RANKING DIGITAL RIGHTS IN CENTRAL ASIA

Public Fund Civil Internet Policy Initiative (CIPI)

2022

Conducted by:

Public Fund Civil Internet Policy Initiative (CIPI)

This research was conducted with financial support of Internews within the framework of the Greater Internet Freedom Project funded by USAID in June-September 2022 for scoring of digital rights compliance of business sector in Central Asia.

Greater
Internet
Freedom

Table of Contents

I. Introduction

The countries of central Asia — Uzbekistan, Kyrgyzstan, Kazakhstan, Turkmenistan, and Tajikistan — are currently undergoing a rapid analogue to digital transition. Internet access and mobile penetration are transforming the relationship between individuals and institutions even as they blur the boundaries between citizens, states, and digital service providers — i.e., mobile and internet service providers. In a process of discovery that mirrors what their peers in fully digitized societies have already experienced, central Asians are now discovering that access to mobile and internet technology carries both positive and negative impacts on civil society.

Internet and mobile access are transforming the lives of ordinary people in central Asia. It is radically altering the way business functions, while presenting digital entrepreneurs with unprecedented opportunities for participating in the innovation ecosystem. Governments, meanwhile, are trying to maximize the benefits of a digital economy while minimizing the loss of sovereignty and social disruption. This includes using digital technology against their own citizens. The public is becoming aware that state authorities can use the internet against them, but the subject has not yet sparked significant debate[1].

But while the rapid introduction of digital technology is transforming the lives of people who live in areas where the necessary infrastructure exists, it remains out of reach for those who reside in less developed or more remote areas. Nevertheless, despite challenges that include recovery from the COVID-19 pandemic, the region is seeing expanded digital access, increasingly robust connectivity, and refurbished internet infrastructure.

This paper addresses several questions about Central Asia's ongoing transition to a digital society.

- *How is it affecting the state's relationship with its society, citizens, and businesses?*
- *How is it affecting the relationship between business and consumers*?
- *Who is empowered and who is disempowered?*
- *Do central Asian countries have the capacity to manage new digital technologies?*
- *Who are the main influencers and investors in the region's digital technology?*
- *How can human rights watchdogs influence digital rights and enhance collaboration with state actors, activists, and citizens?*

[1]Lozanova, Youlia, et al. *Global ICT Regulatory Outlook 2020*. International Telecommunications Union. Geneva, 2020. https://www.itu.int/dms_pub/itu-d/opb/pref/D-PREF-BB.REG_OUT01-2020-PDF-E.pdf

Because central Asia is plagued by political volatility and uncertainty, digital readiness and resilience are particularly important issues. Global economic downturns have a negative impact on the pace of technology–led development, limiting investments in the digital future with vulnerable and marginalized communities feeling the consequences most acutely. Digital preparedness is essential in the politically volatile regions of Central Asia. The volatile environment means that the economy tends to suffer negatively which in turn hampers technology development and loss of investments in digital futures of citizens. Often it is those that are vulnerable and marginalized that tend to feel these gaps severely.

The countries of Central Asia share more than just geography; they also share a similar legacy. More importantly, they could share a digital future.
Sustainable development of the digital economy is important, as are innovation and digital transformation. But human rights, privacy, data protection and freedom of expression are also critical issues. The global principles on freedom of expression and privacy (the principles) have been developed by digital service providers, investors, civil society organizations and academics (the participants) with the goal of protecting and advancing freedom of expression and privacy in the information and communications technology industry globally. The principles are based on internationally recognized laws and standards for human rights, including the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights, and the International Covenant on Economic, Social and Cultural Rights. The application of these principles is informed by the UN Framework and Guiding Principles on Business and Human Rights, and the OECD's Guidelines for Multinational Enterprises.

The purpose of this study is to assess the current state of internet and mobile service providers in Central Asia, while offering them a roadmap toward improvement. The improvements we recommend would help secure online business, thereby increasing user loyalty in the region's expanding and highly competitive e–business environment. We also hope this study will lay the foundation for mobile and internet providers to consider digital rights in their policy reviews and practices, while demonstrating the importance of respecting and protecting human rights, freedom of expression, and the right to privacy.

II. Background and Context

a. Geographic overview

Central Asia covers an area of 4,003,451 km^2. It is bordered by 2 economic powerhouses, China in the east and Russia in the north and you also find Afghanistan and Iran to its South. Historically, it was a significant part of the Silk Road. The physical landscape is dramatic, ranging from vast steppes to high, rugged mountains, formidable deserts to large rivers, lakes, and seas.

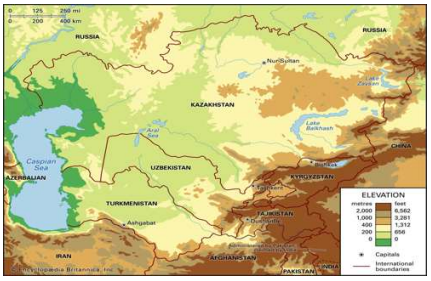


Figure 1 - (source: Encyclopedia Britannica)

The region is economically diverse, comprising a mix of upper middle– and low–income countries that are of major strategic importance due to their geographic location and natural resources. Most central Asian countries — Tajikistan, Uzbekistan, Kyrgyzstan — are landlocked, which means they are far from intercontinental submarine cables. The limited access to cost–effective international bandwidth is a distinct disadvantage that forces those countries to rely on their neighbors for transit and interconnections[2]. Turkmenistan and Kazakhstan, however, could connect via Azerbaijan to fiber–optic cables under the Caspian Sea that connect Central Asia to Europe

b. Internet adoption

Central Asia's ethnically diverse population of more than 77 million is relatively young, with a median age of 27.6 years. Since young people are more likely to be early adopters and agents of internet and mobile technologies, the region is well positioned for rapid digital transformation. But it faces challenges — i.e., a lack of essential infrastructure and a relatively sparse population density. Only 48 percent of the population of Kyrgyzstan, Tajikistan, and Uzbekistan, which are most central Asian countries, live in urban centers, compared to 54 percent worldwide.

One of the challenges shared by all the countries of central Asia is an **underdeveloped internet ecosystem**. According to a 2015 report[3] coauthored by the Asian Development Bank and the UN

[2] https://merics.org/en/tracker/networking-belt-and-road-future-digital

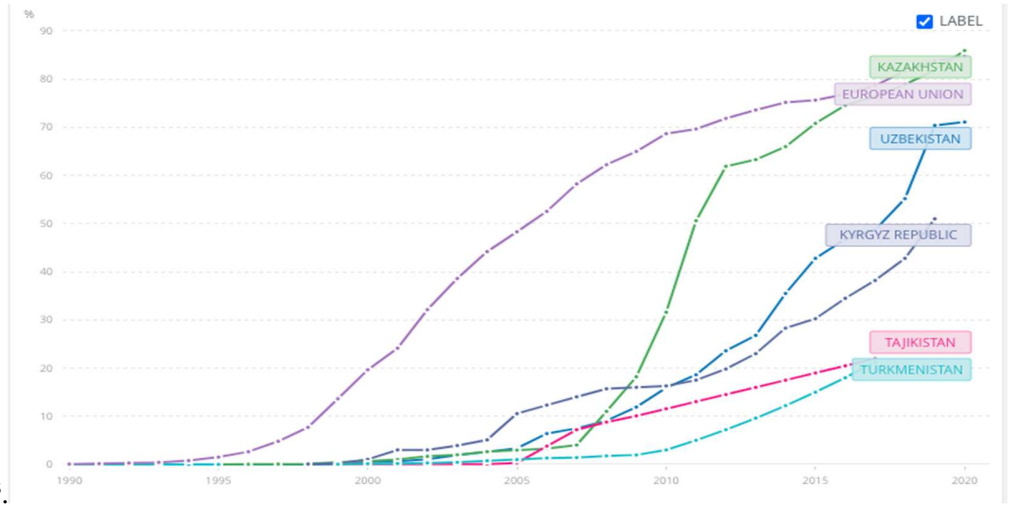
[3] Unleashing the Potential of the Internet in Central Asia, South Asia, the Caucasus and Beyond

Economic and Social Commission for Asia and the Pacific, central Asia's socioeconomic and demographic characteristics present a set of "natural disadvantages" **that act as barriers to internet diffusion**. These include low population density and vast rural hinterlands that can be difficult to cover by physical networks — i.e., they are "uneconomic" – with internet and mobile service providers deciding it's not cost effective to provide digital services in these areas. Nevertheless, in recent years some central Asian countries have seen rapid rates of economic growth of around five percent per annum, on average. Despite the challenges, internet access has steadily grown during the past decade, thanks to expanded geographic coverage and reduced prices. Of providing services to consumers.

Rating	Country	Internet download speed (Mbps)	Cost per month (USD)	Affordability (%)	Cost for 1 GB of Internet traffic (USD)	Score
43	Kazakhstan	1.39	11.5	2.72%	0.9	82.45
110	Kyrgyzstan	1.58	24.3	11.56%	1.0	73.02
112	Uzbekistan	0.96	15.4	6.46%	2.0	72.55
131	Tajikistan	0.38	30.4	24.72%	4.4	66.02
161	Turkmenistan	0.32	213.8	51.17%	13.5	50.12

Figure 2 - Rating of central Asian countries by cost and affordability of internet[4]

Significant disparities in internet adoption continue, especially between urban and rural dwellers. The relative affluence of urban populations does not fully explain the gap in internet adoption[5].



https://www.adb.org/sites/default/files/project-document/178531/unleashing-internet-potential-central-asia-south-asia-caucasus-and-beyond.pdf

[4] Karimova, Altynay. "How is Mobile Communications and the Internet Developing in Central Asia?" Central Asian Bureau for Analytical Reporting, October 25, 2021. https://cabar.asia/en/?p=48695&_utl_t=ln

[5] Lovelock, Peter. "Digital Economy Study in Central and West Asia." ADB, 2015.

Figure 3. Individuals using Internet (% of population) — Central Asian countries[6]

High–speed internet access is limited and expensive in Central Asia. The rate of domestic fixed broadband penetration ranges, according to TeleGeography,[7] from 3.1 percent in Tajikistan to 35 percent in Kazakhstan. Both fixed and mobile broadband internet speeds are significantly below the global average across Central Asia countries. Telecommunication service providers and internet service providers (ISP) prioritize highly populated urban centers, where the returns on investment are higher and quicker to realize. According to the World Bank[8] almost half the population in Central Asia is not digitally connected; they are thus missing out on employment opportunities, falling behind in education, and not receiving adequate healthcare. The digital divide is exacerbating existing social inequalities and hampering economic growth.[9] The pandemic caused many problems, but it also acted as a stimulus to unprecedented opportunities in digital innovation and catalyzed understanding of critical socio–economic opportunities reinforced by digital transformation in the region. However, the availability of technologies does not automatically lead to digital transformation.

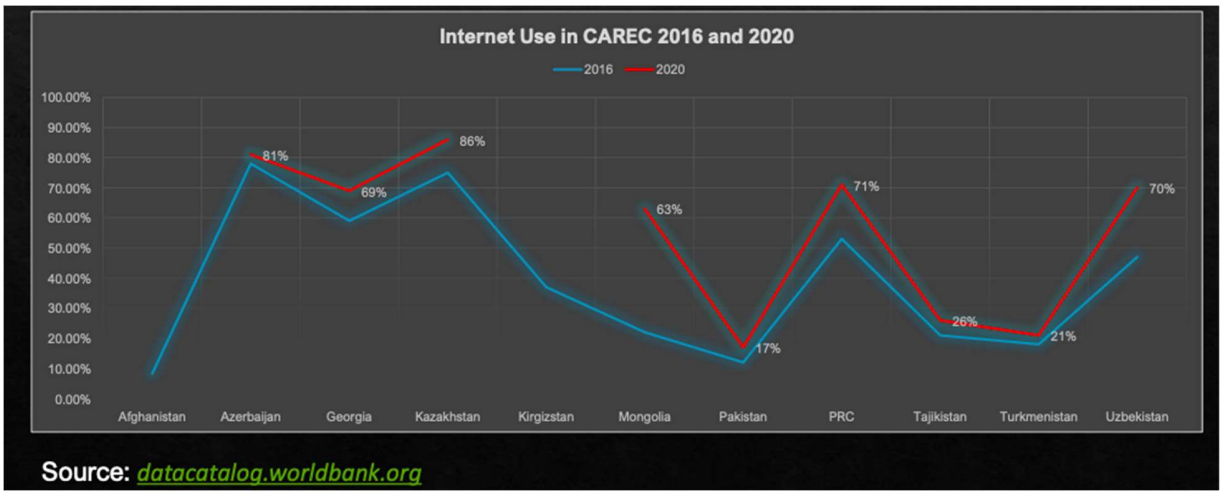


Figure 4. Digitalization accelerated by COVID 19[10]

6 https://data.worldbank.org/indicator/IT.NET.USER.ZS?locations=KZ-TJ-UZ-KG-TM-EU

7 https://www2.telegeography.com/our-research?hsCtaTracking=f0cd9377-8e45-449a-9902-8ee3c2ef5f8e%7Ca946cb73-99cb-4858-98f4-d4a80dad8729

8 https://www.worldbank.org/en/news/press-release/2020/12/02/urgency-of-bridging-digital-divide-in-central-asia-increases-as-a-result-of-the-covid-19-pandemic#:~:text=ALMATY%2C%20December%202%2C%202020%20%E2%80%94,Digital%20Divide%20in%20Central%20Asia%E2%80%9D

9 https://www.eurasia.undp.org/content/rbec/en/home/presscenter/pressreleases/2021/embracing-equality-in-a-digital-era-in-central-asia.html

10 https://www.carecinstitute.org/wp-content/uploads/2022/02/Session-2-1%EF%BC%9ADigital-CAREC-Regional-Digital-Divide-ADB_eng.pdf

The Covid–19 pandemic tested the readiness and capabilities of Central Asia's ICT and digital services, while acting as a catalyst for innovation, because it forced almost all essential services to become available online. Regional governments, international organizations, NGOs, and some businesses introduced work from home, distance learning, online public services, automated chatbots, e–shops, and e–pharmacies.

III. Policy and Regulatory Framework/ Enabling Environment

Kazakhstan, Tajikistan, Uzbekistan, and Kyrgyzstan are all member–states of the UN, which has ratified or acceded to the human rights treaties listed in Table One (below). The UN Guiding Principles on Business and Human Rights (UNGP)[11] are the global standard for preventing and addressing the risk of adverse impacts on human rights linked to business activity and provide the internationally–accepted framework for enhancing standards and practices regarding business and human rights[12]. According to the OHCR:

> "States are obligated under international human rights law to protect against human rights abuse within their territory and/or jurisdiction by third parties, including business enterprises. Even if States do not fulfill their obligations, all business enterprises are expected to respect human rights, meaning they should avoid infringing on the human rights of others, and should address adverse human rights impacts with which they are involved. If abuses occur, victims must have access to effective remedy through judicial and non-judicial grievance mechanisms"[13].

Many member-states have, however, thus far failed to comply with the treaties.

Human Rights Treaties[2]	Kazakhstan	Tajikistan	Turkmenistan	Uzbekistan	Kyrgystan
1. CAT	A	A	A	A	A
2. CAT-OP	R	-	-	-	A
3. CCPR	R	A	A	A	A
4. CCPR-OP2-DP	-	-	A	A	A
5. CED	A	-	-	-	-
6. CEDAW	A	A	A	A	A
7. CERD	A	A	A	A	A
8. CESCR	R	A	A	A	A
9. CMW	-	R	-	-	A
10. CRC	R	A	A	A	A
11. CRC-OP-AC	R	A	A	A	A
12. CRC-OP-SC	R	A	A	A	A
13. CRPD	R	-	A	Signed	Signed

Note: R – ratification; A – accession

(Source: Human Rights of Osaka, March 2017)

Table 1. Ratified/Acceded to Human Rights Treaties[14]

[11] https://www.ohchr.org/sites/default/files/Documents/Issues/Business/Intro_Guiding_PrinciplesBusinessHR.pdf

[12] The Human Rights Council unanimously endorsed the Guiding Principles in its resolution 17/4 of 16 June 2011. https://www.ohchr.org/en/business-and-human-rights

[13] https://www.ohchr.org/en/business-and-human-rights

[14] Ratification/accession status taken from United Nations Human Rights, Source: https://www.hurights.or.jp/archives/focus/section3/2017/03/central-asia-human-rights-issues.html#1

Like all member states, Central Asian countries routinely submit Universal Periodic Reports (UPR) to the UN Human Rights Commission (UNHRC), in which they declare what actions they have taken to improve human rights. However, these reports do not reference digital rights under the UNHRC's rubric of human rights and freedom of expression. Nor do tech companies and digital service providers participate in the monitoring process. Given that their services are growing exponentially across the region in response to demand, digital service providers and tech companies must improve their corporate policies and practices on privacy and data protection so that they are in line with the UNGP[15]. Currently tech companies in the region are not in compliance. Governments should appoint an ombudsman for digital rights and data privacy to monitor citizens' digital rights. Human rights NGOs should also work to protect digital rights.

a. Policies for the implementation of digital rights

The first waves of digitization in Central Asia were mainly focused on moving from analogue to electronic services with the sole purpose of increasing the efficiency of public services. But comprehensive digital transformation involves rethinking and reorganizing public services from the ground up to meet users' changing needs. This requires opening access to data and improving digital service delivery.[16] As smartphones host an increasing number of online services, regulators in Central Asian countries are struggling with various challenges, such as digital identity, data protection and privacy, blockchain and Artificial Intelligence (AI). **Central Asia's regulatory landscape lags significantly behind.** According to the International Telecommunication Union (ITU) regulatory score, Central Asia ranks below 40, on a scale of 0 to 100, when compared to 95 countries — including Italy, Ireland and Switzerland.[17] Some Central Asian countries have created laws, rules and regulations that are overly broad and unduly restrictive, which often renders them irrelevant or counterproductive.[18] Government institutions should work closely with non-governmental stakeholders to develop adequate rules and regulations to regulate digital rights as human rights. These stakeholders include tech companies, e-commerce, Fintech, NGOs working on ICT and ICT4D, and NGOs that deal with internet policy and human rights.

b. Uneven data privacy and data protection

The emergence of the e-government, which introduced biometric ID systems[19] and safe city initiatives in Central Asian countries, has dramatically changed the relationship between the state

---

[15] https://www.ohchr.org/sites/default/files/Documents/Issues/Business/Intro_Guiding_PrinciplesBusinessHR.pdf

[16] *Citizen-oriented digital transformation in the public sector*. https://www.researchgate.net/publication/325495066_Citizen-oriented_digital_transformation_in_the_public_sector

[17] https://www.adb.org/sites/default/files/publication/696281/adbi-wp1248.pdf and (Kattel and Mergel 2018)

[18] https://asia.nikkei.com/Opinion/Incoherent-regulations-will-devastate-Asia-s-digital-economy

[19] For example, Tajikistan began creating a biometric data registry in 2010 when it announced that it would begin creating and issuing biometric passports (Travel Document) that would contain citizens' digital photographs and fingerprints. On 2016 The Tajik government decided to expand this data system by mass fingerprinting citizens for issuing National ID, in 2019, this effort was largely successful, and as of 2020 around 2.5 million citizens had biometric passports. Although the government will continue

and its citizens. On the one hand e-government can foster good governance, access to public services, some transparency, and some democratization; on the other hand, it allows states to engage in massive data acquisition and digital surveillance. The governments of Central Asia cite national security as their justification for monitoring internet activity, routinely blocking access[20] as a means of controlling domestic unrest. Since 2001, the government of Tajikistan has mandated that all companies *install a system of operational search measures* in their equipment to allow full government access to data[21], while the Kazakhstan government requires all ISPs to force their users to install *a root certificate* into their devices. This essentially allows the government to carry out man–the–middle attacks on Kazakh internet traffic[22].

