data for journalistic purposes, namely a journalistic exemption that should have been applied in this case. However, the competent authority chose to interpret the law differently, thereby intentionally or not exerting pressure on investigative journalists. The European Commission also commented on the case, noting that the application of general data protection regulations that violate fundamental rights, such as freedom of speech and information, constitutes an abuse of GDPR.

¹ OCCRP, *OCCRP Strongly Objects to Romania's Misuse of GDPR to Muzzle Media*, 9. 11. 2018

² OCCRP, *English Translation of the Letter from the Romanian Data Protection Authority to RISE Project*, 9. 11. 2018



The Serbian Commissioner

A data subject filed a complaint because Google, as the data controller, violated their right to erasure of personal data. The complaint states that there is an ongoing proceeding against a media publisher in Belgrade that published the disputed information, which appears in internet search results.

In response to the complaint, Google's representative stated, among other things: that the article was originally published by a media outlet, and although Google is not a media outlet but a search engine, it has a responsible role in ensuring respect for fundamental human rights such as freedom of expression, information, and media; that their legal basis for data processing is legitimate interest, and the validity of legitimate interest as a legal basis has been confirmed by the CJEU judgment in the case of Google Spain and the guidelines of the Working Party 29; that providing an internet search service involves enabling internet users to provide and access information through the search engine, which is a right protected by Article 10 of the European Convention on Human Rights and the Constitution of the Republic of Serbia.

The representative also referred to five criteria that should be considered when assessing requests for removal:

1. the complainant's role in public life,
2. whether the data is related to the complainant's professional life,
3. whether the data constitute hate speech, defamation, insult, or similar criminal offenses in the field of expression based on a court decision,
4. whether the data have been verified,
5. as well as
 - a. whether the data relate to a relatively minor criminal offense,
 - b. whether the offense occurred a long time ago, and
 - c. whether processing the data relating to the offense harms the data subject.

Google also stated that the guidelines of Working Party 29 explicitly point that businesspeople are considered to have a role in public life; that the complainant is a director of a company and that media in Serbia have interviewed or otherwise presented the complainant as a successful entrepreneur on multiple occasions, including the complainant's appearances on TV and in printed media. They also mentioned that the complainant is a public figure. The purpose of making the complainant's personal data available by the Google search engine is to fulfil the basic function of a web search engine, i.e., providing links to web pages containing information about the complainant in response to user queries using the complainant's name.

When deciding on the validity of the complaint, the Commissioner conducted a balancing test between the right to personal data protection v. the right to freedom of the media and the right to information. The Commissioner held that the conditions for deletion were not met because the processing is necessary to exercise the freedom of expression and information, as the complainant is a person with a role in public life. It was also determined, among other things, that the original content was published for journalistic purposes; that the inaccuracy of the provided data or harm suffered by the complainant due to the processing was not proven; that it does not involve the processing of special categories of data, nor is it about a minor; and that there is no other criterion by which the right to personal data protection of the complainant could outweigh the right to freedom of expression and information.

The Commissioner found that in this specific case, the public interest in accessing information about the complainant outweighs the right to personal data protection, and that removing the relevant link at the moment would represent a disproportionate limitation of the right to freedom of expression.¹

¹ *Protection of personal data: Positions, opinions and practice of the Commissioner, publication no. 7, Belgrade, 2022. Case number: 072-16-05/2021-6, pp. 84-90 [in Serbian]*



13.2. Free access to information of public importance

In the processing of information of public importance containing personal data, in addition to the Law on Personal Data Protection, the Law on Free Access to Information of Public Importance also applies. This means that a public authority providing such information to a requester, while containing personal data, must ensure a balance between the right of the public to know on one hand, and the right to personal data protection on the other.

A public authority from which information of public importance containing personal data is requested should, before making the requested information available, anonymise all personal data that are not absolutely necessary for the specific information and its context. This further implies that the public authority will need to find an appropriate balance between the two opposing rights in each specific case – the right of the public to know and the right to personal data protection.

The Law on Free Access stipulates that a public authority will not enable a requester to exercise the right to access information of public importance if it would violate the right to privacy, reputation, or any other right of the person to whom the requested information pertains, except (1) if the person has consented to it, (2) if it concerns a person, event, or occurrence of public interest, especially a holder of a state or political function and if the information is important considering the function that person performs, or (3) if it concerns a person who, through their behaviour, especially related to private life, has given cause for the requested information.⁹⁴

13.3. Processing of the national identification number

The processing of the unique master citizen number (UMCN) is governed by the provisions of a special law that regulates the UMCN,⁹⁵ with the application of the provisions of the PDPL regarding the protection of the rights and freedoms of the data subjects.

