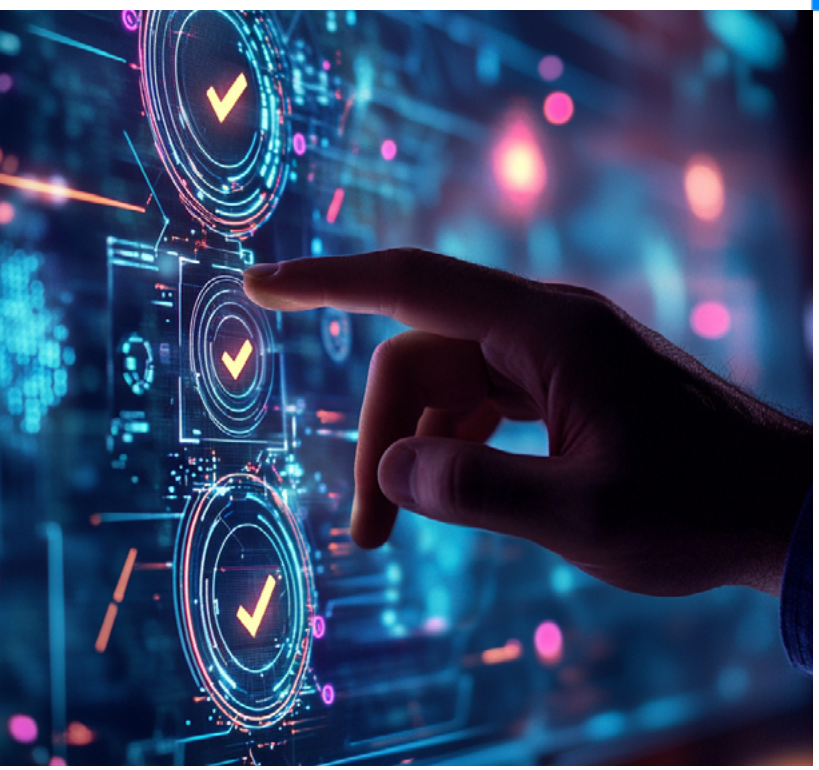
DRCQ

Digital Rights Rating



2024

Digital Rights
Rating 2024

2024

Purpose

The annual research aims at assessing policies and practices of companies in Kazakhstan's FinTech, E-commerce and Telecom sectors:

- on disclosing data as part of their interaction with government agencies;
- on complying with standards for the protection of digital human rights;
- on making efforts to ensure users' rights to freedom of information and privacy.

The research has been prepared by:

- Ruslan Daiyrbekov
- Vadim Melyakov
- Yelzhan Kabyshev
- Danila Bekturganov
- Malika Azhikenova

Research Advisor:
Leandro Ucciferri, World Benchmarking Alliance - Engagement Lead for Ranking Digital Rights (RDR)

Contents

About Us

Digital Rights Compliance Ranking 2024 has been compiled by experts from the law firm Digital Rights Center Qazaqstan (DRCQ) in cooperation with Ranking Digital Rights (RDR).

This research project was launched by DRCQ to conduct an independent study aimed at assessing policies and practices of digital platforms in Kazakhstan. The research focuses on the disclosure of information in the context of relations with government agencies, compliance with the standards for the protection of digital human rights, and measures to ensure users' rights to freedom of information and personal privacy.

This year, the categories of companies assessed were divided into 3 major sectors - FinTech, E-commerce, and Telecom - for which respecting and protecting human rights should be a priority as per the highest standards of the UN Guiding Principles on Business and Human Rights.

We have also improved our methodology for selecting companies to increase transparency and make the methodology easier to understand, which is described in the relevant section of this report.

The team at DRCQ includes professional cyber lawyers (IT & IP Law), attorneys, telecom and communications experts, media lawyers, fintech and e-commerce lawyers, as well as technical experts, programmers and financial analysts, covering a wide range of matters for clients.

> *"Through the prism of the indicators of Ranking Digital Rights and by following the recommendations suggested, these companies will have reason to be proud of their reputation, opening up opportunities to provide their services not only in the Kazakhstani digital market, but also at the international level. The rating will allow companies to move to the next level of corporate responsibility and understand what additional efforts should be made to improve the level of compliance and protection of digital rights of users",*
>
> — **Ruslan Daiyrbekov**,
> Director at DRCQ.

Methodology for Selecting Companies for the Digital Rights Compliance Ranking 2024

We have been consistently striving to improve all aspects of our legal practices at DRCQ as well as strengthen the credibility of our analytical, public-facing projects like the Digital Rights Compliance Ranking. As part of the feedback for Digital Rights Rating 2023, we have scrutinized the feedback we received and significantly evolved our methodology for selecting companies.