Most Central Asian countries have passed laws and regulations to protect personal information. Kazakhstan, Kyrgyzstan, and Tajikistan have clearly modeled their legislation on the European Union's General Data Protection Regulation (GDPR). But the governments in these states are also granted legal access to personal user data in the name of *national security*. Kyrgyzstan is ostensibly more democratic than its neighbors, in that its data protection is regulated by a 2008 law that stipulates the government cannot collect personal data without the owner's consent, but its laws regarding *personal privacy* are weak and allow the government significant access. [23] Tajikistan also modeled its the GDPR regulations, while Uzbekistan adopted the "law on personal data"[24] that is to that of the Russian Federation's.[25] None of these laws prevent government authorities from violating the *rights and freedom of citizens*[26].

c. Data Infringement

Leakage of personal data can cause enormous financial and reputational damage to a company. For the users data leakage poses not only a threat to financial security, but in some cases their lives, health, and psychological well-being. Leaked data can be used to spam, bully, blackmail, cyberstalk, to gain access to devices and identities, and to engage in criminal activity.

Most leaks, however, are committed not by government authorities but by bad actors in the private sector. In recent years Central Asia has seen several data–related scandals. In 2020 a database in Kazakhstan was leaked, compromising the personal information of about 11 million people —

issuing biometric passports and national ID to its citizens, the vast majority have had their biometric data included in the overall biometric registry.

[20] https://www.accessnow.org/central-asia-internet-shutdowns-harm-rights/

[21] "Obzor Telekom Rynka Tadzhikistana: Fiksirovannaia, Mobilnaia i Mezhdunarodnaia Sviaz" [Tajikistan Telecom Market Review: Fixed, Mobile and International Communications], Digital Report, June 5, 2017, https://digital.report/tadzhikistan-svyaz/.

[22] https://daviscenter.fas.harvard.edu/sites/default/files/files/2021-06/Digital_Silk_Road_Report.pdf

[23] https://daviscenter.fas.harvard.edu/sites/default/files/files/2021-06/Digital_Silk_Road_Report.pdf

[24] https://www.jdsupra.com/legalnews/uzbekistan-non-compliance-with-data-3022823/

[25] https://www.dataguidance.com/sites/default/files/gdpr_v_russia_december_2019.pdf

[26] Ibid

equivalent to the country's entire population.[27] Investigative journalists revealed in 2019 that the government of Kyrgyzstan had been selling citizens' data to financial organizations, telecommunications companies, and banks since 2017.[28] Another notable scandal took place in 2017, when it was uncovered that Sooranbay Jeenbekov, then candidate for president, used citizens' private data to win the election. Hackers found that a little–known real estate website called Samara was hosting the personal data, including the PINs, passport numbers, and phone numbers of two million citizens from the State Registration Service's server.[29]

Web services and IT companies are coming together to form ecosystems with a huge number of different legal documents, policies and rules that put the average customer under a lot of pressure. Customer contracts tend to be very long and too complicated for the average citizen to understand, leading many to sign without reading the document carefully. If they had read the small print, they would have seen that by signing they gave the company the right to collect, use and transfer private data to third parties. Digital service providers often make changes to their user policies without notifying their customers. Accessibility, transparency, and clarity in presenting complex legal terms and policies will allow the companies to improve relationships with their users.

We believe that users have the right to all the information necessary to protect their right to freedom of information, privacy, and data protection, and that digital service providers should act accordingly. The UN's Guiding Principles on Business and Human Rights stipulate that private companies have a duty to respect human rights, regardless of their obligation to the state.

While **Central Asian states have based their legislation on personal data on the EU's GDPR,** they have failed to create implementation mechanisms. Users need to be aware of their digital rights and of the responsibility of institutions, public or private —telecoms, e-commerce platforms, e-health, e-education, Fintechs — to follow the law.

---

[27] "Zloumyshlenniki vylozhili v set dannye millionov kazakhstantsev" [Attackers Have Posted the Data of Millions of Kazakhstanis on the Network], Kursiv - Delovye Novosti Kazakhstana, April 7, 2019, https://kursiv.kz/news/obschestvo/2019-07/zloumyshlenniki-vylozhili-v-setdannye-millionov-kazakhstancev

[28] Tatyana Kudryavtseva, "Passport Data of Kyrgyzstanis to Be Sold to Banks, Cellular Companies," 24.Kg, November 6, 2019, sec. English, https://24.kg/english/134288__Passport_data_of_Kyrgyzstanis_to_be_sold_to_banks_cellular_companies/.

[29] Rinat Tukhvatshin, "Samarageti, epizod 1. Kak server pravitelstva Kyrgyzstana ispolzovali dlia popytki vliianii a na prezidentskie vybory" [Samaragate, Episode 1. The Government of Kyrgyzstan was used as a Server to try to Influence on presidential elections] https://kloop.kg/blog/2017/10/26/samara_elections_kg/.

IV. Research Scope and Methodology

The purpose of this study is to analyze the existing policies and practices of some of the most prominent technology companies in Kazakhstan, Kyrgyzstan, Tajikistan, and Uzbekistan, and to evaluate their commitments to protecting online privacy and freedom of expression. This analysis uses a comparative analysis approach of at least 16 companies in four Central Asian countries — Kazakhstan, Kyrgyzstan, Tajikistan, and Uzbekistan. The 16 companies are KCELL, KaR-Tel, Sky Mobile, Nur Telecom, TT Mobile, Indigo Tajikistan, Unitel, Coscom, OLX Group, YALLA CLASSIFIEDS OÜ, Rashod, OLX CLASSIFIEDS, Kaspi Bank, Optima Bank, Alif Bank, and Kapitalbank. Comparative analysis refers to the comparison of two or more processes, documents, data sets or other objects. The research focuses on three key categories of digital services — telecommunications providers, e-commerce platforms, and financial technologies (Fintech).

16 companies were evaluated in all four countries.

	Telecom operators	**e-commerce**	**Fintech**
Kazakhstan	Kcell KaR-Tel	OLX Group	Kaspi Bank
Kyrgyzstan	Sky Mobile Nur Telecom	YALLA Classifieds OÜ	Optima Bank
Tajikistan	TT Mobile Indigo Tajikistan	Rashod	Alif Bank
Uzbekistan	Unitel Coscom	OLX Classifieds	Kapitalbank

We partnered with Ranking Digital Rights (RDR), who provided guidance and support throughout the research process. Since 2013, RDR has been a leading organization in the tech corporate accountability field, studying and challenging the status quo of Big Tech companies through the publication of the RDR Corporate Accountability Index and, more recently, the 2022 Big Tech Scorecard. RDR developed a methodology that is regarded as a gold standard in assessing how the policies and practices of technology companies affect human rights, with a special focus on the rights to privacy and freedom of expression. RDR's methodology is grounded in the Universal Declaration of Human Rights and the UN Guiding Principles on Business and Human Rights. The RDR Corporate Accountability Index methodology comprises 58 indicators across three categories — governance, freedom of expression, and privacy — with more than 300 questions in total, that assess companies' transparency and normative practices and are informed by relevant literature,

case studies and best practices, and human rights risk scenarios that anticipate potential harms that can result from poor company policies and practices[30].

Since 2016, civil society organizations have adapted the RDR methodology to study technology companies around the globe. This is the first time RDR methodology has been used to evaluate local digital services in Central Asia.
For this study, RDR methodology was used to assess key digital services in four countries, including online banking and Fintech, as well as e-commerce platforms and telecommunications companies. We believe that the COVID pandemic has become a catalyst for a boom in online shopping and banking in Central Asia and that this will lead to wider use of digital services. Banks and businesses are producing more and more online services, attracting a rising number of customers from diverse age groups who provide their personal data and agree to the rules set out by the digital service providers without understanding the implications.

CIPI believes, therefore, that it is important to examine emerging issues human rights, privacy, and digital rights as Fintech and online shopping play an increasingly prominent role in Central Asian society. This study has provided an opportunity to understand the nuances of RDR methodology when applied to digital service providers that fall beyond the scope of human rights monitoring.

For this research, CIPI selected a subset of the indicators from the 2020 Corporate Accountability Index methodology[31], focusing on the following issues:

- Governance: Policy commitments to respect human rights and management oversight, evaluated at the parent level of the companies.
- Access to terms of service, enforcement processes, account, and content restrictions.
- Internet shutdowns and zero–rating practices (applicable only to telecommunications companies).
- Access to privacy policies, inference of user information, data protection standards (collection of user data, sharing and retention).
- Process for responding to government demands for the disclosure of user information.

To evaluate the selected indicators, the research looks at publicly available information on each company's website. The indicators in the governance category are the only ones evaluated at the group level — e.g., the owner and controlling company of the local entity. For example: Beeline, a telecommunications provider, is a subsidiary of the Dutch group VEON, while OLX Group, a multinational classifieds platform, is owned by the Dutch internet group Prosus.

The research methodology involved the following steps:

[30] https://rankingdigitalrights.org/rankings-report-cards/
[31] https://rankingdigitalrights.org/2020-indicators

Step 1:

Primary data collection. On each company's website, the researchers looked at the following:

- Relevant policy documents,
- Other contractual or legal documents about the services
- The company's blog.
- Transparency reports
- Other official web pages that might provide relevant information for answering the questions under each indicator and setting a score.

Step 2:

Secondary review. The researchers, together with CIPI's team, cross–checked the data collected and the preliminary findings.

Step 3:

Review and reconciliation: The CIPI team, Internews and RDR discussed the results of steps one and two to resolve differences, and to apply a unified and objective approach that ensures the indicators have been evaluated consistently.

Step 4:

Final Scoring: The RDR team provided the technical infrastructure to access the final scores assigned to each company and service.

EVALUATION AND SCORING:

Each indicator has a list of elements, and companies receive credit (full, partial, or no credit) for each element they fulfill.

The evaluation includes an assessment of the disclosure for every element of each indicator, based on one of the following possible answers:

a) **Yes**/ full disclosure. Company disclosure meets the element requirement.
b) **Partial**. Company disclosure has met some but not all aspects of the element, or the disclosure is not comprehensive enough to satisfy the full scope of what the element is asking for.
c) **No disclosure found**. Researchers were not able to find information provided by the company on their website that answers the element question.
d) **No**. Company disclosure exists, but it specifically does not disclose to users what the element is asking. This is distinct from the option of "no disclosure found," although the result in both cases in no credit.

e) **N/A**. Not applicable. This element does not apply to the company or service. Elements marked as N/A will not be counted for or against a company in the scoring process.

POINTS

- Yes/full disclosure = 100
- Partial = 50
- No = 0
- No disclosure found = 0
- N/A excluded from the score and averages.

By using the RDR methodology, we were able to assess each company's status and offer a roadmap to help them improve their policies and practices. The results of this research will help businesses in providing greater security and trust to their users, mitigating potential reputation risks that result from data breaches and dubious privacy practices. We hope this study will lay the foundation for an ongoing scrutiny of the policies and practices of online services, increasing the efforts to respect and protect human rights in the digital space.

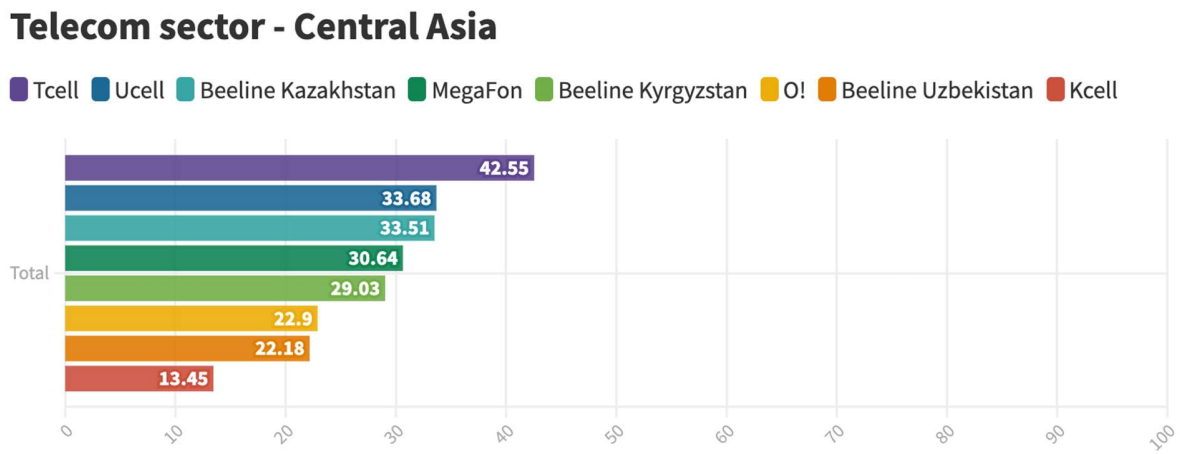
V. Main Findings

The consolidated results are predicated on respect for digital rights in terms of the governance, freedom of expression, privacy policies, and protection of personal data. Research was carried out on 16 companies. Some performed better than others, but there's still vast room for improvement in corporate policies on privacy and data protection. The policies we reviewed were poorly considered and implemented and are not in compliance with the UNGP's call for businesses to respect human rights.

- Apart from Beeline's subsidiaries in Kazakhstan and Uzbekistan, digital service providers do not disclose any information about their board of directors and executive staff. We were, however, able to find some information about company employees on other websites. LinkedIn was particularly useful in helping us understand company structures and departments.
- None of the companies publish transparency reports online. However, some — like OLX Kazakhstan— have been nominated for awards or mentioned in the parent organization's annual reports. They are subjected to audits and other routine reporting, but all we could find online was Tcell's 2012 annual report, which was only one page long and included scant information.
- All the digital service providers we studied comply with domestic laws that require new users to present their government identity card or passport when registering. None of the companies provide an option for users to register anonymously.
- All the companies disclose user information to government bodies, upon request and without a court order, under the pretext of anti–fraud and anti–terrorism activities.
- All the telecommunications companies we evaluated have a history of filtering websites and even shutting down the internet entirely. None, however, discloses their policies regarding government requests to shut down the internet or the specific services they provide. According to the companies they do disclose information related to technical shutdowns or emergency situations, but overall they do not publish any disclosure on their sites.
- None of the companies disclosed how they handle personal data — i.e., its processing and storage, or what happens to a user's data after they close their account. It is impossible to verify that a company has deleted a former user's data from their servers, even in cases where the companies claim in their policies that they do not retain the data.
- All the companies disclose sharing some data with third parties, without regard to how the data might be used. All the countries covered in this report have legislation on the books, which stipulates that consent of the owner is mandatory for data to be transferred to third parties.

- Companies are not required to notify users of policy changes. Instead, the onus is on the user to check the company website for news of changes. Nor do most companies retain an archive of older policies OLX's subsidiaries in Kazakhstan and Uzbekistan are exceptions.
- Both the privacy policies and the terms of service are usually long, complex legal documents. For example, OLX Kazakhstan's privacy policy is more than 40 pages long. None of the companies help their users understand the clauses in their policies. Thus, the average user is very unlikely to read the policies carefully.
- All the companies evaluated provide their policies in the respective local languages and in Russian. Some companies — such as Tcell, Kcell, Beeline Kyrgyzstan and Beeline Kazakhstan — make their policies and contracts available in English, but only the documents in Tajik and Russian are legally binding.