The Law on the Unique Master Citizen Number stipulates that the UMCN is determined electronically, in accordance with the rules prescribed by the law, and is entered into a unique electronic record of personal identification numbers maintained by the Ministry of the Interior. The Law on UMCN further prescribes that the processing of personal data and records maintained by the Ministry of the Interior, as well as the content of these records, updates, deletions, retention periods, and data protection measures, are subject to the provisions of the laws regulating records and data processing in the field of internal affairs.⁹⁶

The UMCN is used for maintaining records of personal data and for linking with other records of state authorities and authorised users who have a legal basis for using the master citizen number.

94 Law on Free Access to Information of Public Importance, Article 14.

95 Law on the unique master citizens number ("Official Gazette of RS", number 24/18).

96 Law on records and data processing in the field of internal affairs ("Official Gazette of RS", number 24/18).

13.4. Processing in the field of labour and employment

In addition to the provisions of the PDPL, labour and employment matters are regulated by the Labour Law.⁹⁷

According to the Labour Law, personal data of an employee processed for the purpose of concluding an employment contract include the first and last name, address of residence/domicile, type and level of professional qualification, as well as data related to the employee's job position (title and job description, workplace, type of employment relationship, contract duration, starting date of work, working hours, salary amount). These data are collected with the conclusion of an employment contract, by the employer, but the retention period for the data is not specifically determined. The legal basis for processing these specific data is the law, although in practice, employers often collect a broader range of data about their employees. In such cases, employers should consider whether they can classify the processing of certain data under a different legal basis, such as legitimate interest. Employers should exercise caution, especially when collecting sensitive data and information about criminal convictions of their employees, being aware that they must clearly define the purpose and legal basis for processing (if a valid legal basis exists). Otherwise, such data should not be processed. Within typical processing situations, examples of certain situations are provided where the processing of employee data is not based solely on labour law regulations, but other legal bases must be determined for such processing.

PDPL stipulates that if the law regulating labour and employment or a collective agreement contains provisions on the protection of personal data, specific measures for the protection of human dignity, legitimate interests, and fundamental rights of data subjects must also be prescribed, particularly with regard to the transparency of processing, the exchange of personal data within a multinational company or a group of business entities, as well as a monitoring system in the work environment.

13.5. Processing for archiving, research, and statistics

If the processing of personal data is carried out for archival purposes in the public interest, scientific or historical research, or statistical purposes, appropriate technical, organisational, and personnel measures are applied to ensure data minimisation. For example, if the purpose of processing can be achieved through pseudonymisation, then this technical measure for the protection of personal data should be applied.

The intention of the legislator is to require the data controller processing personal data for any of these purposes to anonymise personal data in a way that the data subject cannot be identified, provided that the purpose of processing can be achieved in this manner.

If the processing is conducted for scientific or historical research, or statistical purposes, the provisions of the PDPL regarding the right of access of data

⁹⁷ Labour law ("Official Gazette of the RS", no. 24/05, 61/05, 54/09, 32/13, 75/14, 13/17 - US decision, 113/17 and 95/18 - authentic interpretation).

subjects, the right to rectification and completion, the right to restrict processing, and the right to object do not apply, if such limitations are necessary to achieve these processing purposes, or if the application of rights provisions would hinder or significantly impede the achievement of these processing purposes. The same applies to processing for archival purposes in the public interest, with the additional note that in this case, the provisions of PDPL regarding the right to data portability, the right to erasure or restriction of processing carried out by competent authorities for specific purposes, the obligation of the data controller to provide information regarding correction or erasure of data and restriction of processing, the obligation of informing the data controller regarding correction or erasure of data and restriction of processing carried out by competent authorities for specific purposes, as well as the exercise of rights by data subjects when processing is carried out by competent authorities for specific purposes and the supervision by the Commissioner, do not apply.

13.6. Processing by churches and religious communities

PDPL stipulates that if churches and religious communities implement comprehensive rules regarding the protection of individuals in relation to processing, those existing rules can continue to be applied provided they are aligned with PDPL. In this case, the provisions of PDPL relating to the inspection and other powers of the Commissioner apply, unless the church or other religious community establishes a separate independent body to exercise those powers, provided that such a body meets the conditions set out in Chapter VI of the law pertaining to the criteria for selecting the Commissioner.