Our goal is to make sure that every company understands the selection criteria and process, and can trust our assessment to further enhance its own transparency and raise the trust of its users and customers.

Stage 1. Open online voting among followers in social networks

In spring, we organized an online voting among followers of our official pages in social networks (Instagram, Telegram, Facebook and LinkedIn). The voting allowed users to choose from a variety of companies operating in Kazakhstan in three key sectors of the digital economy: FinTech, E-commerce, and Telecom. Followers could also suggest their own choices of companies in the comments to the posts.

Stage 2. Voting among the participants of themed events via email survey

The online survey was also conducted among audiences that demonstrated active interest in digital rights and internet regulation through participation in major events and forums such as Privacy Day and Qazaqstan IGF. The audience of these events consists of representatives of various stakeholders, business, academia, civil society and government agencies.

Stage 3. Formation of a pool of independent experts from Kazakhstan to conduct voting using a questionnaire

A pool of independent experts from Kazakhstan was created by DRCQ researchers in order to emphasize professional competence in the process of selecting companies. The pool includes public figures with significant contribution to the formation of the business community, development of entrepreneurship and promotion of digital rights in Kazakhstan.

Questionnaire for experts:

The questionnaire created using the results of the online voting in the previous stages was provided to independent experts.

Leading professionals of the digital industry rated each company on a point system in the questionnaire:

1 point — I do not believe that the company should be included in the Ranking
2 points — more likely "no" than "yes"
3 points — there are some doubts, but I admit that this company should be considered
4 points — this company is suitable for inclusion in the Ranking, but it may be worth considering other options not included in this list.
5 points — this company should definitely be included in the Ranking of 2024

Independent experts also had the opportunity to suggest their candidate companies in the questionnaire.

Stage 4. Analysis of results and start of work

Having analyzed the final results from the questionnaire, the following digital companies received the highest voting scores in the Telecom, FinTech, and E-commerce categories:

FinTech:

- Halyk Bank
- Freedom Bank
- Jusan Bank

Telecom:

- Freedom Telecom
- Beeline
- Kcell/Active

E-commerce:

- OLX
- Satu
- Yandex Delivery

Companies that were also nominated in the voting, but did not receive enough points to be included in the ranking this year, and yet may be included in the future: Forte Bank, Forte Market, TransTelecom, Wildberries, OZON, Airba Fresh, Arbuz.kz, Sulpak, Buhta.kz, Technodom, ByBit, Mechta.kz.

Information on Selected Companies

In selecting the categories for the Digital Rights Compliance Ranking 2024, we based our choices on the importance of the sectors of the digital economy that have the greatest impact on lives of users in Kazakhstan.

1 Fintech is a rapidly growing sphere that not only simplifies access to financial services, but also handles large amounts of sensitive data, including users' financial information.

2 E-commerce - the sector of e-commerce has become an integral part of everyday life of people in Kazakhstan. This segment actively collects and uses personal data to provide services, marketing and delivery, which makes analyzing their privacy and transparency policies critical.

3 Telecom is the backbone of the country's entire digital infrastructure. Companies in this sector provide internet access and connectivity to millions of users, and store data on users' online activities.

Halyk

FREEDOM BANK

JUSAN

FREEDOM TELECOM

5G Kcell activ

satu

olx KAZAKHSTAN

Яндекс Go

Halyk Bank of Kazakhstan JSC

Halyk Bank of Kazakhstan JSC is the largest general-purpose commercial bank in the Republic of Kazakhstan. As of 2024, it offers a variety of services, including a super-application with mobile banking, its own marketplace and many types of banking and financial transactions.