VI. Telecom Companies



TOTAL COMBINED SCORE COMPRISING OF ALL INDICATORS OF THE TELECOM SECTOR

GOVERNANCE

G1. POLICY COMMITMENT

VEON is the main player in the telecommunications sector studied for this paper. Founded in Moscow in 1992 as VimpelCom, a Russian telecommunications company, it rebranded in 2017 to expand beyond telecommunications services. Now based in the Netherlands, VEON controls various brands across Central Asia and provides services to a combined population of 680 million.[32] VEON's portfolio includes services in e-commerce, Fintech, and streaming, but their primary industry is the telecommunications sector, with Beeline as the leading brand. For this study we evaluated Beeline's subsidiaries in Kazakhstan[33], Kyrgyzstan[34], and Uzbekistan.[35] As a European entity, VEON shows in its policies a strong commitment to human rights and freedom of expression, reflecting EU laws and regulations that impose requirements to protect user privacy and freedom of expression. But Beeline's subsidiaries in Central Asia either fail to comply with the parent company's policies or do so selectively. For example, Beeline's country–specific websites contain no clear indications that VEON's partnership codes are fully enforced, or that it has monitoring and enforcement mechanisms in place.

[32] https://www.veon.com/our-brands/
[33] https://beeline.kz/ru/about
[34] https://beeline.kg/ru/about-us
[35] https://beeline.uz/ru/about

VEON purportedly requires all its brands to comply with its code of conduct, but that is not the case for the subsidiaries we evaluated. Beeline Kazakhstan, which makes its policy available in Kazakh, Russian, and English, includes an explicit statement on human rights and privacy:

> Human rights business partners will respect and promote universal human rights as stated in the United Nations' Universal Declaration of Human Rights. Business Partners will not aid human rights abuses of any kind and will respect the personal dignity, privacy and rights of each individual at all times. Business partners will not tolerate any unacceptable treatment of employees, such as but not limited to mental cruelty, physical abuse, mistreatment of persons with disabilities, slavery and sexual harassment[36].

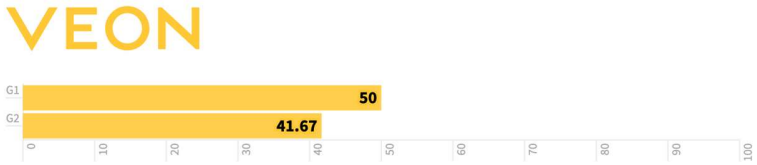
Beeline Uzbekistan also adopted the code of conduct, making it available in Uzbek and Russian. It includes an explicit statement on human rights[37] and privacy like that of Beeline Kazakhstan. Beeline Kyrgyzstan, however, altered the human rights statement. According to the English[38] and Russian[39] versions in the section on labor and human rights, "business partners will respect and promote universal human rights as stated by the United Nations" and respect privacy and confidentiality.[40]

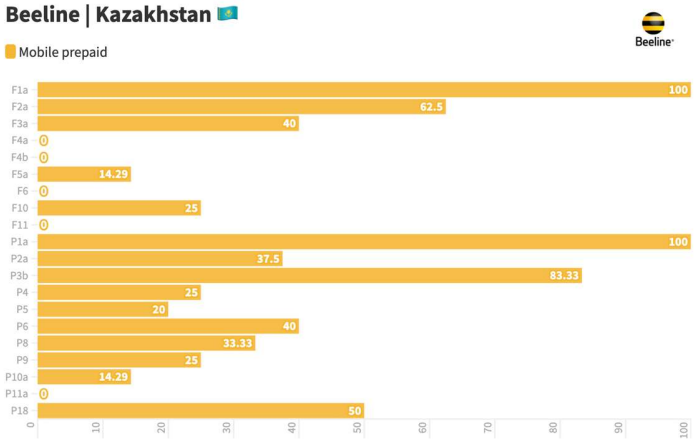
None of the companies commit explicitly to the right to freedom of expression.

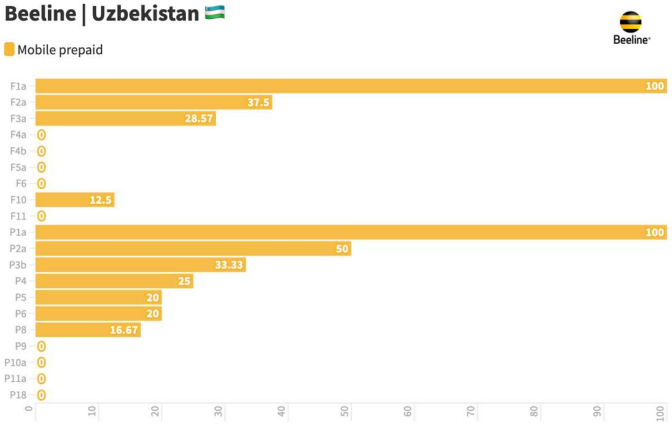
The question is, can VEON force its subsidiaries in Central Asia to adopt the company's code of conduct? Currently, all the subsidiaries put their business reputations first. Only Beeline Uzbekistan provides information on its website about its compliance with Speak UP. VEON maintains several confidential tools that can be used to report potential violations of the law, of VEON's code of conduct and/or its policies or procedures. VEON guarantees data security and anonymity of requests.

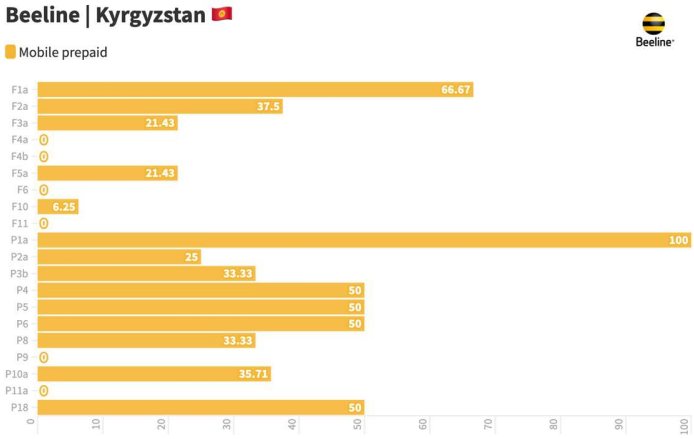
---

[36] https://beeline.kz/binaries/content/assets/example/2017-10-31-bp-code-of-conduct-final---kar-tel.pdf?isFrame=true
[37] https://beeline.uz/binaries/content/assets/other-documents/compliance/kodeks_povedeniya_biznes_partnerov_ru.pdf
[38] https://beeline.kg/binaries/content/assets/example/poleznye-documenty/%D0%BA%D0%BE%D0%B4%D0%B5%D0%BA%D1%81-%D0%BF%D0%BE%D0%B2%D0%B5%D0%B4%D0%B5%D0%BD%D0%B8%D1%8F-%D0%B1%D0%B8%D0%B7%D0%BD%D0%B5%D1%81-%D0%BF%D0%B0%D1%80%D1%82%D0%BD%D0%B5%D1%80%D0%BE%D0%B2-%D1%80%D1%83%D1%81%D1%81.pdf
[39] https://beeline.kg/binaries/content/assets/example/poleznye-documenty/%D0%BA%D0%BE%D0%B4%D0%B5%D0%BA%D1%81-%D0%BF%D0%BE%D0%B2%D0%B5%D0%B4%D0%B5%D0%BD%D0%B8%D1%8F-%D0%B1%D0%B8%D0%B7%D0%BD%D0%B5%D1%81-%D0%BF%D0%B0%D1%80%D1%82%D0%BD%D0%B5%D1%80%D0%BE%D0%B2-%D1%80%D1%83%D1%81%D1%81.pdf
[40] https://beeline.kg/binaries/content/assets/example/poleznye documenty/%D0%BA%D0%BE%D0%B4%D0%B5%D0%BA%D1%81-%D0%BF%D0%BE%D0%B2%D0%B5%D0%B4%D0%B5%D0%BD%D0%B8%D1%8F-%D0%B1%D0%B8%D0%B7%D0%BD%D0%B5%D1%81-%D0%BF%D0%B0%D1%80%D1%82%D0%BD%D0%B5%D1%80%D0%BE%D0%B2-%D1%80%D1%83%D1%81%D1%81.pdf
https://beeline.kg/binaries/content/assets/example/poleznye-documenty/%D0%BA%D0%BE%D0%B4%D0%B5%D0%BA%D1%81-%D0%BF%D0%BE%D0%B2%D0%B5%D0%B4%D0%B5%D0%BD%D0%B8%D1%8F-%D0%B1%D0%B8%D0%B7%D0%BD%D0%B5%D1%81-%D0%BF%D0%B0%D1%80%D1%82%D0%BD%D0%B5%D1%80%D0%BE%D0%B2-eng.pdf









We also examined TeliaSonera,[41] a European telecom. Megafon[42] is a Russian mobile service provider that is state–owned in Tajikistan, where it has 1.6 million users, while Kcell is owned by Kazakhtelecom[43] and Ucell of Coscom[44] is state–owned in Uzbekistan. Tcell[45] has, since 2017, been a subsidiary of the Aga Khan Fund for Economic Development (AKFED)[46], which is headquartered in Europe. AKDN's website shows clear policies but omits a commitment to human rights and freedom of expression. Instead, AKDN and AKFED commit to AKDN's ethical framework, which specifies a "collective focus on respect to human dignity and relief to humanity, the reach of their mandates beyond boundaries of creed, color and race and nationality."[47]

---

[41] https://www.teliacompany.com/en. TeliaSonera that was not part of the research, since they are no longer the parent/operating company

[42] Telia Sonera owned 25% of Megafon until October 2017.

[43] TeliaSonera owned KCELL until December 2018 when TeliaSonera sold it to State owned Kazakhtelecom https://www.kcell.kz/en/about

[44] https://ucell.uz/ru/myucell/about_company

[45] TeliaSonera owned 60% of Tcell until it was sold in April 2017, currently subsidiary of AKFED

[46] https://www.tcell.tj/corporations/about-tcell/tcell-shareholders.php

[47] https://d1zah1nkiby91r.cloudfront.net/s3fs-public/ethical-factsheet.pdf

AKDN's ethics policy does not mention freedom of expression explicitly but does specify respect for pluralism[48]. Tcell's policies include no mention of human rights or freedom of expression; nor does the telecom indicate compliance with its parent company's ethical framework.

Ucell/Coscom, MegaFone Tajikistan, and O! Kyrgyzstan make no explicit reference to human rights or freedom of expression. Its code of ethics stipulates "priority of the rights, freedoms and legitimate interests of citizens" and that "the company respects the right to privacy and ensures the confidentiality of personal data in accordance with the laws of the Republic of Uzbekistan."[49] According to the privacy policy on its website, Coscom/Ucell "supports and complies with the norms of international law and standards related to human rights" and protects their customers' privacy.[50]

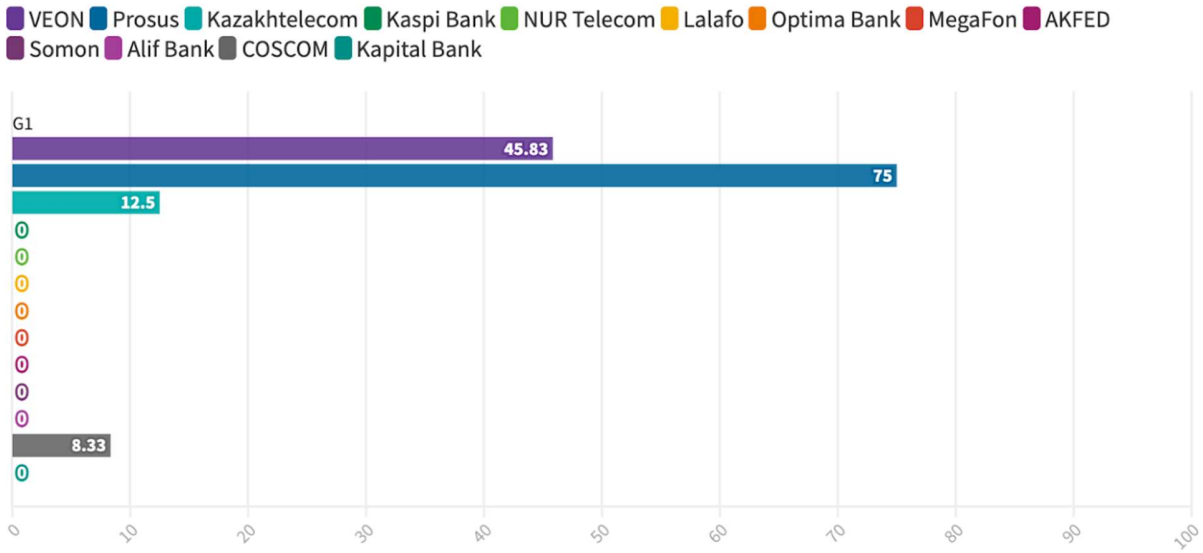
In Kazakhstan, Kcell references Kazakhtelecom's business code of conduct, which stipulates respect for "the dignity, rights and personal freedom of an individual, trust in employees and equal rights for all."[51] According to the statement in its privacy policy Kcell upholds international human rights and respects their customers' right to privacy.[52]

Neither Tcell, Kcell, or Ucell discloses any policy commitments to freedom of expression.

G2. Governance and management oversight

Beeline Kazakhstan[53] and Beeline Uzbekistan[54] include on their websites information about their boards of directors and management, but Beeline Kyrgyzstan does not.[55] None of the companies, however, disclose the roles of the executives or the boards of directors; nor do they whether or how management has oversight over practices that affect freedom of expression and information. Although ACFED/AKDN in the case of Tcell[56] have detailed information on the boards of directors of the network, but Tcell does not have information listed about the Board and the staff of the company at all. Neither Kcell, nor Nur Telecom (mobile operator O!) nor Ucell discloses information on their board of directors, their staff, or their respective roles. Megafon-Tajikistan lists on the name of its executive director listed on the company website, with no information about the board of directors.

[48] https://d1zah1nkiby91r.cloudfront.net/s3fs-public/ethical-factsheet.pdf
[49] https://ucell.uz/ru/myucell/sustainability/code_of_ethics
[50] https://ucell.uz/ru/useful_info/confidentiality
[51] https://telecom.kz/storage/uploads/6b/41/51886b2f4143e109a0ee92b6e927827230e04f41/TxdjqmVUBWA08ePtuu5gUY4DfgxQ0Eojczh8ZOfB.pdf
[52] https://www.kcell.kz/uploads/2022/4/27/5e09a07e87c6fa9a19d0d2e050206471_original.639742.pdf
[53] https://beeline.kz/ru/about/rukovodstvo
[54] https://beeline.uz/ru/about/managementcompany
[55] https://beeline.kg/ru/about-us
[56] https://beeline.uz/ru/about/managementcompany



TOTAL SCORE ON GOVERNANCE INDICATORS IN THE TELECOM SECTOR

FREEDOM OF EXPRESSION

F1. Access to policies

All the telecom companies provide relatively easy access to the policies, legal documents and terms of use — i.e., Beeline Kyrgyzstan's[57] policy appears on the company website in Kyrgyz and Russian, while Beeline Kazakhstan's appears in Kazakh and Russian. Beeline Kyrgyzstan provides English versions as well. Beeline Uzbekistan provides easy access to all legal documents[58] in Uzbek and Russian.

Tcell's subscriber contract is available in Tajik, Russian, and English. In section 7.6, of the contract, the company stipulates that customers may choose their contract in Tajik or in Russian, and that both have equal legal weight.[59] While Kcell's user agreement can be located only by executing a search[60] Kazakhtelecom's user agreement at the bottom of the homepage[61]. And while Kcell's

[57] https://beeline.kg/binaries/content/assets/example/poleznye-documenty/%D0%B4%D0%BE%D0%B3%D0%BE%D0%B2%D0%BE%D1%80-%D0%BE%D0%B1-%D0%BE%D0%BA%D0%B0%D0%B7%D0%B0%D0%BD%D0%B8%D0%B8-%D1%83%D1%81%D0%BB%D1%83%D0%B3-%D1%81%D0%BE%D1%82%D0%BE%D0%B2%D0%BE%D0%B9-%D1%81%D0%B2%D1%8F%D0%B7%D0%B8.pdf
[58] https://beeline.uz/ru/yuridicheskie-dokumenty
[59] https://www.tcell.tj/en/
[60] https://static.kcell.kz/page/legal/public-agreement-rus-22.pdf
[61] https://telecom.kz/

website is in three languages — Kazakh, Russian and English — the user agreement appears in Russian only. The terms of service for Megafon were easy to locate, in Tajik and Russian, while O! (Nur Telecom) displayed theirs in Tajik and Russian.

Notification of policy changes

All telecom companies use different means to inform their users of changes. For example, Beeline Kyrgyzstan sends SMS messages or posts relevant information on their website, except in cases where the changes have no negative impact on the user.[62]

Ucell and Tcell inform users about changes in their services by posting updates on their websites, sending SMS notices and via mass media. Kcell informs users of most changes by SMS — except updates on tariffs, which they post only on the website.

Some companies maintain online archives, but they can be difficult to find on the company website. Ucell's archives — of services, tariffs, and corporate tariffs— could be found only through the search option.[63] Some companies keep archives of information beyond policies. Tcell, for example, keeps users' account activity history —i.e., the date, time, duration and cost of incoming and outgoing calls and the number of SMS messages sent. [64] Tcell also retains a record of telephone messages left by users with the operator, for the purpose of changing the package of services or making claims.[65] Beeline Kazakhstan also retains the archive of its products and services.[66]

MegaFon and O! (Nur Telecom) update their subscribers via SMS notifications, mass media, and website posts.