13.7. Processing for humanitarian purposes by authorities

PDPL provides that a public authority may process personal data for fundraising purposes for humanitarian reasons, but must apply appropriate measures to protect the rights and freedoms of the data subjects in accordance with PDPL. Data collected in this manner by a public authority cannot be transferred to other entities.

14. Sanctions

Both GDPR and PDPL provide appropriate protection mechanisms in cases of unlawful processing of personal data. In such instances, individuals whose rights or personal interests have been violated have specific legal remedies available to them – objection or complaint. Different sanctions are prescribed for non-compliance with obligations set forth in these laws, depending on the type and severity of the breach. Additionally, during the course of inspection proceedings, the Commissioner has the authority to impose appropriate sanctions. Under certain circumstances, individuals may also have the right to seek compensation for any damages suffered as a result of unlawful processing of their data.

14.1. Misdemeanour penalties

Relevant provisions: <i>GDPR</i> – Article 83, Recitals 75-77, 85, 88, 148-152; <i>PDPL</i> – Articles 95 and 87.

The Law on Misdemeanours defines a misdemeanour as an unlawful act determined by law or another regulation of a competent authority, for which a misdemeanour sanction is prescribed. Accordingly, Article 95 of PDPL provides a list of 32 violations for which a data controller or processor may be held administratively liable. Some of these include processing personal data contrary to the principles of processing, processing personal data for other purposes contrary to PDPL, restricting the right of access to data subjects, failure to correct inaccurate data, and more.

Monetary fines for violations of standards and duties prescribed by the law are applicable to legal entities, entrepreneurs, as well as natural persons or responsible persons in a legal entity. While other forms of judicial protection are primarily directed at safeguarding personal interests, misdemeanour proceedings are conducted for the protection of public interests. The primary goal of prescribed fines is preventive in nature, aimed at increasing awareness of the importance of respecting the protection of personal data.

Data controllers as legal persons who violate the Serbian law can be fined in misdemeanour proceedings up to a maximum of 2,000,000 RSD, while the minimum prescribed fine for misdemeanours in this field is 50,000 RSD. If a data controller commits multiple violations simultaneously, under current misdemeanour regulations, the maximum fine could amount to 4,000,000 RSD. In the case of data controller entrepreneurs, a lower fine ranging from 20,000 to 500,000 RSD is prescribed.

For disclosing personal data obtained in the course of their duties, a natural person who has not kept such data as a professional secret may be fined, with penalties ranging from 5,000 to 150,000 RSD.

In addition to fines imposed by the misdemeanour court on the data controller in misdemeanour proceedings, the law also stipulates that the Commissioner may impose a fine on the data controller through a misdemeanour order in the amount of 100,000 RSD, if a violation is found during inspection supervision. The Commissioner may impose fines for six specifically defined types of violations, including situations where the data controller - a legal entity (1) continues processing for direct marketing despite a data subject's objection to such processing; (2) fails to maintain prescribed records of processing; and (3) fails to publish contact details of the data protection officer and submit them to the Commissioner (when such an officer is appointed).

Following the example of the GDPR, Serbian law also provides certain parameters that must be taken into account when determining the amount of a monetary fine, which is relevant in a potential misdemeanour proceeding. This includes circumstances such as:

- the nature, gravity, and duration of the violation,
- the type of data,
- the existence of intent or negligence on the part of the violator,
- what the controller has done to mitigate the damage,
- whether there have been previous cases of violations of personal data protection regulations,
- whether the controller cooperates with the Commissioner to rectify the consequences of the violation,
- how the Commissioner became aware of the violation, etc.

While Serbian data controllers are subject to the jurisdiction of PDPL, their operations may also be considered in relation to the GDPR if their activities fall within the scope of its jurisdiction. Penalties prescribed by Serbian law are significantly lower than those in EU regulations, although they have been substantially increased compared to the rules of the old law. However, if a data controller from Serbia is subject to the GDPR, it is important to note that within the EU territory, fines are not imposed by a misdemeanour judge in a misdemeanour proceeding, but directly by competent supervisory authorities in the form of administrative fines, which are significantly higher than in Serbia. The maximum fine that can be imposed on a data controller is 20,000,000 EUR or 4% of the global annual turnover, whichever is higher. This significant increase in monetary fines further motivates data controllers, processors, and other entities to comply with the provisions of the GDPR and highlights the increasing importance of data protection in the EU, given the growing value of personal data and increasingly sophisticated processing methods.