Freedom Bank Kazakhstan JSC

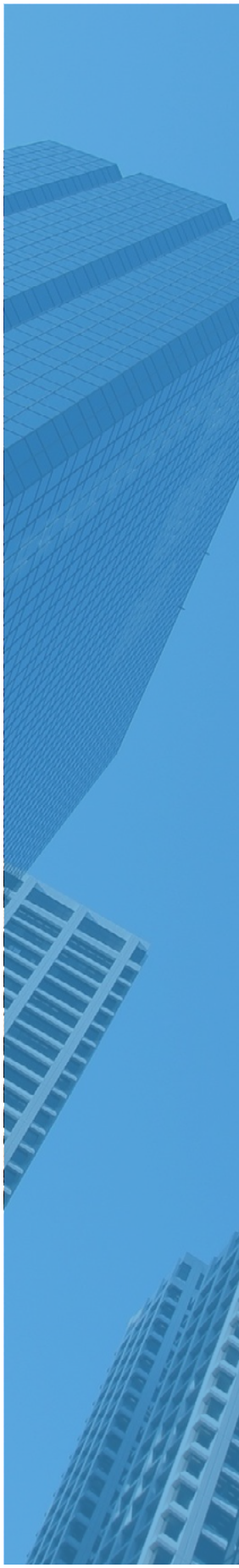
Freedom Bank Kazakhstan JSC specializes in providing financial services to individuals and small businesses. The bank has been represented in the market of Kazakhstan for 15 years, since 2009, when the bank received a license to conduct banking and other operations. The bank provides services of mobile banking, mortgage programs, opening of brokerage accounts, insurance and many other financial services through its super-application.

First Heartland Jusan Bank JSC

First Heartland Jusan Bank JSC is a retail bank in Kazakhstan. Today the Bank has more than 100 branches in 42 cities of Kazakhstan, 2.5 million customers and about 5 thousand employees. It has its own super app, marketplace, digital mobile operator and a range of investment instruments, together with many other financial services.

Beeline Kazakhstan

Beeline Kazakhstan is one of the largest telecom operators in Kazakhstan, providing mobile communications, fixed internet and other solutions. The company is managed by Veon and serves millions of customers across the country. Beeline is actively implementing innovative technologies, including 4G, IoT and Big Data, as well as developing an ecosystem of digital services such as mobile applications, e-wallets and cloud solutions.



Freedom Telecom

Freedom Telecom is a telecommunications company developing broadband Internet access to every home and open Wi-Fi access in major cities in the Republic of Kazakhstan. The company has ten branches: in Astana, Turkestan, Shymkent, Ust-Kamenogorsk, Atyrau, Semei, Aktau, Almaty, Konayev and Taraz. Customers are individuals, large, medium and small businesses, and also government agencies in Kazakhstan.

Kcell JSC (Kcell and Activ brands)

Kcell JSC (Kcell and Activ brands) is a major mobile operator in Kazakhstan, providing communication services, mobile Internet and digital solutions for private and corporate customers. The Company is actively developing 4G and 5G networks, ensuring connection speed and stability. Kcell focuses on innovation, offering customers a wide range of digital services, including online payments, entertainment platforms and cloud-based solutions.

SATU.kz

SATU.kz is a popular aggregator of ads in Kazakhstan, providing a convenient platform for buying and selling goods and services. The portal unites thousands of sellers and buyers, offering a wide range of categories: from electronics and household appliances to real estate and cars. It has been operating on the Kazakhstan market since 2008. There is a mobile application.

OLX Kazakhstan

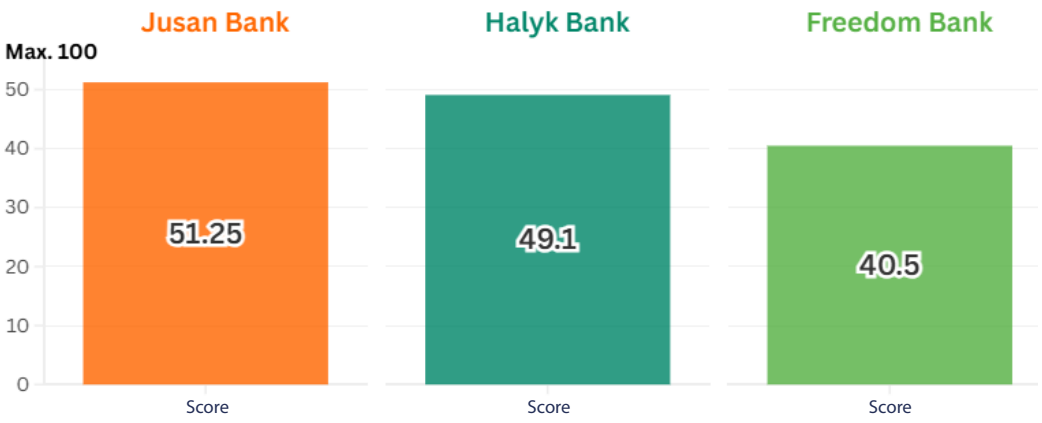
OLX Kazakhstan is a large online platform for placing ads, allowing users to buy, sell or exchange goods and services. The platform covers a wide range of categories: real estate, auto, electronics, clothing, services and so much more. The platform is available from both computer and mobile devices. In Kazakhstan, OLX was launched in 2014. In 2024, the OLX app was among the top 10 most downloaded apps in Kazakhstan through the App Store.