Network shutdowns and government demands to restrict content and limit user accounts

All the companies comply with government demands to restrict access to certain websites. Beeline Kazakhstan's public agreement stipulates that by signing their contract, the user allows the company to give their personal data to third parties, including state law enforcement and judicial authorities. [67]

---

[62] (Clause 3.2. Agreements https://beeline.kz/binaries/content/assets/public_offer/public_offer_ru.pdf
[63] https://ucell.uz/ru/search?q=%D0%B0%D1%80%D1%85%D0%B8%D0%B2&form-button=%D0%9F%D0%BE%D0%B8%D1%81%D0%BA
[64] Tcell Subscriber Contract
[65] Ibid
[66] https://beeline.kz/b2b/ru/products/archived/tariffs
[67] https://beeline.kz/binaries/content/assets/public_offer/public_offer_ru.pdf

Beeline Uzbekistan's user agreement stipulates that the company has the right to "centrally manage telecommunications networks and facilities and public internet access points, as well as limit or suspend their operation."[68] And under circumstances of emergency situation announced the based for potential internet shortages are explained as following: "6. Force Majeure 6.1. ...Force majeure means extraordinary events or circumstances which could not be foreseen or prevented by the Parties accessible to them. Such "extraordinary events or circumstances" include, but not limited to: fires, acts of third parties, natural disasters (floods, earthquakes, etc.), military actions, actions or regulations of authorized governing bodies of the Republic of Uzbekistan, as well as any other circumstances, beyond the reasonable control of the Parties, the extraordinary nature of which the parties could neither foresee nor prevent"[69].

Tcell's user contract stipulates that the company is not accountable for partial or full performance of its obligations, as well as non-performance or improper performance of its obligations if it fails to act as a consequence of force majeure circumstances. The companies defer to government requests to limit services or change the form and procedure for payment. And in the event of an emergency (military actions, natural disasters, quarantines, etc.), the company reserves the right to filter or block of IP address and to prevent the user from information resources and internet services (addresses, sites, servers, teleconferences, mailing lists, etc.) both in Tajikistan and abroad. Access restrictions are also introduced if the user violates generally accepted norms for internet use. The state also retains the authority to suspend or limit services in the event of an emergency — e.g., military actions, natural disasters, quarantines.[70] Chi Gap, a Tcell application for smartphones that is similar to WhatsApp, notifies users in its privacy policy that the company "reserves the right to make changes, suspend, delete or block the user at any time if they the terms of the contract —or if the government orders the company to do so. The company also stipulates that it will provide user information to government authorities upon request.[71]

All the companies have, on occasion, shut down their networks at the request of state authorities. Users are informed about these shutdowns retroactively, via social media and the company websites. After internet access in Kazakhstan was disrupted for a week during the January 2022 anti–government protests[72], Beeline Kazakhstan posted a brief apology in the news section on its website. The company attributed the suspension of services to reasons beyond their control and offered their users financial compensation for the inconvenience.[73] Kazakhtelecom generally posts

[68] https://beeline.uz/binaries/content/assets/example/publicoferta-25122018ru.pdf
[69] Ibid , https://beeline.uz/binaries/content/assets/example/publicoferta-25122018ru.pdf
[70] Subscriber contract https://tcell.tj/en/links/subscribers/subscription-agreement.php
[71] TCELL http://tcell.tj/internet/mobile-apps/pconf.pdf
[72] https://www.cfr.org/blog/consequences-internet-shutdowns-kazakhstan
[73] https://beeline.kz/ru/events/news/compensation.html

notices about suspensions of service to its website, as does Kcell. But they posted no information about the suspension of internet and mobile services in January 2022.

After Tajikistan shut down its internet services in Gorno–Badakhshan due to political tensions, Tcell posted an update to its website on March 16, 2022 that attributed the suspension of service to weather conditions. [74] MegaFon posted a similar notice on March 22 in the news section of its website.
Internet access was blocked in Kazakhstan during the Karakalpakstan protests of July 2022,[75] but Beeline Uzbekistan made no reference to those events. Instead, it informed users that the company had carried out some maintenance work from July 5 – 6. [76]

Beeline Kyrgyzstan did not cite the Alatoo riots when explaining why their mobile and internet service was disrupted.[77] Instead the company told users, via its official Twitter account, that mobile service had been interrupted due to heavy network traffic.[78] In the news section of its website, the company ascribed suspended internet service to planned work on the networks. [79]

In December 2021 O! Kyrgyzstan of Nur Telecom informed users via the news section on its website that service had been disrupted the previous day due to a breakage of the optical cable on partner network, which cased temporary interruptions in communications and mobile internet in Jalal–Abad, Osh, Naryn and Batken. The company apologized and offered users 2 GB of free data as compensation.

Identity policy

All the companies require new subscribers to present their national ID or passport when registering for an account, to comply with local laws. Ucell's user agreement stipulates that the user will, upon request, present their ID when contacting customer service.[80] In the section on how to become a new subscriber, Tcell Tajikistan's website stipulates that a domestic user must be a citizen and must present a national ID card; foreign passport holders, including naturalized citizens, must show that they are registered with government authorities.[81] Kcell registration form specifies that users must provide original documents to prove their identity.[82]

---

[74] https://www.tcell.tj/content/news/gbao/?sprase_id=54754
[75] RFL " August 1. 2022. Two major national mobile operators shut down mobile Internet and text and picture messaging from 0830 to 1330, citing "urgent maintenance work on telecommunications networks." https://www.rferl.org/a/uzbekistan-sms-internet-university-exam-police-cheating/25477815.html
[76] https://beeline.uz/ru/events/news/profilkticheskie_raboti_v_beepul_05-06_07_2022.html
[77] https://ru.sputnik.kg/20201006/V-Bishkeke-ne-rabotaet-sotovaya-svyaz-Operatory-obyasnili-pochemu-1049888349.html
[78] https://twitter.com/BeelineKG/status/1313193111435259904
[79] https://beeline.kg/ru/events/actions
[80] https://ucell.uz/media/files/docs/Public_offer_prepaid_ru.pdf
[81] https://www.tcell.tj/en/links/subscribers/connection.php
[82] https://static.kcell.kz/page/legal/public-agreement-rus-22.pdf

Beeline Uzbekistan in Public Agreement imposes detailed demands on new subscriber, who must, in addition to the usual required information — i.e., last name, first name, patronymic, place of permanent or temporary residence, and the number of their national ID — present another document, such as a passport or a driver's license, or military ID card, which shows the user's place of residence and is notarized to confirm its authenticity.[83]

Beeline Kazakhstan requires new subscribers to fill out a registration form, in which they agree to provide the company with original identity documents. The registration form stipulates that the company reserves the right to request extensive personal information from the user. Businesses must provide proof that they are legally registered as a business, along with their tax registration; individuals, meanwhile, must provide — in addition to their first name, surname, and patronymic, their email and home addresses — the number and issuing date of their identity card, their state ID number, and the subscriber's identity number of mobile device.[84]

Beeline Kyrgyzstan informs users via its website that the company collects the following data: Full name, date of birth, address, complete details shown on the user's identity document, telephone number, email address, and gender. This data, the company informs potential customers, is "the minimum necessary" to register in compliance with the law in Kyrgyzstan.[85]

O! Kyrgyzstan (Nur Telecom) requires an identity document to register. MegaFon Tajikistan requires new users to show a national ID or passport to register. MegaFon Tajikistan's service agreement notes that it requires users to present proof of identity in compliance with state law.

PRIVACY

Access to privacy policies

Most digital service providers post their privacy and confidentiality policies at the bottom of the homepage. Beeline Kyrgyzstan posts their policy in Kyrgyz and Russian, in the section called "legal documents." Beeline Kazakhstan posts its policies alongside the user agreement and other documents,[86] in Kazakh and Russian. Beeline Uzbekistan posts its legal documents at the bottom of the homepage; it explains, in Uzbek and Russian, the company's policy regarding the collection,

[83] https://beeline.uz/binaries/content/assets/example/publicoferta-25122018ru.pdf
[84] https://beeline.kz/binaries/content/assets/public_offer/public_offer_ru.pdf
[85] https://beeline.kg/ru/legal-information
[86] https://beeline.kz/binaries/content/assets/public_offer/privacy/privacy-ru, https://beeline.kz/binaries/content/assets/public_offer/privacy/privacy-kk

processing and protection of personal data. Ucell's policy is posted in Uzbek, Russian, and English, at the bottom of the homepage, in the section called "useful information.[87] Kcell posts its policy on the left side of the homepage, in a section called "confidentiality policy," but only in Russian.[88] Tcell does not post its privacy policy on its homepage, but does make it available in Chi Gap mobile program[8990]in Tajik, Russian, and English.

Neither MegaFon Tajikistan nor O! (Nur Telecom) post their privacy policies on their websites. A Google search yields this link to a .pdf document, available in Russian only, which summarizes MegaFon's user agreement. In the single paragraph of the document that describes the company's privacy policy, users are informed that by registering with MegaFon they consent to "the application of personal data processing procedures" and to "the transfer and processing of information" whether the user is in Tajikistan or abroad. The paragraph stipulates "the laws, regulations and standards of the country in which your information is stored and processed may differ from the laws of the Republic of Tajikistan." In other words, Tajikistan's laws will be applied even when the customer is using their mobile device in another country. O! does not post its privacy policy on its website, but a Google search yielded the documents in Russian and Kyrgyz.

P2. Notification of changes

P2(a). Changes to privacy policies

Beeline notifies users of changes to their privacy policies and/or practices only by posting it on their websites. In their user policies, the company's subsidiaries in Uzbekistan, Kyrgyzstan, and Kazakhstan request users to check the website regularly for updates.

Tcell stipulates that it "reserves the right to update or modify" its policies "at any time with or without notice."[91] Ucell's privacy policy does not include information on how customers are notified of changes, but a document called "subscriber's right to confidentiality" informs users that they should check the site regularly for updates to services. Kcell does not provide any information about updates to user policies.[92]

In most cases, the mobile service providers provide no prior notice notices of changes to their privacy policies. They post the updates on their websites the same day as the new policy is implemented. Since none of the companies send direct notifications to subscribers, the onus for staying informed is on the user.

---

[87] https://ucell.uz/en/useful_info/confidentiality,https://ucell.uz/ru/useful_info/public_offer
[88] https://www.kcell.kz/uploads/2022/4/27/5e09a07e87c6fa9a19d0d2e050206471_original.639742.pdf
[89] https://www.tcell.tj/en/mobile-apps/chigap.php
[90] in Tajik: https://www.tcell.tj/tj/mobile-apps/chigap.php ; in Russian https://www.tcell.tj/mobile-apps/chi-gap.php ; and English https://www.tcell.tj/en/mobile-apps/chigap.php,
[91] https://www.tcell.tj/en/mobile-apps/chigap.php
[92] https://www.kcell.kz/uploads/2022/4/27/5e09a07e87c6fa9a19d0d2e050206471_original.639742.pdf

Users Information and data collection practices

All the companies reviewed use similar practices of collecting of user information and storing the data but not limited to:

- Identification data — i.e., full name, date of birth, age, address, details of an identity document (name, serial number, date on which the document was issued, authority that issued the document), telephone number, and e–mail address, as well as demographic data and gender.
- Communication data regarding the services rendered as per the user contract — i.e., type of plan, method of payment, information obtained when visiting the service provider's website.
- Data on the user's mobile device — e.g., the operating system, signal strength, device ID and settings, names of installed software, and the subscriber's location/movement.
- Subscriber interaction data — e.g., services, information about orders, bills, advances and payments, marketing permissions and prohibitions, subscriber contact details and related records, such as calls to the call center.
- Data generated while the communication services are in use — e.g., calls and SMS, information about participants in calls and texts, duration of calls, data transfer protocols, and location data.
- Data collected by cookies and similar technologies when the user browses the internet.
- All the companies anonymize this data to produce reports about patterns in customer use of their devices.
- All the companies also refer to other data which they do not specify.

Beeline Kyrgyzstan informs its users that its policy for collecting personal data is predicated on the minimum requirements set out by the country's laws. Similarly, Beeline Uzbekistan cites compliance with the law when describing its policies on collecting user data, which includes collecting individual identification numbers, social identification number of individual, social network accounts, personal preferences, personal connections; model of the subscriber's device and the operating system it uses, IP address, MAC address, IMSI, and biometric data."[93]

Beeline Kazakhstan also cites the law in a 2013 document titled "On Personal Data and Its Protection," in which the company informs users that they are obliged to approve the list of personal

[93] https://beeline.uz/binaries/content/assets/other-documents/oferta/%D0%BF%D0%B5%D1%80%D0%B5%D1%87%D0%B5%D0%BD%D1%8C-%D0%BF%D0%B5%D1%80%D1%81%D0%BE%D0%BD%D0%B0%D0%BB%D1%8C%D0%BD%D1%8B%D1%85-%D0%B4%D0%B0%D0%BD%D0%BD%D1%8B%D1%85-%D0%B0%D0%B1%D0%BE%D0%BD%D0%B5%D0%BD%D1%82%D0%B0.pdf, https://beeline.uz/binaries/content/assets/example/publicoferta-25122018ru.pdf

data necessary and sufficient for fulfillment of their tasks, unless otherwise provided by laws Republic of Kazakhstan. In its approved list of personal subscribes, the company [94] divides the data into two categories — personal data, which is collected, and data that is accumulated. Overall, the range of data Beeline Kazakhstan collects is similar to other companies.

Tcell does not site Tajikistan's law on personal data, though it was passed in 2018. The subscriber agreement specifies that the company retains user data at its own discretion, in accordance with the law. The privacy policy for Chi Gap specifies that users must provide their phone number a (name and photo are optional); users of the app who are not Tcell customers must provide a copy of their passport and allow access to their mobile device's address book. The company stores the phone numbers and names in address book (but not emails, notes or any other personal Information) uses the information to: (a) inform the subscriber when the contacts become active on Chi Gap; (b) show which of the subscriber's contacts are already on the app; (c) correctly display the name of each contact as it appears in address book when a call is received; (d) synchronize contacts with the app, which runs on iOS. The copy of address book (names and phones) is stored on a live database, which is not backed up. If the subscriber deletes the address book from Chi Gap's servers, it will be deleted immediately. The subscriber's phone number will be used to identify them when they log into the app. The company also retains a call detail record (CDR) for each message and call made via the app. [95] Tcell's contract also notes that it retains a record of a telephone messages the subscriber makes to the company to change their service package.[96]

Ucell's right to data privacy document includes information about the user's gender and language, as well as information about participants in calls or group chats, call duration, data transfer protocols, location data, and data on devices used.[97] Kcell does not disclose any information.

O! (Nur Telecom) specifies in its privacy policy that the company retains user data from subscribers' social media accounts, including "last name, first name and patronymic, email, year of birth, gender, login and password information." It also retains information about the number, cost, and time of orders users place for the company's products or services, information about their participation in company promotions, about subscribing to information support services, their IP address, preferred browser, cookies, user location, access time, address of the requested page, and details about the device they use to access the company's services. MegaFon's service agreement details that the company retains at their discretion the user's personal data, subscriber number, services they use, and calls they make, in compliance with Tajikistan's laws.

---

[94] https://beeline.kz/binaries/content/assets/public_offer/privacy/privacy-list-ru
[95] Chi Gap Subscriber Contract
[96] Chi Gap Subscriber Contract
[97] UCell/Coscom Subscribers' right to data privacy,https://ucell.uz/ru/useful_info/confidentialityhttps://ucell.uz/ru/useful_info/confidentiality https://ucell.uz/media/files/docs/Public_offer_prepaid_ru.pdf

Sharing of user information

All the service providers share user information with third parties in much the same manner. Beeline Uzbekistan's user policy stipulates that the company shares user data with their partners, including transborder partners, in accordance with laws regarding confidentiality. Beeline Kazakhstan's personal data processing policy also states that by law the company can and may transfer the user's personal data to third parties. In addition, upon request from law enforcement authorities company may share the user's personal data and/or restrict user access to subscriber services.

Beeline Kyrgyzstan informs users in its privacy policy that the company shares user data with third parties (including transborder partners) and that it shares personal information with companies affiliated with the VEON Group. The agreement specifies that sharing user data with third parties is for both legal and commercial purposes — i.e., tailoring special offers and messages the company sends to users and facilitating transactions via the financial institutions with which they partner.

On Ucell's website the page titled Subscriber's Right to Data Privacy informs subscribers that the company shares their data with Coscom's data processers, who work on contract and might be located outside Uzbekistan. Ucell also shares user data with other telecommunications companies and with various service providers, such as billing companies. Foreign telecoms that provide mobile roaming services to Ucell customers when they are abroad may collect and process user data according to their own policies rather than those of Ucell's.

Tcell, via Chi Gap's privacy policy, informs user that the company might "if necessary, share personal information (excluding address book and related information) and traffic data with trusted partner service providers and/or agents — e.g., banking organizations payment providers, customer support, or hosting services." But Tcell acknowledges that while it will never a customer's address book with a third party, it will give access to law enforcement authorities upon request. As with Ucell, Tcell's user contract includes a clause that stipulates foreign telecoms with which the company has roaming agreements may apply their local legislative norms to the collection, storage, and transfer of user data —except for passport data — even when those laws are different from Tajikistan's.

Kcell does not disclose what information and data it collects and stores, but its privacy policy stipulates that the company has the right to share information. The company documents do not mention the types of user information, but in general they can be shared only with authorized bodies (which are specified in the Kcell and Kazakhtelecom's Privacy Policies). There is no mention of judicial and state bodies, but the company's relevant documents specify that it can transfer user data to authorized bodies, which can be considered third parties.