Guidelines

A recommendation for data controllers who are uncertain about the application of PDPL to their operations is to consult previous practice using publicly available sources. The Serbian Commissioner's website offers information and documents related to various procedures in the field of personal data protection and their outcomes,

including decisions and opinions of the Commissioner, decisions of domestic courts, decisions of the Constitutional Court of Serbia, as well as decisions of international courts and bodies. This is an informal source of such practice, although very useful, primarily in the field of misdemeanour law.

Determining the amount of a misdemeanour fine is at the discretion of the supervisory authority, in accordance with the rules provided in the GDPR and PDPL. Although the prescribed fine amounts differ significantly between the EU and Serbian laws, the EDPB Guidelines on the imposition of administrative fines under the GDPR can serve as a helpful reference for establishing criteria when determining the amount of a misdemeanour fine.¹

¹ EDPB, *Guidelines 04/2022 on the calculation of administrative fines under the GDPR*, 12. 5. 2022



Practice

Google LLC was fined 50 million EUR by the French supervisory authority (CNIL) for failing: 1) to provide easily accessible information, written in clear and simple language during the configuration of Android mobile devices and the creation of Google user accounts, and 2) to obtain user consent for the processing of their personal data for personalized advertising. Google appealed this decision to the State Council of France (Conseil d'Etat), which confirmed the decision in June 2020.¹ This financial penalty against Google was the first fine CNIL imposed under the GDPR and was initiated by two non-governmental organizations, None Of Your Business (NOYB) and La Quadrature du Net.

In May 2023, the Croatian Personal Data Protection Agency (AZOP) determined multiple violations and imposed one of the highest fines, amounting to 2,265,000.00 EUR, on a debt collection agency.² The decision was based on the fact that the controller had violated the principles of lawfulness, fairness, and transparency by not adequately communicating its privacy policy and by failing to conclude a data processing agreement with the processor. Additionally, the controller had not implemented appropriate technical and organisational security measures, leading to the breach of rights of a significant number of clients.

¹ NOYB, €50 million fine for Google confirmed by Conseil d'Etat, June 19, 2020

² GDPR Hub, *AZOP (Croatia) - Decision of 4 May 2023 - debt collection agency*



14.2. Nonmonetary liabilities

In addition to monetary sanctions, various other measures can be taken against data controllers who violate personal data protection regulations. According to the law, the Commissioner is authorized, among other things, to:

1. monitors compliance using inspection powers;
2. request and obtain access to all personal data and other relevant information from the controller, as well as access to all premises, assets, and equipment of the controller;
3. issue warning to the controller concerning law violations;
4. issue a reprimand;
5. instruct the controller to comply with requests from data subjects regarding exercise of their rights;
6. order the alignment of data processing activities with the law in a specific manner and within a specified period;
7. impose temporary or permanent restrictions on data processing activities and prohibition of processing;
8. order correction or deletion of personal data; or
9. suspend the transfer of personal data to recipients in another country or to international organisation.

Practice

Following an inspection, the Commissioner determined that a business entity, providing bicycle rental services, processed personal data of individuals by collecting and retaining their personal documents. The Commissioner issued a decision prohibiting further processing of personal data in this manner, and a subsequent inspection was conducted to verify compliance with the decision.¹

¹ *Protection of personal data: Positions, opinions and practice of the Commissioner, publication no. 8, Belgrade, 2023. Case number: 072-04-2333/2021-07, pp. 15-17 [in Serbian]*



In separate case of unlawful personal data processing, a business entity has been permanently prohibited from processing ID and passport numbers during online purchases of goods.² It is not necessary to process this data during the purchase; it may be processed later, when the purpose is to refund the purchase amount or cancel the purchase in the case of a previously paid advance.

² *Protection of personal data: Positions, opinions and practice of the Commissioner, publication no. 8, Belgrade, 2023. Case number: 072-21-1134/2022-07, p. 26 [in Serbian]*



In addition to lodging a complaint with the Commissioner for the violation of data protection rights, who can impose one of these measures when initiating proceedings against the controller, individuals can also address a court in a litigation procedure for the violation of their rights. In this regard, nearly identical rules are provided by both the Serbian law and the GDPR.