Yandex Go Delivery

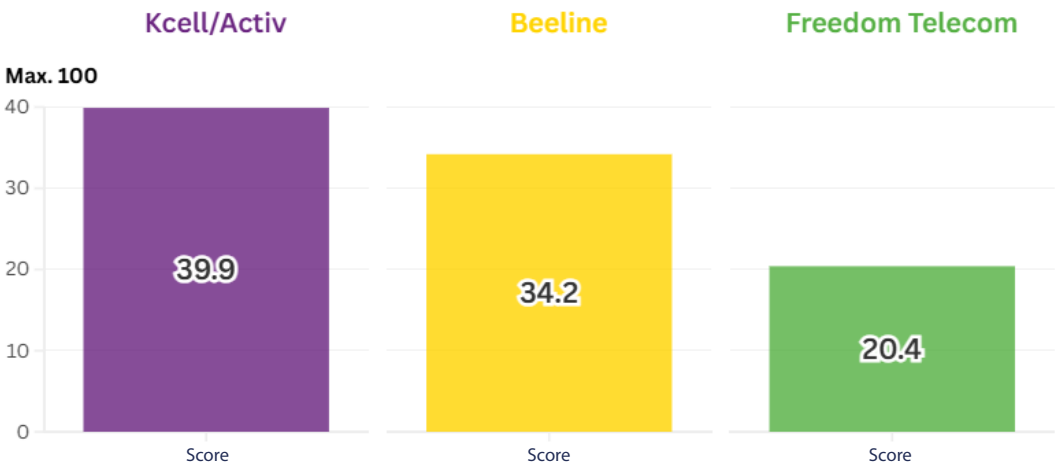
Yandex Go Delivery is a mobile application of Yandex related to transportation and delivery. It was created on the basis of Yandex Taxi service. It includes several Yandex services: Taxi, Transportation, Food, Shops, Delivery, Market, and electric scooter rental. In Kazakhstan, the service has been operating since 2016 as a Taxi service, having developed in 2020 as a super-application with a variety of transportation and commercial functions.

Total Scores of Companies by Digital Economy Sector

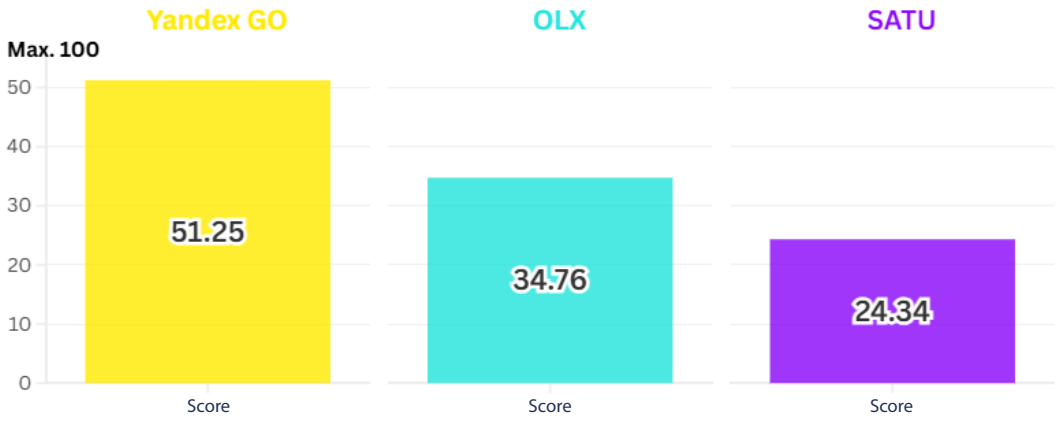
FinTech



Telecom



E-commerce



Methodology

For the purpose of analyzing companies' public attitudes and policies on digital human rights compliance, we used the official web pages and web resources of the parent companies/group of companies. All publicly posted documents of the companies were taken and archived for the period from May to July 2024 and were reviewed by us as part of the research work until the end of August 2024.

The indicators which are used to assess the companies are based on the 2020 Ranking Digital Rights corporate accountability methodology. The indicators and sub-indicators are described in greater detail on our website, on the Methodology page as well as in the Annex of the Report.