MegaFon Tajikistan does not disclose its policies regarding user data and third parties. It only specifies, in clause 10.8 of the contract, that it retains the right to use subscriber data as it wishes, if its policies are legal in Tajikistan.

In its privacy policy, O! informs subscribers that it does not share user data with third parties — "except as expressly provided for" by the laws of Kyrgyzstan.

Retention of user information

All the companies surveyed take nearly identical positions on the retention of user information. Because there is no clear monitoring system there is no transparency as to whether the companies delete subscriber data.

Beeline Uzbekistan informs subscribers that it retains their personal data "for as long as the company needs," purportedly to provide various subscriber services. Beeline says that they delete user data once they have processed it in accordance with the law in Uzbekistan.

Beeline Kyrgyzstan's personal data storage policy also indicates to subscribers that the company retains user data for processing, for an unspecified length of time as mandated by the laws of Kyrgyzstan. In the web page titled legal information Beeline informs subscribers that it retains the right to use their data to create aggregated and anonymized analytical information and reports — e.g., "to calculate the percentage of our customers in a particular region."

Beeline Kazakhstan's privacy policy includes "terms of personal data storage," which specifies that the company retains user data for "as long as necessary" to complete collection and processing , after which it will be destroyed, in accordance with the law in Kazakhstan.
Ucell's website has a section in its "subscriber's right to privacy" titled "how long do we keep your data?" The answer: for the [unspecified] period necessary— "except where a longer retention period is required or permitted by Uzbekistan law. Once they have finished processing the data, Ucells says, they delete or anonymize it.

Tcell's privacy policy contains mixed messages. Section six specifies that if the company detects no subscriber use of Chi Gap for 90 days it will assume the subscriber deleted the app, in which case Tcell will remove the subscriber's address book from its servers. On the other hand, since Tcell cannot be *certain* that the subscriber deleted the Chi Gap app, the company will not deactivate the account — i.e., retain the subscriber's phone number and device ID.

Tcell's subscriber contract stipulates that the company retains records of messages from the user to the company for the purpose of changing the subscriber's service bundle or for making a claim against the company. Tcell's contract also notes that the company retains, at its own discretion and in accordance with the laws of Tajikistan, all the information provided by the subscriber — i.e., personal data, subscriber number, information on the services provided, and information about the subscriber's calls.

Kcell does not disclose what types of user information it retains, but the company's privacy policy specifies that it does not "retain personal data for longer than required by law" and notes that the purpose of retaining user data is quality control of customer service. Kcell assures its users that once the data has been processed it is deleted or anonymized. Kazakhtelecom does not provide any information about its policies regarding retention of user data.

MegaFon – Tajikistan's user contract stipulates on page 4 (clause 2) that it retains an electronic record of the personal information provided by the subscriber. The company does not, however, specify what information is they collect from the subscriber. O! does not any information about its policies regarding the retention of user data.

Users' access to their own user information

All the companies surveyed for this study provide policies on user access to their own information. In many cases, however, it is unclear how long it takes to obtain that information and what details it includes.

According to Beeline Kazakhstan's public agreement, the company is obliged to provide a customer service helpline that is available 24/7. Upon request from the subscriber, the company is also obligated to provide account updates by SMS or the automatic service system. According to its privacy policy, Beeline Kazakhstan will provide subscribers, upon request, with a list of companies that have access to their personal data, as well as information about how the data is used and stored. Similarly, if a Beeline Kazakhstan subscriber wants the company to make any changes to their personal data they must submit a request in writing.

Beeline Uzbekistan's policy is the same as Beeline Kazakhstan's. Users can submit a request in writing to receive information about the processing, storage, and sharing of their personal data. Beeline Kyrgyzstan publishes a summary of the subscriber's data rights in its privacy policy, which stipulates that users have the right to receive a copy of the data the company holds about them upon submitting a written request.

The information about confidentiality on Ucell's website also notes that subscribers can submit a request for information about their data, just as they can request itemized bills.

Tcell's subscriber contract includes a clause (1.1.30) titled "account activity history" that informs users of their right to request information on the date, time, duration, and cost of their incoming and outgoing calls and on the number of SMS they send.

Kcell and O!, however, do not provide the user with any information about their data.

MegaFon Tajikistan indicates in clause 11.6 of its user contract that it provides subscribers with information about their service tariffs, the territory covered by mobile service and the state of the user's account (tariffs owed), as well as updates about technical issues that might prevent the subscriber from accessing services.

Process for responding to government demands for user information.

All the companies surveyed comply with government demands for user information. Beeline Kazakhstan notes on its website page titled "public offer" (clause 8.2 under section 5) that law enforcement authorities can stop and/or restrict provision of services to the subscriber, per the laws of Kazakhstan.

Beeline Kyrgyzstan specifies to subscribers that the company might transfer user data "to law enforcement agencies, state authorities and other organizations" if they need to do so in order comply with the laws of Kyrgyzstan. Beeline Uzbekistan does not disclose any information about its policies regarding demands from law enforcement for user data.

Ucell informs its customers that the company provides user information to law enforcement, legal or judicial authorities upon request, in compliance with the law in Uzbekistan.

Tcell emphasizes in its Chi Gap privacy policy that it does not "rent, sell, or share" subscriber information to third parties, but acknowledges that it may provide the information to legal or law enforcement authorities, if necessary, to comply with the law in cases of "national security, law enforcement, or other issues of public importance." Chi Gap's user agreement stipulates in section 4 ("restrictions on the use of the Chi Gap app") that the company reserves the right to make changes, suspend, delete, or block the user if they breach of the terms of the contract, or upon receiving an order from government authorities in Tajikistan. Section 12 of Chi Gap's Privacy Policy ("disputes and resolution") specifies that all disputes between the subscriber and the service provider shall be resolved through negotiations. If the parties are unable to resolve their dispute, the laws of Tajikistan require the matter to be resolved in court. Section 6 of Tcell's subscriber agreement

("special conditions") specifies that the company–subscriber relationship is regulated by of Tajikistan's telecommunication laws.

Kcell does not disclose in its subscriber agreement what information and data it collects and accumulates. Nor does company documents mention what types of user information it shares — only that it does share information with "authorized" bodies, without specifying judicial and state authorities.

MegaFon (clause 10.8. of the user Agreement (MegaFon-Tajikistan) states that it uses the subscriber's personal data —subscriber number, information about the services provided, information about the subscriber's calls — at its own discretion and in accordance with the law in Tajikistan.

P18. Inform and educate users about potential risks

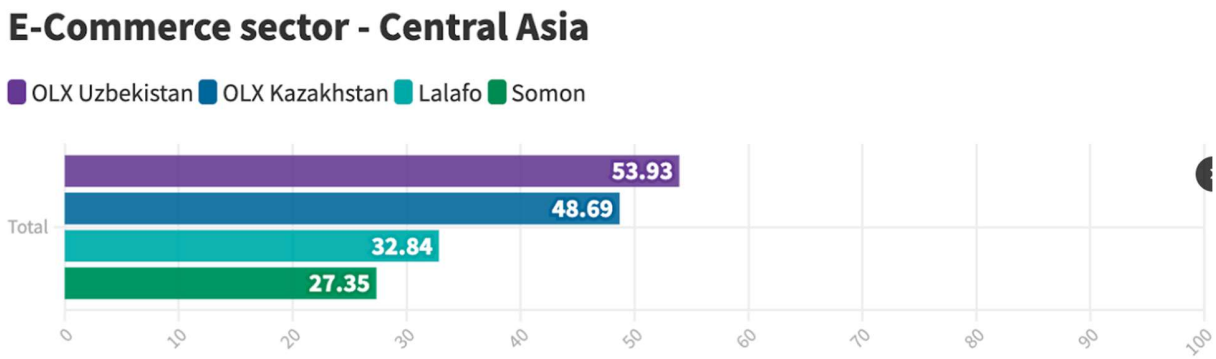
Companies are obviously interested in the wellbeing and safety of their subscribers. Each has its own way of informing and educating them about potential risks.

Beeline Uzbekistan provides information and education on potential risks. It also has a hotline program called Speak Up, which allows users to report anonymously to compliance any concerns about the company violating the law or its code of conduct. Beeline Kyrgyzstan provides safety lessons in its Beeline Video Lessons section, which can be watched with special permission. Neither Beeline Kazakhstan nor Kcell provides its users with similar information or learning opportunities.

Ucell provides information about fraud prevention and a Speak Up line, with the company's recommendations for best practices.

Tcell's website provides various practical materials and information on how to avoid scammers. MegaFon and O! also offer practical information on how to avoid scammers.

VII. E-Commerce Companies



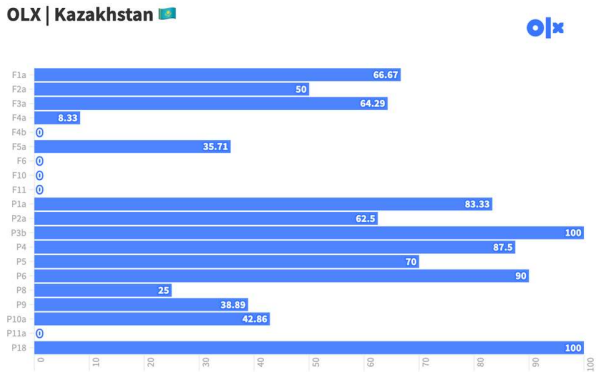
Despite some economic growth in recent years, economic diversification in Central Asia is low, with a high level of dependence on a small number of trading partners. E-commerce is still in the early stages of development in Tajikistan and Uzbekistan, although in 2018–21 the government of Uzbekistan approved a program for its development. The government of Tajikistan established an e-commerce development council under the auspices of the Chamber of Commerce and Industry, with the aim facilitating public–private dialogues to develop a more vibrant e–commerce ecosystem in Tajikistan.

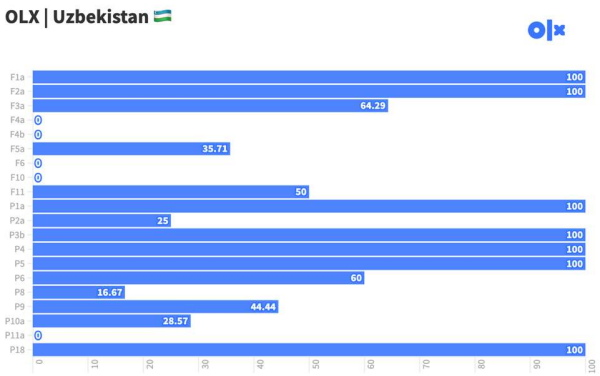
Since the e–commerce market is relatively young in Central Asia, the companies that provide e-commerce services have a very short history, although the covid-19 pandemic advanced the development of the e-commerce sector in the region. We reviewed four companies — OLX Uzbekistan, OLX Kazakhstan, Lalafo.kg in Kyrgyzstan and Somon.tj in Tajikistan. Our findings show that the majority of these companies have significant shortcomings in all four categories — from compliance with the law to user–friendly websites and inclusiveness. Online services that sell goods and services must specify clearly how the data is transferred to third parties, but these companies do not provide comprehensive information about how they ensure secure data storage or the geographical location of their servers.

Most, if not all, of these companies need to apply more rigorous practices to minimizing the user data they collect and to publishing their confidentiality policies in a simple and easily understood format on their websites. Nor do these companies indicate whether it is possible to submit a request to receive a copy of one's own personal data.

G1. Policy Commitment

G2. Governance and management oversight





Compliance. Table of Prosus/OLX Group/Olx.uz/ Olx.kz

OLX Uzbekistan and OLX Kazakhstan are subsidiaries of the Prosus/OLX Group. OLX Group adopted Prosus's human rights statement which, while comprehensive, does not include freedom of expression (except for gender expression) or freedom of information. All the annual report/ performance and sustainability reviews are explicitly about human rights, although the 2021 Prosus Annual report stipulates that its human rights statement describes an "approach covering topics that include remuneration, dignity at work, privacy and employee confidentiality, forced labor, and health and safety."[98] The authors of the annual report go on the specify that "as a global corporate citizen" the company is "committed to contributing to the advancement of universal human rights" in accordance with the UNGP. OLX's very detailed privacy statement[99] specifies that the company is cognizant of its responsibility "to uphold and support the rights of every individual, as set out in the UN Guiding Principles on Business and Human Rights." It continues: "As a wholly owned subsidiary of Prosus NV we are committed to following their statement on human rights and to continuously work with all our stakeholders to build a company based on these fundamental principles."[100]

[98] https://www.prosusreport2021.com/images/uploads/2021/06/Prosus2021_Annual_report.pdf
[99] https://www.olxgroup.com/privacyP-statement
[100] https://www.olxgroup.com/impact

In practice, however, OLZ Kazakhstan and OLX Uzbekistan are not in full compliance with their parent organization's statement on human rights; nor do they adhere fully to the code of business ethics and conduct. OLX Uzbekistan mentions human rights and freedoms only in the list of prohibited goods and services — specifically those that discredit the honor and dignity or business reputation of others, or which allow their privacy to be violated. These include personal data or email lists; items or photographs containing material that incites hatred, in particular based on national, ethnic, racial, religious or non-religious differences; profanity and offensive statements, including those of a racist and/or religious nature; a description and/or comments regarding any types of fraud and/or extortion; provision of services capable of compromising personal data. OLX Kazakhstan does not mention human rights or freedom of expression on its site or in its policies.

Corporate governance for OLX subsidiaries in Kazakhstan and Uzbekistan should be as transparent as they are for its European parent company, but this is not the case. There is no information on the local board of directors and staff on the websites either OLX Uzbekistan or OLX Kazakhstan, although information about the staff and board can be found on LinkedIn or other internet resources. OLX Kazakhstan only mentions the names and title of OLX Group's board of directors. Neither subsidiary provides information about the role of the board or about its code of ethics and conduct. There is no link to the parent organization's policies on the roles and profile of the board of directors, nor of the management. Neither company discloses any information about the executive committee level or any of the staff member in any corporate documents on its website.[101] It is not clear that there is a compliance mechanism to ensure that the parent organization's policy of adhering to the code of Business ethics and conduct is followed, nor is there a Speak Up program for monitoring subsidiaries' compliance.

Neither Lalafo Kyrgyzstan nor Somon.tj Tajikistan discloses any information about their board and staff; nor do they show that they share their parent company's commitment to human rights or freedom of expression. Nevertheless, Somon.tj does have a privacy policy for personal data. The company notes in its privacy policy that it complies with the law in Tajikistan and the Council of Europe's Convention for the Protection of Individuals.

Olx Kazakhstan's privacy policy also emphasizes its commitment to guarding user privacy. The company notes in its confidentiality policy notes that it processes data in compliance with the law in Kazakhstan and that it is committed to the Convention for the Protection of Individuals.

[101] https://help.olx.kz/hc/ru/articles/360044886793-%D0%9F%D1%80%D0%BE-OLX ,

FREEDOM OF EXPRESSION

F1. Access to policies

Somon,tj Tajikistan's user agreement appears on the homepage of the company's website, with a license agreement – rules of the site at the bottom. The document is in Russian only, in dense legal terminology that would be difficult for ordinary users to understand. The document does not appear at all in Tajik. Lalafo Kyrgyzstan's user agreement is on the main page of the site, in the upper left corner, in Russian only.

OLX Uzbekistan posts its terms of services and other documents at the bottom of the company website's homepage in both Uzbek and Russian. The documents are well-structured and the terminology easy to understand.

OLX Kyrgyzstan posts its terms of service in the site's help center, under legal information and privacy. The user agreement, however, expired on September 9, 2021; since then, the company has not posted any update. And while the expired user agreement is posted in both Kazakh and Russian, they are overly long and poorly structured.

F2. Notification of policy changes

Somon.tj Tajikistan's user agreement stipulates that it is subject to change without notice and that amendments to the agreement comes into force as soon as they are posted to the company's website, unless specified otherwise. This places the onus on the subscriber to check the website regularly for amendments to the user agreement. Somon.tj Tajikistan also retains the right to suspend services without notice to a subscriber who violates the terms of the agreement.

Lalafo Kyrgyzstan reserves the right to change the terms of the user agreement (clause 1.5), including the price and description of tariffs, and / or to cancel the contract any time, at its discretion. Changes to the user agreement come into force as soon as they are posted, unless specified otherwise.

OLX Uzbekistan's terms of service specify, in red bold font, that the company reserves the right to change its rules for organizational, legal or technical issues and to change its prices without notice. Again, updates are posted on the company website; the user can see them when they log into their account. Amendments to the rules come into effect within 15 days of their posting, unless specified otherwise.

OLX Kazakhstan's user agreement is the same as OLX Uzbekistan's. Both companies require their subscribers to log into their accounts for updates to the tariffs or changes to the rules.

F6. Data about government demands to restrict for content and accounts

Somon.tj stipulates in its user agreement (appendix 1.5) that it may provide personal data to competent authorities upon request, as required by the law in Tajikistan.

Lalafo Kyrgyzstan's user agreement informs subscribers that their user of the company's services is governed by Kyrgyzstan's laws. The company retains the right to restrict or terminate the subscriber's access to services if they violate the law or for other reasons, at its discretion.

We did not find any disclosure document on the website of OLX Kyrgyzstan or OLX Uzbekistan.

F11. Identity policy

All the companies except Somon.tj Tajikistan require subscribers to submit a government ID or passport at some point.

OLX Kazakhstan does not require new subscribers to present government ID to register, but in its user agreement the company specifies that it might require supporting documents to confirm the accuracy of a user's personal details. Failure to provide the documents can be equated with providing false information. If the information in the supporting documents does not correspond with what the user provided at registration or cannot be used to confirm the user's identity, OLX Kazakhstan can block the user's access to the site without prior notice.