14.3. Compensatory damages

Relevant provisions: GDPR – Article 82; PDPL – Article 86.

The PDPL, following the GDPR model, provides that any individual who has suffered material or immaterial damage due to a breach of provisions related to personal data protection has the right to claim compensation from the controller who caused such harm. Therefore, if an individual believes they have suffered such harm due to unlawful actions of a controller, they can establish the existence and amount of such harm through a litigation procedure. On the other hand, a controller can be exempt from liability for the harm if they can prove that they are in no way responsible for its occurrence. However, while the claim for compensation will most often be directed at the controller responsible for personal data processing, in cases where the controller failed to fulfil certain legally prescribed obligations or acted contrary to instructions received from the controller, the processor can also be held liable.

The amount of damages will always depend on the circumstances of the specific case. It is important to note that in the field of personal data protection, the significance is not only the amount of damages for an individual, but also the possibility for a large number of individuals to join the proceedings. In such cases, the total amount of damages for all individuals, each with relatively small individual damages, can be significantly higher than fines (at least concerning misdemeanour liability according to Serbian regulations). The claim for damages is submitted according to the general rules of the Law on Obligations, while the Personal Data Protection Law does not regulate additional requirements in this regard.

Practice

One of the most well-known class action cases related to the violation of personal data protection standards is the case of British Airways.¹ In September 2018, a cyber attack occurred, following which it was estimated that the rights of over 420,000 individuals were violated, including both employees and clients of the airline company. In addition to the fact that the Information Commissioner's Office of the United Kingdom proposed a fine of 204.6 EUR million against British Airways in July 2019

¹ The Daily Swig, *British Airways agrees to pay victims of record-breaking data breach*, 9. 7. 2021



for violating Article 32 of the GDPR – not implementing sufficient technical and organisational measures to ensure data security, which allowed hackers to steal personal data of a large number of individuals – all British Airways passengers were invited to join class action against the controller.² Eventually, the proposed amount was settled out of court, and British Airways also issued an apology to all individuals whose rights were violated.



² Data Claim, *British Airways Data Breach*

According to the rules of obligations, the damage for which compensation is sought can be both material and non-material, and in any case, it must be proven to be compensable. Regarding non-material damage, it's important to emphasise that not every breach of privacy or personal data violation can be considered non-material harm that requires compensation. According to the Serbian Law on Obligations, compensation can be awarded only for physical pain, mental suffering due to reduced life activity, disfigurement, defamation, loss of honour, freedom or personal rights, death of a close person, as well as for fear. Therefore, an individual can demand that in addition to material damage, and independently from it, non-material damage resulting from unlawful processing be established if it led to a violation of personal rights. It's also stipulated that when deciding on the request for compensation for non-material damage and its amount, the court takes into account the importance of the violated interest and the purpose for which the compensation serves, as well as the consideration that the compensation should not favour tendencies incompatible with its nature and social purpose.

In case there are multiple controllers or processors, those whose responsibility is established will be jointly liable for the damage.

14.4. Reputational risk

In recent years, there's been a growing public awareness of the significance of personal data on the internet, the scale of the data industry, the wealth amassed by global corporations through data, as well as the risks to citizens' privacy caused by public and private actors. The new EU regulation has set data protection standards in line with new societal values and expectations, presenting companies with a serious choice between a profitable business model and the ethical demands of the community.

Continuous monitoring of user behaviour, profiting from reselling data, or a careless approach to personal data security have become increasingly unbearable risks to business reputation. The treatment of “ordinary” citizens' personal data can be crucial for all controllers whose business models are predominantly based on the use of personal data, or where personal data processing is of great importance due to their quantity, type, and scope (e.g., hotels, healthcare institutions, insurance companies and banks, traditional and social media, etc.).

In cases where a controller's business model relies on a crucial relationship of trust with users and clients, reputational risks may take precedence over the threat of fines. Working to mitigate these risks is an ongoing process and, in addition to complying with legal rules, involves a commitment to higher standards. This is especially evident in obtaining valid consent and providing relevant information, efficiently responding to user requests, as well as implementing carefully selected data security measures.