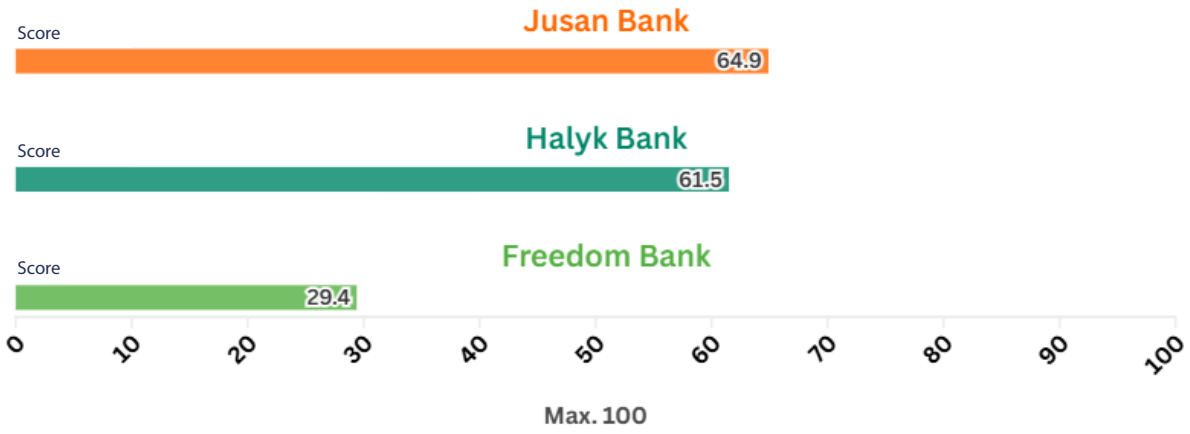
The issues under research were grouped according to three indicators.

G. Corporate Governance

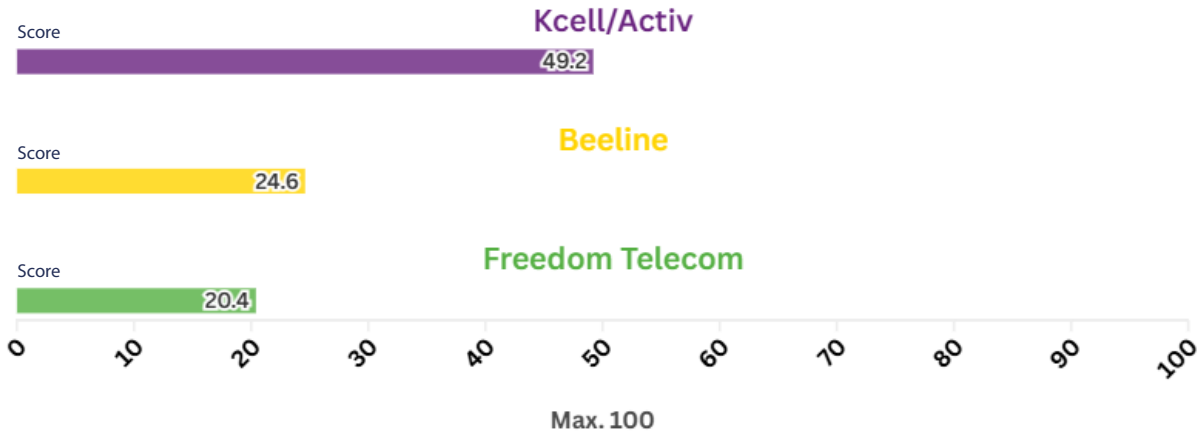
The indicators in this category are intended to demonstrate that the company has governance processes in place that honor human rights to freedom of expression and privacy. For a company to perform well in this category, its business disclosures should, as a minimum, reflect and preferably exceed the UN Guiding Principles on Business and Human Rights and other human rights standards on freedom of expression and privacy adopted by the Global Network Initiative. Also, to achieve a high score in this category, a company must demonstrate that it conducts regular independent audits, training programs for employees on protecting sensitive data, and consultations with stakeholders. It is important to provide mechanisms to protect user rights, such as a customer complaint function, and to have documented processes for responding to breaches, such as internal investigations and remedial actions.