OLX Uzbekistan specifies in section four of its terms of service that to register for an account a subscriber must fill in and submit a webform on the site and submit it with an email address or phone number, a unique password or authentication through an external service — e.g., Facebook, Google, or Apple. Only in section 12 does OLX add that it reserves the right to request additional information form the user to verify their identity. To create a new user account, OLX requires a valid email address, password, and passport details. User accounts include geographic location, first and last name, phone number, and a headshot.

Lalafo Kyrgyzstan's user agreement specifies in section 1.12 that registration is voluntary, but users who choose to register receive access to additional services. The company reserves the right at any time to require the user to submit additional documentation to confirm the details they submitted at registration.

Somon.tj does not require new users to submit ID to register for an account. Its user agreement (appendix 1) stipulates that the company may require a valid email address and password. User's accounts include their geographic location, first and last name, phone number and headshot.

PRIVACY

P1. Access to privacy policies

Somon.tj's privacy policy is posted at the bottom of the homepage under "rules of the site," but is available in Russian only; there is no Tajik version. Lalafo Kyrgyzstan's privacy policy is posted at the top of the homepage, under the menu. The user agreement and privacy policy are one document and are available in Russian only; there is no Kyrgyz version. OLX Uzbekistan's privacy policy is posted at the bottom of the homepage in both Russian and Uzbek. OLX Kazakhstan's confidentiality/privacy policy is posted at the bottom of the homepage and can also be found in the help center. Available in both Kazakh and Russian, it is 19 pages long.

P2. Notification of changes

All the companies post updates to their user agreement on their website, with changes coming into force as soon as they are published. Somon.tj, a classified advertisements site similar to Craigslist, confirms in its user agreement that occasional changes to its policy privacy come into effect as soon as they are posted on the company's website; the current version is always at the same place.

Lalafo Kyrgyzstan has a similar privacy policy. In clause 3.2, the company admonishes subscribers that they have no choice but to accept whatever terms the company sets. If a user objects to changes to the policy privacy, their only option is to stop being a Lalafo customer. The company last posted changes to the policy on November 23, 2021.

OLX Kazakhstan, too, informs subscribers that the company's privacy policy is subject to changes that come into effect as soon as they are posted to the website. Subscribers who object to changes are invited to stop being subscribers. By choosing to remain a subscriber, the customer is de facto consenting to the changes.

OLX Uzbekistan follows the same policy about changes to their privacy policy but is less transparent as to how it notifies subscribers about changes. In section eight of the document the company stipulates that changes are posted without prior notice and that they come into effect immediately;

but while they specify that the updates are posted to a specific place on the website, they aren't clear about how they inform customers that changes have been made.

P3(b). Inference of user information (per RDR)

The companies / service providers surveyed for this paper use similar methodology to collect user data. The privacy policy in Somon.tj's contract stipulates that by signing the user consents to the company processing their personal data and transferring it to third parties, including third parties located abroad. , in accordance with this Privacy Policy and with the User Somon.tj service agreement[102].

Lalafo Kyrgyzstan specifies in its privacy policy that it uses web analytics, or tracking tools, provided by third–party service providers such as Google Analytics. Lalafo explains that the purpose of these tracking tools is to detect errors as well as to improve and customize services, products, and content based on the user's interests. Tracking tools use cookies to store data, which may be transmitted to and stored on servers abroad. Users can opt out of having their data mined via cookies.

Olx Kazakhstan's privacy policy stipulates that user data is collected and processed by its parent company, Olx Group, in compliance with the laws of Katzakhstan. Analysis of user data is carried out to customize advertisements and services. [103]

Olx Uzbekistan's privacy policy stipulates that by using the website, mobile app, or related Olx services, the user consents to the company processing their personal data, including their social media data.[104]

P4. Sharing of user information

All ecommerce companies share user information with multiple entities both domestically and internationally, depending on the type of transaction. Lalafo Kyrgyzstan's privacy policy specifies that the company might transfer anonymized information to third party service providers, trusted partners, or entities authorized to customize and/or improve advertising or services. Third parties must abide by Lalafo's privacy policy, meaning it cannot use the data except to carry out the task for which it is intended, and cannot share it with others.

Somon.tj's privacy policy includes the same stipulations as Lalafo Kyrgyzstan regarding data shared with third parties — i.e., that the third parties handle user data solely for the purpose it is intended

[102] https://somon.tj/about/rules/
[103] OLX.kz privacy policy
[104] OLX.uz Privacy Policy

and cannot be shared or used in any other way. Somon,tj's contract also stipulates that the company will not rent or sell user data.

Olx Uzbekistan's privacy policy does not deviate substantially from the companies cited above. In addition to stipulating that user data is only shared with third for specific purposes and cannot be used in any other way, Olx informs the user that by signing the contract, they allow the company to collect and process their data.

Olx Kazakhstan's privacy policy reads the same as Olx Uzbekistan's, with the additional stipulation that that in its Confidentiality Policy: 5. INFORMATION EXCHANGE specifies that if the company is sold, the user data already collected will be transferred to the new owner to ensure continuity.

P6. Retention of user information

Olx Kazakhstan's privacy policy informs users that the company will keep their personal data "for as long as necessary." The stated purpose for retaining user data is to "combat fraud and abuse." OLX Kazakhstan reserves the right to delete an account that has been dormant for more than 24 months, along with all the data stored in it. The customer contract stipulates that Olx Kazakhstan reserves the right to block a user account permanently, if it has been blocked or suspended for more than six months." Olx Uzbekistan's privacy stipulates that the company reserves the right to retain user data for as long as it needs. According to its user contract, Olx Group has the right to terminate the contract if the user violates the law. But while the privacy policy refers to the company's right to block or closer user accounts, there is no indication it will also delete personal data.

Somon.tj Tajikistan specifies that it may retain user data for as long as it needs to fulfill business purposes. Lalafo Kyrgyzstan does not disclose any information about its policy regarding the retention of user information.

P10(a). Process for responding to government demands for user information

All the companies surveyed for this report comply with government demands for the information of users in their jurisdictions.
Somon,tj Tajikistan informs users via their privacy policy that by signing the contract the user consents to the company's providing their personal data to government agencies upon request.

Olx Kazakhstan's privacy policy specifies that the company reserves the right, in compliance with the law, to provide information to individuals and government agencies for the purposes of combatting fraud and abuse on the site, investigating alleged violations of the law, and to combat any other alleged violations of Olx's rules.

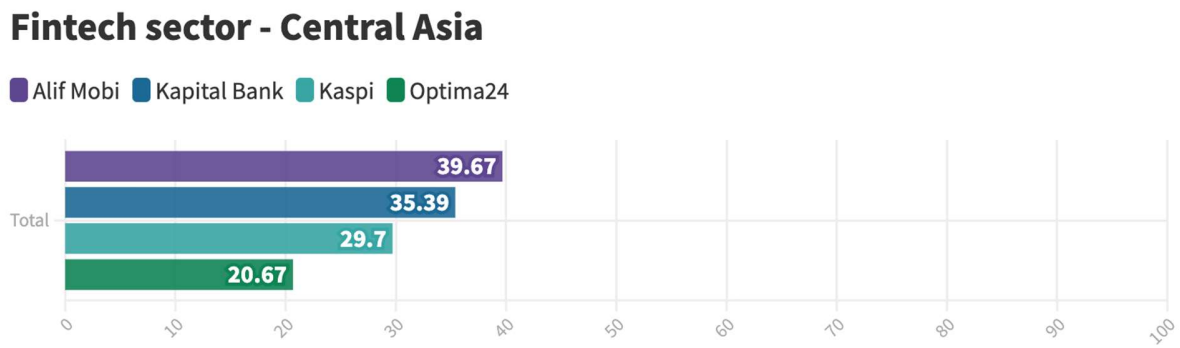
Olx Uzbekistan uses similar language to describe its policy for sharing user information with government and law enforcement authorities — i.e., that the company will share the information upon request to combat fraud and abuse of the site, to investigate violations of the law, and upon request from the authorities. Whether or not the user is informed when Olx shares their data with the authorities is a matter that the company reserves the right to decide at its own discretion.

Lalafo Kyrgyzstan does not share information about its policy for sharing information with government or law enforcement authorities.

P18. Inform and educate users about potential risks

Most of the companies surveyed for this paper take steps to educate their users about protecting themselves from cybersecurity risks. Lalafo Kyrgyzstan is the exception. Somon.tj's website has a section called safety, with information on how to avoid scammers, how to identify and avoid clicking on a fake links, etc. The company also sends this information to the user's personal account.Olx Uzbekistan's website has a section called Safety! / Xavfsizlik! with an overview of cybersecurity risks and how to avoid them, including five rules for user security. OLX Kazakhstan published a series of blog posts about cybersecurity risks, such as how to protect from phishing and fraud, how to recognize fake links, and how to make payments securely on the internet. Lalafo Kyrgyzstan provides information on safe buy and sell protocols..

VIII. Fintech Companies



TOTAL COMBINED SCORE COMPRISING OF ALL INDICATORS OF THE FINTECH SECTOR

Fintech companies are a relatively new phenomenon in Central Asia, with the Covid–19 pandemic acting as a catalyst for the sector's rapid development and expansion. Banks and other financial institutions reacted almost immediately to provide online and mobile financial and banking services. Mobile and online are increasingly a part of even in the most remote areas of Central Asia.

For this paper we examined four Fintech companies: Kaspi in Kazakhstan; Alif mobi Tajikistan; Optima Bank in Kyrgyzstan; and Kapital Bank in Uzbekistan.

This is only the second time RDR's methodology has been used to assess Fintech services.

GOVERNANCE

G1. Policy Commitment

None of the Fintech companies surveyed for this paper have any documented policy that articulates a commitment to human rights nor freedom of expression.

G2. Governance and management oversight

Some of the banks publish no information about their board of director, management staff, or oversight policy. Alif Bank is an exception in that it has a supervisory board but it does not publish any information about its composition or its role. Nor does it share information about its executives, management, or other staff. There is no information on whether the company has in place any formal oversight over practices and policies that affect freedom of expression and information.
Alif Bank has policies and regulations on the protection of personal and confidential data of clients, but it does not disclose whether the board of directors exercises formal supervision. Alif's website has a section called regulations on the protection of personal data in which it refers not to Alif Bank but only to "the Bank." For example: "the Bank established a procedure for processing and protecting personal data that ensure compliance with GDPR law." The bank assures users that their personal data is secure and protected in accordance with the rights and freedoms guaranteed by the law Tajikistan. None of the other banks examined for this paper disclose information on the board of directors, bank management, or a commitment to privacy.

Optima Bank shares information about the bank's management and its board, but there is nothing about oversight or a policy on human rights and freedom of expression in their privacy policy.

FREEDOM OF EXPRESSION

F1. Access to policies

F1(a). Access to terms of service

All the Fintech companies surveyed for this paper provide relatively easy access to the policies, legal documents, and terms of use. Alif Bank's policies are at the bottom of the homepage, but while all

the documents on the site are available in Russian and some in Tajik, the application for public offer is in Russian only.

Kapital Bank puts its relevant policies at the top of the homepage. The public offer document is located there too, in Russian and Uzbek.

Kaspi Bank puts its terms of use at the bottom of the homepage in Kazakh and Russian.

Optima Bank's policies are difficult to locate and require the user to navigate to a login page, where they choose "offer" at the top of the page to access a .pdf document that provides public offers in English, Kyrgyz, and Russian.

Notification of policy changes

All the banks we surveyed inform their clients/users about policy changes mainly via their websites, with some variations.

Alif Bank, in its terms and conditions for banking services," informs clients that it sends notifications one month in advance via e-mail or SMS, in addition to posting the information on the bank's website. The bank sends holders of public offers notification of amendments to the agreements by publishing them on the bank's website.

Kapital Bank notifies holders of public offers of changes five days prior to their implementation, via notification in electronic form to the client's personal account. Notification of changes to the rules and tariffs are sent out at least 10 days before implementation. New legislation in Uzbekistan requires that clients be notified one day in advance of changes to the bank's legal or postal address.

When Optima Bank changes the terms of the contract it sends the client a new version of the terms via a webpage called Optima24. The client then logs into Optima24 and gives their consent to the new terms. If the client does not wish to accept the new terms, they must appear in person at the bank within seven days to submit a written refusal along with legal documents that confirm their identity.

A clause in Kaspi Bank's agreement informs clients that the bank will notify them of changes by posting them to the site within three days of their implementation.

F3. Process for policy enforcement

All the banks surveyed for this paper restricts the user's account or content. The differences are in the circumstances that trigger restrictions.

Alif Bank reserves the right to refuse, unilaterally and without explanation, to execute payments made via its mobile wallet using bank cards, according to the clause on provision of services in its

public offer. In such a case the bank will notify the client of its refusal and terminate the account within 15 days. The bank also reserves the right, per the terms of comprehensive banking services of the agreement, to block the user's e-wallet at the request of authorized state bodies, on the bank's own initiative, or at the request of the client. Alif Bank uses the Bank of Tajikistan's Korti Milli payment system and the Alif mobi e-wallet for bank payment cards used to effect online payments or transfers of funds. Both systems refuse transactions if they are suspected of links to money laundering, financing of terrorism, etc.

Kapital Bank's rules for comprehensive banking services specifies that it can unilaterally suspend the client's operations (with an exception for crediting funds received from an individual) or freeze the client's account or card in cases where the bank suspects the client is engaging in money laundering, using proceeds from criminal activity, financing terrorism or arms dealing. Kapital Bank will also block access to remote banking pending presentation of client identification the following day.

Kaspi Bank's privacy policy prohibits the user from posting their profile photo or other identifying information, and from disclosing information about third parties unless they have provided written consent. Threats, violent propaganda, cruelty, insults, racism, and other types of discrimination are all forbidden, as are spam, swearing, erotica, and pornographic services, goods, and images.

Optima Bank lists various circumstances that will trigger the bank's refusal to execute / honor a transaction. They are: insufficient funds; incomplete information about the transaction; a transaction that conflicts with the laws of Kyrgyzstan; failure to pay for access to Optima24. Optima Bank blocks access to the Optima24 system after five unsuccessful attempts to login with an incorrect password. The bank will also impose restrictions on or seize a client's account upon request from state authorities, in compliance with the laws of Kyrgyzstan.

F4. Data about policy enforcement

None of the banks surveyed for this paper discloses data on policy enforcement.

F5. Process for responding to government demands

All the banks surveyed comply with government demands, although neither Kapital nor Optima is transparent about this.

Alif specifies in its terms and conditions that the bank will block e-wallets immediately upon request from authorized state authorities, in compliance with the law in Tajikistan.

Kaspi Bank specifies in its compliance policy that its data processing policy, when dealing with debt collection, legal claims, fraud prevention, and maintaining data security, complies with its "obligations to government authorities. Kaspi's service agreement stipulates that the bank has the right to refuse to process transactions provided for in the agreement in the event of reasons beyond the bank's control, such as a request from state bodies in Kazakhstan.

F6. Data about government demands to restrict for content and accounts

None of the banks provide data regarding government demands to restrict content and accounts.

F11. Identity policy

All the banks require clients to show ID to register for an account and for transactions.

Alif's terms of service require the client to confirm their identity. The transfer rules of alif mobi include a single clause noting that a client is obligated to provide the bank with specific documentation to confirm their identity. The documentation must either be presented in person at one of the bank's branches, or by presenting ID and filling out a form at an office of the bank's agent, or by submitting a signed form and copy of an identity document that have both been notarized.

Kapital Bank's rules for comprehensive banking services for individuals include a clause that stipulates the bank requires documentation to confirm the identity of the client, the client's representative, and the beneficiary, as well as documents that explain the reason for and purpose of client transactions. The bank reserves the right to refuse transactions under circumstances described by the laws of Uzbekistan.

Optima Bank's terms of service indicate that an application to open an account must be accompanied by an initial deposit, which can come from a third party. The application must be presented with identity documents for the client and for the depositor if they are a third party. Minors younger than 16 who wish to open an account must present a birth certificate, proof of address, confirmation of their school's identity, and a photograph. Upon reaching the age of 16, they must also present a passport. The bank confirms the client's identity before carrying out any transactions on their behalf.

Kaspi Bank's terms of agreement includes a section titled "obligations of the parties" that indicates the bank has the right to request identity and other documents to implement foreign exchange controls, in compliance with Kazakhstan's legislation and the bank's internal regulatory controls.

PRIVACY

P1. Access to privacy policies

All the banks post their privacy policies in different forms. Most are easy to locate.

Alif Bank's regulations for the protection of customers' personal and confidential data is at the bottom of the homepage, in Russian only.

Kapital Bank's privacy policy is difficult to locate. Rather than appearing as a stand–document, it appears in the form of limited information under "other conditions" in clause 7.2 of the public offer, where the bank stipulates that by signing the agreement the client consents to the bank's providing third parties with their personal data in compliance with its obligations under the remote banking service (RBS) and contract of complex banking services (RCB). The public offer is available in

Russian and in Uzbek. Only in its mobile app does Kapital Bank offer its privacy policy in a stand–alone document, but the information is the same as that on the bank's website.

Optima Bank's privacy policy appears at the bottom of the homepage in Kyrgyz, Russian, and English.

Kaspi Bank's privacy policy appears at the end of the user agreement, which is on the homepage, in Russian and Kazakh.

P2. Notification of changes

P2(a). Changes to privacy policies

While the banks surveyed for this paper use varying secondary means to notify their clients/users about changes to the privacy policy, the primary means for all of them is updates posted on the website. The onus is thus on the clients/users to stay apprised of changes by visiting the website regularly.