Practice

Reputational risk can arise as a consequence of violating personal data protection even in cases where no sanctions have been imposed. For instance, in a case of unauthorised use of a client's phone number for personal purposes by an employee, the Commissioner did not impose any sanctions or corrective measures on the controller. This was because, following an inspection, it was determined that there was no breach of the provisions of the PDPL. The controller had appropriately addressed the application of technical, organisational, and personnel data protection measures and had taken adequate training and security and privacy testing measures, as required for all employees.¹ Nevertheless, this case garnered significant media attention and potentially harmed the controller's reputation.

¹ *Protection of personal data: Positions, opinions and practice of the Commissioner, publication no. 8, Belgrade, 2023. Case number: 072-04-1450/2022-07, p. 13 [in Serbian]*



14.5. Criminal liability

Violation of personal data protection rules can also lead to criminal liability. The Criminal Code of Serbia prescribes a fine or imprisonment of up to one year if someone (1) unlawfully obtains, discloses to another, or uses for purposes other than intended, personal data collected, processed, and used under the law, as well as when (2) someone collects personal data of citizens in violation of the law or uses such collected data. An aggravated form of this criminal offense, punishable by up to three years in prison, exists if the act is committed by an official in the performance of their duties.

The range of actions covered by this criminal offense is quite broad, encompassing any situation of unlawful processing of personal data. Based on the rules of the PDPL, it can be concluded that any data processing that contradicts the principles of processing constitutes an action under this criminal offense. The same assumption can be made for data processing that violates PDPL rules which are essentially elaborations of the principles. Among such rules, for example, there are those regarding the existence of legal grounds for processing or, more specifically, rules about obtaining consent when that legal basis is relevant. On the other hand, there are certain legal rules under PDPL whose violation likely wouldn't lead to criminal liability because, due to their formal nature, they do not fundamentally endanger the rights and interests of the data subjects, such as formal rules on keeping records of processing actions.

Practice

Civil and criminal courts in Serbia have not yet developed significant practice in this field. Regarding criminal law, it remains nationally specific within EU as well. According to publicly available practices of Serbian courts, criminal proceedings are still rare. Criminal liability, for example, was established in a case involving the unauthorised export of personal data from Serbia without a valid legal basis for transfer. In this instance, the head of the technical department of a Belgrade faculty repeatedly disclosed data about a total of 6,623 graduate students to an Australian agency. The criminal offense of unauthorised collection of personal data was established, and the accused received a conditional sentence.¹

The practice of European courts is generally much more easily and promptly accessible on the respective websites of the institutions themselves.



¹ Judgment of the High Court in Belgrade of May 25, 2015

Dilemmas

Is there a real risk that controllers and processors operating in Serbia, but offering goods or services within the EU or monitoring the behaviour of EU residents, could be fined under the General Data Protection Regulation? GDPR is applied beyond the borders of the EU in specific cases, which means that legal entities outside the EU can face maximum fines. However, the question arises as to how any authority from an EU member state can enforce a fine against an entity that has neither a registered office nor any assets within the EU. Due to the perception that the practical execution of a fine is unlikely, controllers in Serbia might mistakenly believe they are safe from draconian sanctions. However, it is important to consider a few facts:

- All controllers without an establishment in the EU, to which GDPR applies, must appoint an EU representative of their own choosing. The possibility for the representative to be held directly liable is limited only to the representative's obligations, such as record-keeping and providing necessary information to supervisory authorities.
- If entities outside the EU fail to fulfil the obligation to appoint an EU representative, direct enforcement is practically hindered (of course, this is also in breach of another GDPR obligation, for which an administrative fine is also provided), but indirect mechanisms are still available. It is difficult to imagine processing data of individuals within the EU territory without establishing some form of cooperation with entities within the EU, such as IT providers and intermediaries, payment facilitators, etc. By establishing direct jurisdiction over these entities,

EU authorities can effectively prevent data collection or access to services and websites within the EU, using enforcement and other powers they have in accordance with their national laws. Furthermore, controllers and processors subject to EU regulations are unlikely to risk being penalised themselves for cooperating with entities that clearly do not comply with GDPR rules.¹



¹ Robert Madge, *GDPR's global scope: the long story*, 12. 5. 2018

AUTHORS' BIOGRAPHIES

Dorđe Krivokapić is a professor of Information and Communication Technology Law at the Faculty of Organizational Sciences, University of Belgrade. He graduated from the Faculty of Law at the University of Belgrade, and completed his master's studies at the School of Law, University of Pittsburgh, USA. In 2016, he defended his doctoral dissertation at the Faculty of Law, University of Belgrade, on the topic "Conflict of Laws and Jurisdiction stemming from Reputation Infringement on the Internet".