> *Note: Due to the specifics of each sector (FinTech, Telecom, E-commerce), the total number of indicators differs from sector to sector. In this regard, it is most appropriate to compare companies only within their own sector.*

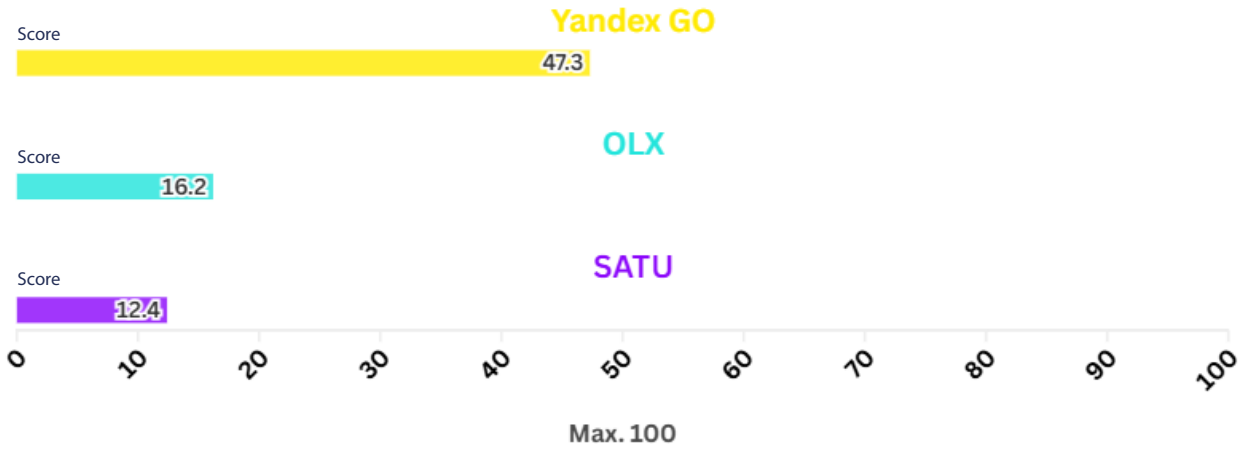
FinTech: G-indicators



Telecom: G-indicators



E-commerce: G-indicators

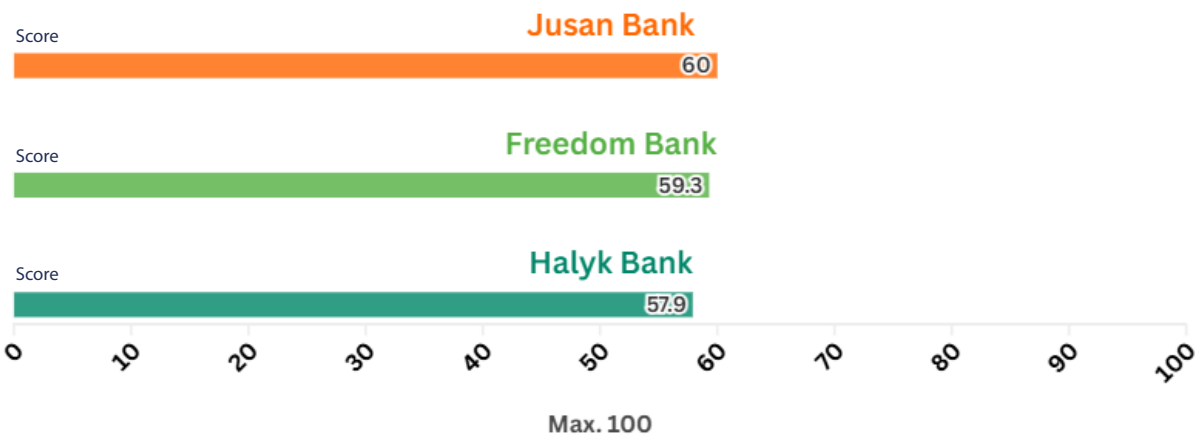


F. Freedom of Expression and Information

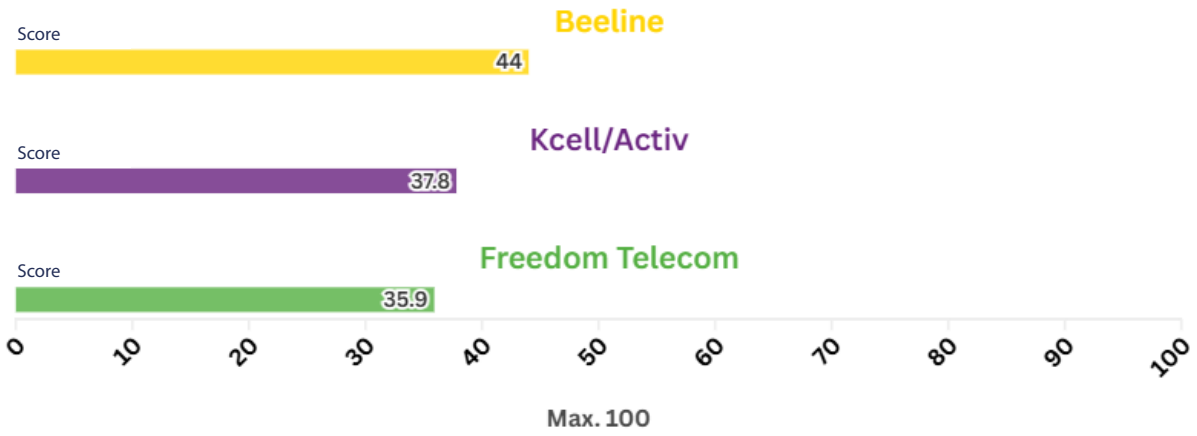
Indicators in this category help in determining if the company has demonstrated respect for the rights to freedom of expression and information in accordance with international human rights standards. The company's published policies and practices clearly demonstrate what actions are taken to address human rights abuses, unless such actions are lawful, proportionate and for a justifiable purpose. Companies that perform well on this indicator show their commitment to the principle of openness not only in how they respond to demands from the government and other stakeholders, but also in how they establish, explain and comply with their own business rules and principles that affect users' fundamental right to freedom of expression and information.