Alif Bank informs alif mobi clients that regulations for handling their user data are subject to change, and that changes come into effect as soon as they are posted.

The privacy policy on Optima Bank's website includes a section titled "changes to the privacy policy," in which users are informed that the bank may change the policy at any time, with changes coming into effect immediately, unless specified otherwise. Optima advises its clients to check the privacy policy regularly to stay informed of changes.

Neither Kapital Bank nor Kaspi Bank shares information about their procedure for notifying users of changes to their privacy policies.

P3(b). Inference of user information

The banks we analyzed follow very similar practices for inference of user information and collecting data information. The difference is in the details —i.e., some are transparent about the details of their policy while other reveal only a few details.

Alif Bank includes specifications about inference of data in several of its regulations and related documents. It defines personal data as "any information relating directly or indirectly to a specific or identifiable person (personal data subject), processed by the bank for predetermined goals." By signing the agreement, clients are giving their consent to the processing of the following personal data:

- Surname, first name, and patronymic.
- Passport and other identity documents.
- Date and place of birth.
- Home address.

- Telephone number and e-mail address.
- Photo/video image.
- Family and property status.
- Education, profession, employment status
- Information about expenses and income.
- Gender.
- Social media accounts.

Alif Bank does not process personal data about race, nationality, political views, religious or philosophical beliefs, intimate life, or criminal record of individuals, unless the law requires it.

Kapital Bank's rules for individual banking services stipulates that by signing the agreement the client consents to the bank processing their personal data. This extends to transferring client data to third parties (after the data has been anonymized), including insurers and creditors.

Optima Bank's privacy policy defines user data as personal data provided by the user/client when they register for an account with the bank and when they use the bank's services — including Optima24's mobile app. The data includes, but is not limited to, the user's IP address and information about the mobile device they use for transactions. To open an account, a client must provide the bank with their full name, gender, date of birth, home address, email address, and phone number. The bank may request additional information. Optima collects data about the user's mobile device — e.g., the model, operating system, unique identifiers, transactions carried out, and location information. When users make payments for goods and services or transfer funds, the bank collects data on the time and number of transactions, the payment method, data on the recipient and / or service provider, and a description of the reason for the transaction.

Kaspi Bank's privacy policy has a section titled "information provided by you," which details inference of user data — i.e., taxi ID number, full name, mobile phone number, date of birth, email address, home address, salary, and other income. In its privacy policy the bank informs customers that it processes their data to provide various services securely — e.g., confirming the user's identity before executing remote contracts and financial transactions; the bank also uses the data to customize its notifications and special offers about its products; and it uses the data to process user requests, including requests that involve services provided by third parties.

P4. Sharing of user information

All the banks share user information with third parties.

Alif Bank indicates in its regulations for processing personal data that the bank has the right to share data with third parties, including data harvested from social media accounts, unless the laws of Tajikistan specify otherwise. Third parties can be in other countries, which means the bank can transfer user data across borders. Alif Bank does not identify the third parties.

Kapital Bank does not specify data types of user information it collects. It informs users via the public offer that by signing the agreement they consent to the bank providing their data to third parties, in compliance with the laws of Uzbekistan. Third parties can be insurers, policyholders,

beneficiaries, creditors, and auditors. The Client also gives consent to the bank and the bank's partners to process any special categories of their personal data and biometric personal data in case, should the need arise.

Optima Bank specifies in its privacy policy that it shares user data with third parties, in compliance with the laws of Kyrgyzstan. The bank has the right to share user data for its own purposes. The user consents to the bank sharing their data by signing the agreement. In cases where the user wishes to execute a transaction with a person or entity not associated with Optima Bank, the bank will request additional user consent.

Kaspi Bank, according to its privacy policy, does not share or transfer user data to third parties, including via transactions executed on the mobile app, except in the following cases: The client (or the client's parent or guardian) have expressly consented; the transfer is necessary for the performance of a contract with the client's parent or guardian providing the services for the user; the relevant laws allow the transfer.

P6. Retention of user information

The banks analyzed for this paper take very similar positions on data retention. But because there is no transparent monitoring mechanism, we were unable to determine whether they do in fact delete user data.

Alif Bank posts its rules for processing personal data, but the information is contradictory. In clause 5.14.6 of the regulations the bank promises to stop processing personal user data once the purpose for which it was initially retained has been achieved, and to destroy it within 30 days, unless the laws of Tajikistan specify otherwise. In clause 5.14.4, however, the bank writes that it destroys data after processing only at the request of the user, who must specify the personal data being processed. The bank says it will block or delete personal data if it is incomplete, outdated, inaccurate, illegally obtained, or not necessary for the stated purpose and is required to notify the user once their data has been destroyed. The regulations further stipulate that the client's consent to the processing of their personal data is valid for five years from the date of the termination of the contract. Once the five years have elapsed, the validity of the consent is renewed for another five years — unless the client withdraws it. To withdraw consent for the processing of their data, the client must submit a written application to the bank. Even then, the bank has a year to destroy the data.

Kapital Bank does not disclose information about every type of user information it collects. But in chapter three, clause 3.18 of its rules for comprehensive banking services for individuals it says that the bank records all client transactions in its information system, in the form of electronic documents and electronic messages. The bank stores these electronic documents and messages for the period specified by the law in Uzbekistan.

Kaspi Bank stores user data for the time deemed necessary to achieve the purpose for which it was collected and to comply with legal requirements in Kazakhstan. In its privacy policy the bank notifies clients that they use the mobile app to initiate the process of deleting their account, after which there is a 14-day waiting period.

During this period, the client can request account recovery. Once the 14 days have elapsed, the entry will be permanently deleted.

Optima Bank does not disclose any information about its policies for user data retention.

P8. Users' access to their own user information

Neither Optima Bank nor Kaspi Bank explain their policies regarding user access to their own data.

Alif Bank deals with user access to their own information in its regulations for the protection of personal and confidential clients. The user can submit a request to the bank to request specific information. But the bank can refuse to provide the information because the laws of Tajikistan can limit user access to their own data.

Kapital Bank indicates in its rules for comprehensive banking services for individuals that upon receiving a request from the client, the bank will provide them with statements that detail the movement of funds in their account and/or other information that is detailed in the user agreement, incompliance with the law of Uzbekistan.

P9. Collection of user information from third parties

All the banks collect data information from third parties, but not all the banks are transparent about their policies.

Alif Bank's terms of comprehensive banking services for individuals specifies that the bank will collect and process any personal data the client posts on social media networks. The purpose of retaining the data, according to Alif, is to customize personal offers. If the user withdraws consent for the processing of their personal data, the bank says it will comply and destroy the data it has already collected within 30 days, unless the data falls into the category of information the bank may retain per the user agreement. The bank is required to notify the user when their personal data has been destroyed.

Kapital Bank specifies in its rules for comprehensive banking services that the bank stores user data to execute agreements, check credit history, and share information with credit bureaus. The client consents by signing the user agreement. All of this is in accordance with the law in Azerbaijan as it pertains to the exchange of credit information.

Kaspi Bank indicates in its privacy policy that it "receives information provided by third parties, which may contain data about the user" and of third parties with whom the user interacts. When the client uses Kaspi's mobile application to execute a transfer of funds, for example, the bank might collect data from the recipient. This data includes ID number, full name, mobile phone number, date and/or year of birth, e-mail address, and home address.

Optima Bank does not disclose any information about its policies regarding third–party data.

P10(a). Process for responding to government demands for user information

All the banks comply with government demands for user information, but not all inform their clients that their data could be turned over to state authorities.

Alif Bank's privacy policy refers to the procedural law of Tajikistan and the current legislation of Tajikistan. Specifically: the bank transfers personal data to state bodies in accordance with the laws of Tajikistan.

Kapital Bank's public offer specifies that the bank will transfer the personal data of a client who seeks any type of credit — e.g., overdraft protection, microloan, consumer loan — to the state register of credit information at the Central Bank of Uzbekistan, to the credit information analytical center and other organizations (financial institutions, bank departments). The bank does not share the names of third parties.

Kaspi Bank's privacy policy mentions that the bank is required by law to respond to government demands.

Optima Bank does not disclose any information about sharing user data with state authorities.

P18. Inform and educate users about potential risks

All the banks we surveyed use different methods to inform their clients about potential risks. Alif Bank includes a "reminder about information security when working with loan management services (LMS)" in its terms of comprehensive banking services for individuals. The bank also posts instructive videos on social media platforms. Kapital Bank does not have a permanent section about consumer fraud on its website, but the bank does post information to its news feed. Optima Bank posts information and instructions about scammers to its website. Kaspi Bank implements security protocols for its clients.

IX. Recommendations

The purpose of these recommendations is to enhance user trust in digital services, thereby increasing potential financial investment.

CIPI conducted a study of the policies and practices of 16 companies of four Central Asian countries —Kazakhstan, Kyrgyzstan, Tajikistan, and Uzbekistan. It examined the services currently available, the website governance policies, legal documents, and annual reports relating public data on interactions with government agencies. CIPI applied RDR methodology to gauge these companies' respect for freedom of information and privacy.

Although the national contexts and legal environment of the selected countries can affect company performance—i.e., certain laws, regulations, or political factors can either enhance or limit a company's ability to perform well on certain indicators, RDR methodology does not compensate for these factors, since its index provides for objective evaluation of what companies do or don't do, regardless of the reason. In circumstances where laws and regulations undermine company performance, we encourage those companies to advocate for laws that allow them to fully respect their users' rights to freedom of expression and privacy by disclosing strong commitments, policies, and practices.

The purpose of providing a rating is to understand the current situation and work out a roadmap toward improvement. These changes can secure online businesses, increase user loyalty to web services and attract potential investors. The recommendations are meant to help the companies improve their reputations, thereby increasing customer loyalty and trust in web services. To improve transparency and raise the standards of compliance with users' digital rights, digital rating experts have, based on the data collected for this paper, prepared the following recommendations. Companies can refer to these recommendations to see where they are complying and where they can improve.

- Publish an explicit commitment to human rights, in particular the right to privacy and to freedom of expression and information. We expect companies to be more vocal about how they intend to respect users' rights, both through their policies in legal documents and on their websites, as well as in public statements from company representatives.
- Be transparent about the composition of the board of directors and the staff, particularly at the executive and management levels. Identify their roles in overseeing how the company's operations affect human rights.
- Publish an annual transparency report that discloses the number of government requests for user data received, the number of requests the company complied with, the number of requests to remove content or accounts. In the case of parent and subsidiary companies,

adopt the parent company's best practices to strengthen policies at the local level where the subsidiaries operate. Have a compliance policy (code of corporate ethics, anti–corruption policy, policy for reporting violations of ethical standards).

- Establish a hotline that users can for help with the process of submitting complaints about the companies' services. These may include, but are not limited to, enforcement of the company's policies, ethics, legal compliance, and anti–corruption measures.
- Disclose the procedure for considering requests from state authorities and individuals that affect users.
- Develop and publish accessible easy–to–comprehended user agreements.
- Publish the privacy policy and user agreement in a section of the company website that is easy to find. For example, have a dedicated webpage for all the policies pertaining to each service the company offers.
- Improve the privacy policy and the user agreement/terms of service, making them easier to understand, providing concise explanations in accessible language without using overly technical terminology, including clear examples of how the clauses affect users.
- Allow users to control how their data is used in targeted advertising by giving them the choice to opt out of tracking.
- Maintain an archive of all the previous versions of the privacy policy and user agreement, so that users can track changes.
- Disclose detailed information on the type and method of user data the company collects and how long they store it, as well as the procedure for destroying user data. Make it easy for users to request and receive a copy of their personal data and notify users immediately if there is a data leak.
- Publish practical materials that educate users on how to protect themselves from cybersecurity risks associated with the company's products or services.
- Disclose how the telecom companies and those providing internet–based services are carrying out legal due diligence of the requests to restrict access to information (groups, accounts, posts, comments, publications) from individuals and government agencies before their execution.
- In cases where a user attempts to access information that was blocked based on a legitimate request, either from an individual or a state body, the company should provide an explanation to the user about the reasons underlying the decision to block the information — for example, if the content is defined by local laws as "illegal information." The company should also inform the user of who submitted the request and on what date, and on what date the decision to block the content went into effect.

X. Annexes

1. Annex #1. Table of Selected RDR Methodology Indicators and Elements

Selected RDR Indicators and Elements
G: Governance:
G1. Policy Commitment **Elements:** 1. Does the company make an explicit, clearly articulated policy commitment to human rights, including to freedom of expression and information? 2. Does the company make an explicit, clearly articulated policy commitment to human rights, including to privacy? 3. Does the company disclose an explicit, clearly articulated policy commitment to human rights in its development and use of algorithmic systems?
G2. Governance and management oversight **Elements:** 1. Does the company clearly disclose that the board of directors exercises formal oversight over how company practices affect freedom of expression and information? 2. Does the company clearly disclose that the board of directors exercises formal oversight over how company practices affect privacy? 3. Does the company clearly disclose that an executive-level committee, team, program or officer oversees how company practices affect freedom of expression and information? 4. Does the company clearly disclose that an executive-level committee, team, program or officer oversees how company practices affect privacy? 5. Does the company clearly disclose that a management-level committee, team, program or officer oversees how company practices affect freedom of expression and information? 6. Does the company clearly disclose that a management-level committee, team, program or officer oversees how company practices affect privacy?
F: Freedom of Expression
F1. Access to policies F1(a). Access to terms of service **Elements:** 1. Are the company's terms of service easy to find? 2. Are the terms of service available in the primary language(s) spoken by users in the company's home jurisdiction? 3. Are the terms of service presented in an understandable manner
F1(b). Access to advertising content policies **Elements:** 1. Are the company's advertising content policies easy to find? 2. Are the company's advertising content policies available in the primary language(s) spoken by users in the company's home jurisdiction? 3. Are the company's advertising content policies presented in an understandable manner?

4. **(For mobile ecosystems): Does the company clearly disclose that it requires apps made available through its app store to provide users with an advertising content policy?**
5. **(For personal digital assistant ecosystems): Does the company clearly disclose that it requires skills made available through its skill store to provide users with an advertising content policy?**

F2. Notification of policy changes

F2(a). Changes to terms of service

Elements:

1. **Does the company clearly disclose that it directly notifies users about all changes to its terms of service?**
2. **Does the company clearly disclose how it will directly notify users of changes?**
3. **Does the company clearly disclose the timeframe within which it directly notifies users of changes prior to these changes coming into effect?**
4. **Does the company maintain a public archive or change log?**

F3. Process for policy enforcement

F3(a). Process for terms of service enforcement

Elements:

1. **Does the company clearly disclose what types of content or activities it does not permit?**
2. **Does the company clearly disclose why it may restrict a user's account?**
3. **Does the company clearly disclose information about the processes it uses to identify content or accounts that violate the company's rules?**
4. **Does the company clearly disclose how it uses algorithmic systems to flag content that might violate the company's rules?**
5. **Does the company clearly disclose whether any government authorities receive priority consideration when flagging content to be restricted for violating the company's rules?**
6. **Does the company clearly disclose whether any private entities receive priority consideration when flagging content to be restricted for violating the company's rules?**
7. **Does the company clearly disclose its process for enforcing its rules once violations are detected**

F4. Data about policy enforcement

F4(a). Data about content restrictions to enforce terms of service

Elements:

1. **Does the company publish data about the total number of pieces of content restricted for violating the company's rules?**
2. **Does the company publish data on the number of pieces of content restricted based on which rule was violated?**
3. **Does the company publish data on the number of pieces of content it restricted based on the format of content? (e.g. text, image, video, live video)?**
4. **Does the company publish data on the number of pieces of content it restricted based on the method used to identify the violation?**
5. **Does the company publish this data at least four times a year?**
6. **Can the data be exported as a structured data file?**

F4(b). Data about account restrictions to enforce terms of service

Elements:

1. **Does the company publish data on the total number of accounts restricted for violating the company's own rules?**
2. **Does the company publish data on the number of accounts restricted based on which rule was violated?**
3. **Does the company publish data on the number of accounts restricted based on the method used to identify the violation?**
4. **Does the company publish this data at least four times a year?**
5. **Can the data be exported as a structured data file?**

F4(b). Data about account restrictions to enforce terms of service

Elements:

1. **Does the company clearly disclose its process for responding to non-judicial government demands?**
2. **Does the company clearly disclose its process for responding to court orders?**
3. **Does the company clearly disclose its process for responding to government demands from foreign jurisdictions?**
4. **Do the company's explanations clearly disclose the legal basis under which it may comply with government demands?**
5. **Does the company clearly disclose that it carries out due diligence on government demands before deciding how to respond?**
6. **Does the company commit to push back on inappropriate or overbroad demands made by governments?**
7. **Does the company provide clear guidance or examples of implementation of its process of responding to government demands?**

F6. Data about government demands to restrict for content and accounts

Elements:

1. **Does the company break out the number of government demands it receives by country?**
2. **Does the company list the number of accounts affected?**
3. **Does the company list the number of pieces of content or URLs affected?**
4. **Does the company list the types of subject matter associated with the government demands it receives?**
5. **Does the company list the number of government demands that come from different legal authorities?**
6. **Does the company list the number of government demands it knowingly receives from government officials to restrict content or accounts through unofficial processes?**
7. **Does the company list the number of government demands with which it complied?**
8. **Does the company publish the original government demands or disclose that it provides copies to a public third-party archive?**
9. **Does the company report this data at least once a year?**

F10. Network shutdown (telecommunications companies)

Elements:

1. **Does the company clearly disclose the reason(s) why it may shut down service to a particular area or group of users?**

2. Does the company clearly disclose why it may restrict access to specific applications or protocols (e.g., VoIP, messaging) in a particular area or to a specific group of users?
3. Does the company clearly disclose its process for responding to government demands to shut down a network or restrict access to a service?
4. Does the company clearly disclose a commitment to push back on government demands to shut down a network or restrict access to a service?
5. Does the company clearly disclose that it notifies users directly when it shuts down a network or restricts access to a service?
6. Does the company clearly disclose the number of network shutdown demands it receives?
7. Does the company clearly disclose the specific legal authority that makes the demands?
8. Does the company clearly disclose the number of government demands with which it complied?