He was born in Kotor, and lives and works in Belgrade. Before his academic engagement, he gained extensive experience in the field of corporate law. Since 2009, he has been employed at the Faculty of Organisational Sciences, University of Belgrade, within the Department of Business Systems Organisation. In 2010 and 2012, he pursued his studies at the Berkman Klein Centre for Internet & Society at Harvard Law School, USA. Since 2018, he has been engaged as a researcher at the Institute of Law and Technology, Faculty of Law, Masaryk University, Czech Republic. As a visiting professor, he has delivered lectures at the Berlin School of Economics and Law in Germany and Aarhus University in Denmark.

As an independent consultant, he has rich experience in advising international corporations, small and medium-sized enterprises, startups, as well as the public sector, academia, civil society, and international organisations. He is actively engaged in research and advocacy at the intersection of law and technology at the national, regional, and European levels, representing academia and civil society in expert bodies of international organizations such as OECD, CoE, OSCE, and others.

He is one of the founders of the SHARE Foundation, where until 2017 as the Program Director he led a team of interdisciplinary researchers in dozens of projects. He is the author and editor of numerous professional publications, including the textbook "Business Law in the Digital Age". He is the producer of the TV series "In the Network". He teaches courses in the fields of business law, information and communication technology law, business ethics, and business systems organisation within the academic programs of the Faculty of Organisational Sciences, Faculty of Electrical Engineering, Faculty of Medicine, and interdisciplinary studies at the University of Belgrade, as well as at the Faculty of Dramatic Arts in Belgrade.

Jelena Adamović is a lawyer. Throughout her career, she has been engaged in several Belgrade law firms specialising in various areas of commercial law. She currently practices law independently. SHARE Foundation has engaged her as a legal consultant and researcher on projects related to digital rights.

Over time, her practice has focused on personal data protection laws, as well as other issues related to data regulation and data economy.

Dunja Tasić Krivokapić was born in Leskovac, where she completed her high school education. After graduating from the Faculty of Law at the University of Belgrade, she began practicing law, and in 2015, she passed the bar exam and became a member of the Belgrade Bar Association. Her practice focuses primarily on corporate and commercial law, personal data protection, intellectual property law, and IT and technology law. She has collaborated with a large number of corporate clients, including technology companies, startups, and clients from creative industries.

She is the author of several publications on personal data protection and provides services for the implementation of GDPR and Serbian data protection laws into clients' business processes, as well as education in this field. She speaks English and Spanish.

Andrea Nikolić is a teaching assistant at the Faculty of Organizational Sciences of the University of Belgrade in the field of Law of Information and Communication Technologies. In parallel, she completed her undergraduate studies at the University of Belgrade Faculty of Law and Union University Belgrade Banking Academy. She completed her master's studies at the Faculty of Law, University of Belgrade, where she is currently a doctoral candidate. She has received numerous scholarships for her academic and scientific achievements.

She started her professional career at a leading corporate law firm in Serbia. Afterwards, she interned in International Arbitration Department at a law firm based in London. Throughout her academic career, she had many research visits at prestigious institutions in the United Kingdom, France, Germany, the Netherlands, etc. She is the author of a large number of scientific papers in the field of alternative dispute resolution and ICT law and was engaged as an expert in different projects in the aforementioned fields.

CIP – Katalogizacija u publikaciji
Narodna biblioteka Srbije, Beograd

658:342.738

HANDBOOK : personal data protection in business
/ Đorđe Krivokapić ... [et al.]. - Beograd : Fakultet
organizacionih nauka, 2023 (Beograd : Službeni
glasnik). - 324 str. : graf. prikazi, tabele ; 24 cm

Izv. stv. nasl.: Priručnik: zaštita podataka o ličnosti u
poslovanju. - Tiraž 150. - Str. 11-12: Commissioner's
foreword / Milan Marinović. - Str. 13-14: Greater
internet freedom Serbia project foreword / Danilo
Barjaktarević. - Authors' biographies: str. 323-324.
- Napomene i bibliografske reference uz tekst.

ISBN 978-86-7680-436-8

1. Krivokapić, Đorđe, 1982- [аутор]

а) Пословање -- Право на заштиту података
о личности

COBISS.SR-ID 123705865