> *Note: Due to the specifics of each sector (FinTech, Telecom, E-commerce), the total number of indicators differs from sector to sector. In this regard, it is most appropriate to compare companies only within their own sector.*

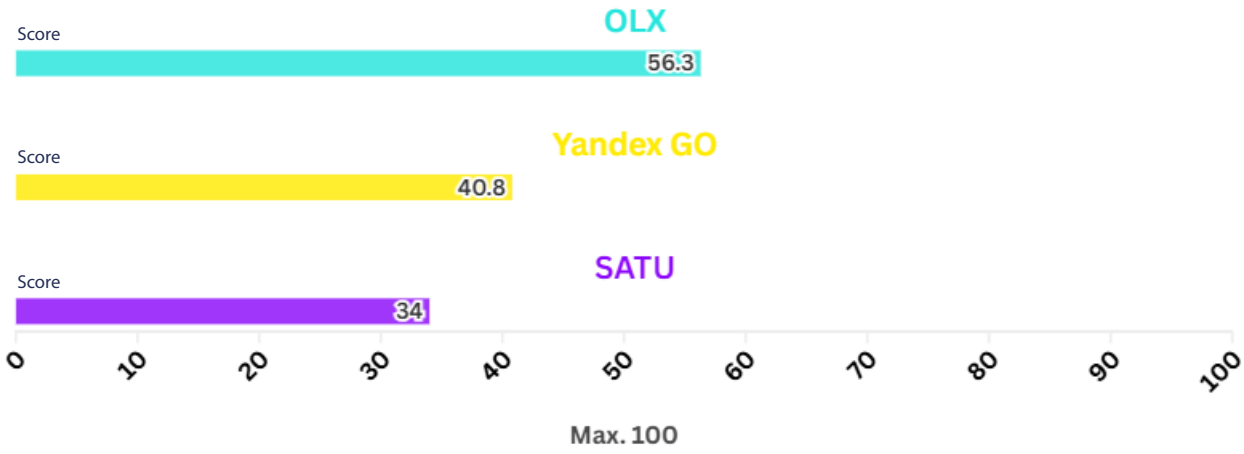
FinTech: F-indicators



Telecom: F-indicators



E-commerce: F-indicators

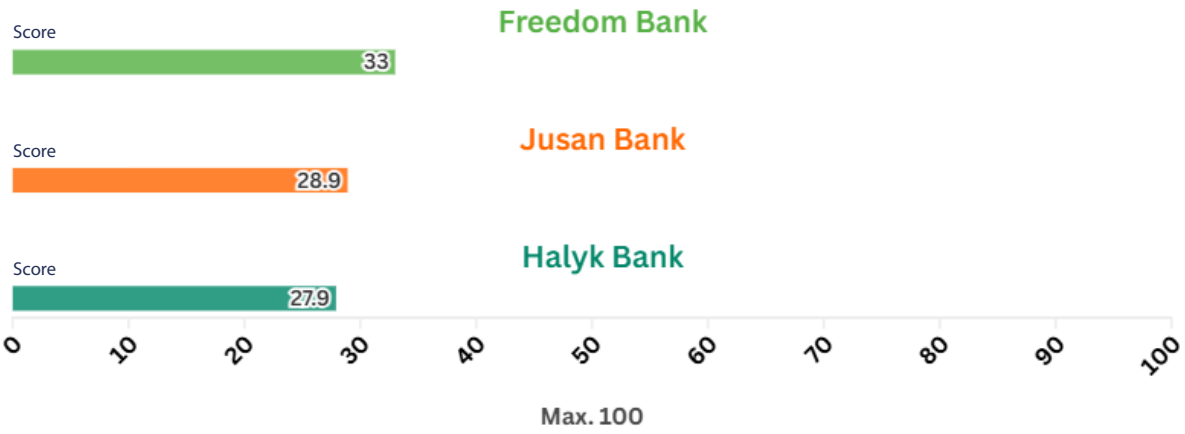


P. Privacy

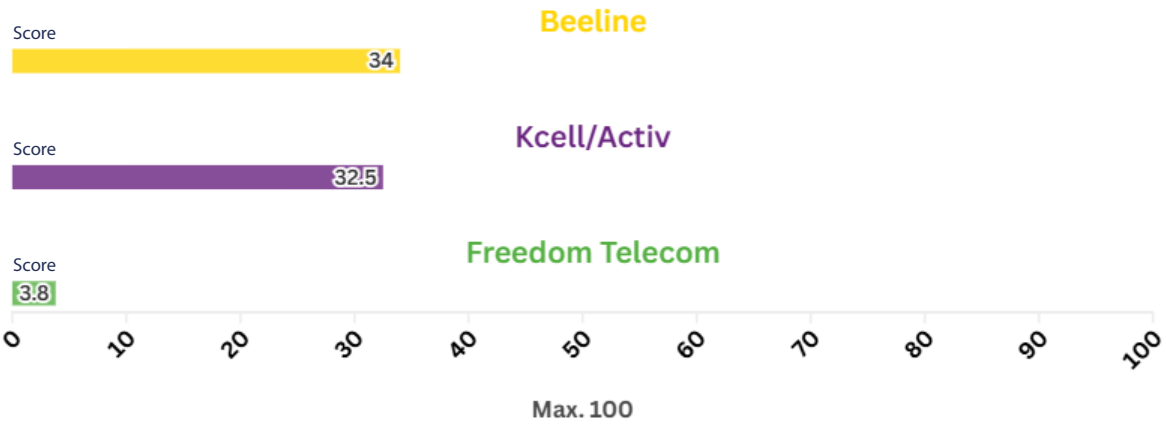
Indicators in this category reflect that companies strive to communicate their commitment to users' right to privacy in an accessible way, through examples of their policies and practices, in line with international human rights standards. They also demonstrate strong dedication to