F11. Identity policy

Elements:

1. Does the company require users to verify their identity with their government-issued identification, or with other forms of identification that could be connected to their offline identity?

P: Privacy

P1. Access to privacy policies

P1(a). Access to privacy policies

Elements:

1. Are the company's privacy policies easy to find?
2. Are the privacy policies available in the primary language(s) spoken by users in the company's home jurisdiction?
3. Are the policies presented in an understandable manner?
4. (For mobile ecosystems): Does the company disclose that it requires apps made available through its app store to provide users with a privacy policy?
5. (For personal digital assistant ecosystems): Does the company disclose that it requires skills made available through its skill store to provide users with a privacy policy?

P2. Notification of changes

P2(a). Changes to privacy policies

Elements:

1. Does the company clearly disclose that it directly notifies users about all changes to its privacy policies?
2. Does the company clearly disclose how it will directly notify users of changes?
3. Does the company clearly disclose the timeframe within which it directly notifies users of changes prior to these changes coming into effect?
4. Does the company maintain a public archive or change log?
5. (For mobile ecosystems): Does the company clearly disclose that it requires apps sold through its app store to notify users when the app changes its privacy policy?
6. (For personal digital assistant ecosystems): Does the company clearly disclose that it requires skills sold through its skill store to notify users when the skill changes its privacy policy?

P3(b). Inference of user information

Elements:

1. **Does the company clearly disclose all the types of user information it infers on the basis of collected user information?**
2. **For each type of user information the company infers, does the company clearly disclose how it infers that user information?**
3. **Does the company clearly disclose that it limits inference of user information to what is directly relevant and necessary to accomplish the purpose of its service?**

P4. Sharing of user information

Elements:

1. **For each type of user information the company collects, does the company clearly disclose whether it shares that user information?**
2. **For each type of user information the company shares, does the company clearly disclose the types of third parties with which it shares that user information?**
3. **Does the company clearly disclose that it may share user information with government(s) or legal authorities?**
4. **For each type of user information the company shares, does the company clearly disclose the names of all third parties with which it shares user information?**
5. **(For mobile ecosystems): Does the company clearly disclose that it evaluates whether the privacy policies of third party apps made available through its app store disclose what user information the apps share?**
6. **(For mobile ecosystems): Does the company clearly disclose that it evaluates whether the privacy policies of third party apps made available through its app store disclose the types of third parties with whom they share user information?**
7. **For personal digital assistant ecosystems): Does the company clearly disclose that it evaluates whether the privacy policies of third party skills made available through its skill store disclose what user information the skills share?**
8. **(For personal digital assistant ecosystems): Does the company clearly disclose that it evaluates whether the privacy policies of third party skills made available through its skill store disclose the types of third parties with whom they shareuser information?**

P5. Purpose for collecting, inferring, and sharing user information

Elements:

1. **For each type of user information the company collects, does the company clearly disclose its purpose for collection?**
2. **For each type of user information the company infers, does the company clearly disclose its purpose for the inference?**
3. **Does the company clearly disclose whether it combines user information from various company services and if so, why?**
4. **For each type of user information the company shares, does the company clearly disclose its purpose for sharing?**
5. **Does the company clearly disclose that it limits its use of user information to the purpose for which it was collected or inferred?**

P6. Retention of user information

Elements:

1. **For each type of user information the company collects, does the company clearly disclose how long it retains that user information?**
2. **Does the company clearly disclose what de-identified user information it retains?**
3. **Does the company clearly disclose the process for de-identifying user information?**
4. **Does the company clearly disclose that it deletes all user information after users terminate their account?**
5. **Does the company clearly disclose the time frame in which it will delete user information after users terminate their account?**
6. **(For mobile ecosystems): Does the company clearly disclose that it evaluates whether the privacy policies of third-partyapps made available through its app store disclose how long they retain user information?**
7. **(For mobile ecosystems): Does the company clearly disclose that it evaluates whether the privacy policies of third-party apps made available through its app store state that all user information is deleted when users terminate their accounts or delete the app?**
8. **(For personal digital assistant ecosystems): Does the company clearly disclose that it evaluates whether the privacy policies of third-party skills made available through its skill store disclose how long they retain user information?**
9. **(For personal digital assistant ecosystems): Does the company clearly disclose that it evaluates whether the privacy policies of third-party skills made available through its skill store state that all user information is deleted when users terminate their accounts or delete the skill?**

P8. Users' access to their own user information

Elements:

1. **Does the company clearly disclose that users can obtain a copy of their user information?**
2. **Does the company clearly disclose what user information users can obtain?**
3. **Does the company clearly disclose that users can obtain their user information in a structured data format?**
4. **Does the company clearly disclose that users can obtain all public-facing and private user information a company holds about them?**
5. **Does the company clearly disclose that users can access the list of advertising audience categories to which the company has assigned them?**
6. **Does the company clearly disclose that users can obtain all the information that a company has inferred about them?**
7. **(For mobile ecosystems): Does the company clearly disclose that it evaluates whether the privacy policies of third-party apps made available through its app store disclose that users can obtain all of the user information about them the app holds?**
8. **(For personal digital assistant ecosystems): Does the company clearly disclose that it evaluates whether the privacy policies of third-party skills made available through its skill store state that all user information is deleted when users terminate their accounts or delete the skill?**

P9. Collection of user information from third parties

Elements:

1. **(For digital platforms) Does the company clearly disclose what user information it collects from third-party websites through technical means?**

2. **(For digital platforms) Does the company clearly explain how it collects user information from third parties through technical means?**
3. **(For digital platforms) Does the company clearly disclose its purpose for collecting user information from third parties through technical means?**
4. **(For digital platforms) Does the company clearly disclose how long it retains the user information it collects from third parties through technical means?**
5. **(For digital platforms) Does the company clearly disclose that it respects user-generated signals to opt out of data collection?**
6. **Does the company clearly disclose what user information it collects from third parties through non-technical means?**
7. **Does the company clearly disclose how it collects user information from third parties through non-technical means?**
8. **Does the company clearly disclose its purpose for collecting user information from third parties through non-technical means?**
9. **Does the company clearly disclose how long it retains the user information it collects from third parties through non-technical means?**

P10(a). Process for responding to government demands for user information

Elements:

1. **Does the company clearly disclose its process for responding to non-judicial government demands?**
2. **Does the company clearly disclose its process for responding to court orders?**
3. **Does the company clearly disclose its process for responding to government demands from foreign jurisdictions?**
4. **Do the company's explanations clearly disclose the legal basis under which it may comply with government demands?**
5. **Does the company clearly disclose that it carries out due diligence on government demands before deciding how to respond?**
6. **Does the company commit to push back on inappropriate or overbroad government demands?**
7. **Does the company provide clear guidance or examples of implementation of its process for government demands?**

P11. Data about government demands for user information

Elements:

1. **Does the company list the number of government demands it receives by country?**
2. **Does the company list the number of government demands it receives for stored user information and for real-time communications access?**
3. **Does the company list the number of accounts affected?**
4. **Does the company list whether a demand sought communications content or non-content or both?**
5. **Does the company identify the specific legal authority or type of legal process through which law enforcement and national security demands are made?**
6. **Does the company include government demands that come from court orders?**
7. **Does the company list the number of government demands it complied with, broken down by category of demand?**
8. **Does the company list what types of government demands it is prohibited by law from disclosing?**
9. **Does the company report this data at least once per year?**
10. **Can the data reported by the company be exported as a structured data file?**

P18. Inform and educate users about potential risks

Elements:

1. **Does the company publish practical materials that educate users on how to protect themselves from cybersecurity risks relevant to their products or services?**

2. Annex #2. Table of Information of the selected companies for this research

Country	Telecom operators	E-commerce	Fintech
Kazakhstan	https://www.kcell.kz/ https://beeline.kz/	https://www.olx.kz/	https://kaspi.kz/
Kyrgyzstan	https://beeline.kg/ (Sky Mobile) https://o.kg/ (Nurtelecom)	https://lalafo.kg/	https://www.optimabank.kg
Tajikistan	https://megafon.tj/ https://www.tcell.tj/ (Indigo)	https://somon.tj/	https://alif.tj/
Uzbekistan	https://beeline.uz/ (Beeline Uzbekistan) https://ucell.uz/ (UCell)	https://www.olx.uz/	https://apelsin.uz/

3. Annex #3. Regulations and Policies in digital sector of Central Asia countries

Policy and Regulation Legislations	Notes	Kazakhstan	Kyrgyzstan	Tajikistan	Turkmenistan	Uzbekistan
National Development Strategy	All 5 countries have adopted their national development strategies with the commitment of digital transformation priorities. For the most part, these documents reflect development issues, one way or another through the use of ICT.	+	+	+	+	+
Digital transformation	All 5 countries entered the transition to digital transformation of all sectors of socio-economic development	State program "Digital Kazakhstan 2018-2022"	Concept of digital transformation "Digital Kyrgyzstan 2019-2023"	National Digital Economy Concept Policies in a number of industries: economics, telecommunications, financial and banking sectors, etc.	within the framework of the State Program for the Development of the Digital Economy for 2021-2025	-
Digital Economy Strategy	All 5 countries have adopted their strategies / concepts, taking into account the complete transition of the national economies to the digital economy	+	Draft Concept "Digital Economy of the Kyrgyz Republic 2021-2023"	+	+	Digital Uzbekistan

Policy and Regulation Legislations	Notes	Kazakhstan	Kyrgyzstan	Tajikistan	Turkmenistan	Uzbekistan
Cyber Security Strategy	This issue remains the most discussed and the adopted documents (both legislation and policies are not always available for wide public acquaintance. Basically, measures for its implementation are more of a tactical than a preventive nature and regulators are appointed among law enforcement or security and special services	Financial sector	+	-	+	Within the framework of Cybersecurity Centre created by the State Unitary Enterprise under the Decree of the President 27/06/2013, No. PP-1989 "On measures for the further development of the National Information and Communication System " and the Resolution of the Cabinet of Ministers dated 16/09/ 2013 No. 250 "On measures to organize the activities of the Centre for the Development of

Policy and Regulation Legislations	Notes	Kazakhstan	Kyrgyzstan	Tajikistan	Turkmenistan	Uzbekistan
						the Electronic Government System and the Centre for Information Security under the State Committee for Communications, Informatisation and Telecommunication Technologies ", as well as the Criminal Code
AI Strategy	The topic is just beginning to acquire a national perspective in all countries in different degrees; countries are beginning to develop their AI strategies and legal frameworks. However, at the policy and practice level, all 5 countries have established centres, laboratories, AI development groups, etc.	- at the level of National strategy, projects and laboratories for AI	- at the level of National strategy, projects, laboratories, IH "Zerde"	+ Draft of the AI Strategy being reviewed and at the level of National strategy, projects and AI laboratories	+ at the level of preparation for the adoption of the legislative framework)	+ Resolution of the President of February 17, 2021 "On measures to create conditions for the accelerated introduction of artificial

Policy and Regulation Legislations	Notes	Kazakhstan	Kyrgyzstan	Tajikistan	Turkmenistan	Uzbekistan
						intelligence technologies"
E-government Strategy	In 4 countries (except Turkmenistan), the legal framework was adopted quite a long time ago (in the middle of 2000). However, the issue of implementing the norms and updating these documents remains open. This is especially true for Tajikistan.	+	+	+	- in draft	+
E - documents	Although in the legislation the actions of e-documents are equated to paper ones, however not always government bodies and businesses accept the e-version of the documents, thus citizens have to use both versions of e-documents	+	+	+	+	+
Cybercrime	In all countries, appropriate amendments have been made to laws, codes (administrative, criminal) and departmental acts. In most cases, special services, the Ministry of Internal Affairs or the General Prosecutor's Office are supervisory or regulatory levers to identify this type of offense / crime.	+	+	+	+ Within the framework of the Concept for the development of the digital economy in the structure of the agency	+

Policy and Regulation Legislations	Notes	Kazakhstan	Kyrgyzstan	Tajikistan	Turkmenistan	Uzbekistan
					"Turkmen telecom" Ministry of Industry and Communications of Turkmenistan established a cyber security service	
Data Privacy	This issue in 5 countries is reflected in the laws on personal data, information protection. There is no separate regulatory/normative acts	+	+	+ Law "On personal information"	+	+

Policy and Regulation Legislations	Notes	Kazakhstan	Kyrgyzstan	Tajikistan	Turkmenistan	Uzbekistan
E-signature	Almost all countries (except for Kyrgyzstan) have adopted a law on electronic digital signature. This fact testifies to the binding to one (digital) technology, which may be the reason that the institutions of e-commerce, digital economy, e-document flow will not develop at the rates that are laid down in them. Since the use of digital technology for many citizens, the public and business sector is difficult and quite expensive.	+	+	+	+ Within the frame work of the Law "On Electronic Document, Electronic Document Manage ment and Digital Services"	+
International certificates and foreign signatures	In this matter, the norms are defined as actions through accepted agreements / contracts with foreign participants	+	+	+	+	+
Personal Privacy	There is no separate privacy law, it goes in the context of information, personal and personal data	+	+	+	+	+

Policy and Regulation Legislations	Notes	Kazakhstan	Kyrgyzstan	Tajikistan	Turkmenistan	Uzbekistan
Consumer Protection	In the context of what other specialized laws define online and offline as one and the same, this law regulates the rules in all specified countries.	+	+	+	+	+
E-commerce	Not all countries have passed the transition from "trade" to "e-commerce" in a legislative form (for example Tajikistan, Turkmenistan). However, policies and in practice, this issue is resolved faster on the ground.	+ Law "On the regulation of commercial activities", § 56, article 1 "eCommerce - entrepreneurial activity in electronic commerce, as well as the sale of services, carried out through information and com munication technologies	+ The Program for the Development of Electronic Commerce in the Kyrgyz Republic for 2021-2025 is under development.	-	-	+

Policy and Regulation Legislations	Notes	Kazakhstan	Kyrgyzstan	Tajikistan	Turkmenistan	Uzbekistan
E-Transaction	All countries have adopted and are implementing these norms, both in laws and policies.	+	+	+	+	+
Data Localization	This issue began its development in the policy and in practice, earlier than the corresponding regulatory framework was adopted. In Tajikistan, the problem still remains. The regulator (Communication Service under the Government of the Republic of Tajikistan) has not yet developed a package of normative legal acts regulating, among other things, data localization issues	+	+	+	No information available	+
IT PARKs	The issue of IT parks becomes a priority for all countries and they begin a repeated situational analysis of the current legislation of their countries, taking into account new trends and opportunities. In Tajikistan, for example, the current law "On Technology Park" from 2010. At the moment, there is a discussion on the adoption of amendments or a new draft law. Also, in the draft of the new Tax	+	+	+	+	+

Policy and Regulation Legislations	Notes	Kazakhstan	Kyrgyzstan	Tajikistan	Turkmenistan	Uzbekistan
	Code of Tajikistan, norms have been established for the provision of benefits and preferences for Technoparks.					
Telecommunications	Almost all 5 countries have adopted a model law, with similar regulations. Only Uzbekistan legally divided "communications" and "telecommunications"	+ Law "On Communications"	+ Law "On electrical and postal communications"	+ Law "On electrical communications"	+ Law "On Communications"	+ Law "On Communications" and Law "On Telecommunications"
Preferential taxation	This issue is resolved, to a greater extent in the policy than in the laws. Some countries' tax codes have established rules for granting benefits. But, in general, separate acts (government decrees, as in Tajikistan) are adopted for certain ICT activities, services or companies.	+ Within the framework of several regulatory legal acts, the Tax Code, the Budget Code, the Joint Action Plan of the Government and the National Bank on the development of the national stock market	+	-	-	+

Policy and Regulation Legislations	Notes	Kazakhstan	Kyrgyzstan	Tajikistan	Turkmenistan	Uzbekistan
		for 2018 - 2021, etc.				
E-banking	This issue is resolved in practice before laws are passed. The market dictates its conditions and market players (including regulators) make decisions at the policy level, by internal acts or agreements	+ Resolution of the Government of the Republic of Kazakhstan "On the Plan of Joint Actions of the Government of the Republic of Kazakhstan and the National Bank of the Republic of Kazakhstan for the Development of the National Stock Market for 2018-2021)	+	+	+	+

Policy and Regulation Legislations	Notes	Kazakhstan	Kyrgyzstan	Tajikistan	Turkmenistan	Uzbekistan
Cross border data flow/data transaction	All countries have established their own standards for virtually unimpeded transactions, however, in practice the implementation differs. According to experts there is initiatives among the EAEU member states to develop cross-border data transfer regulation, cross-border trust space to ensure information interaction between legal entities and individuals within the EAEU, a single platform for digital identification of business entities, job placement and employment facilitation ecosystem. (Source: https://unctad.org/system/files/non-official-document/tdb_ede3_2019_s06_Eurasian_en.pdf)	+	+	+	+	+
Digital Code	In Pipeline in Kazakhstan and Kyrgyzstan					

2022