protecting and safeguarding digital security of both users and company's employees. In addition, the category assesses whether companies are open about their policies for processing personal data, including its collection, use, storage and transfer to third parties. It also examines how companies take measures to minimize the risks of data breaches, give users control over their data, and clearly communicate their privacy mechanisms.

> *Note: Due to the specifics of each sector (FinTech, Telecom, E-commerce), the total number of indicators differs from sector to sector. In this regard, it is most appropriate to compare companies only within their own sector.*

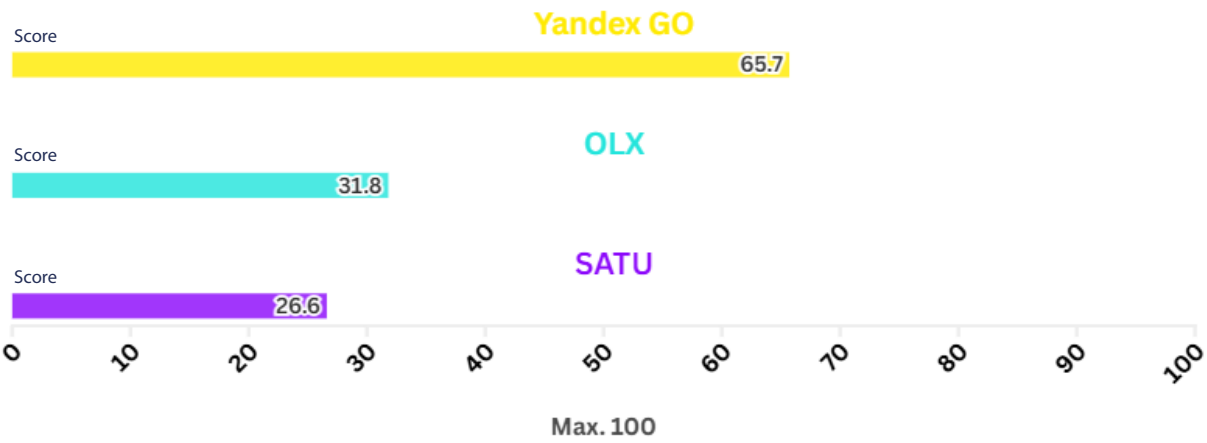
FinTech: P-indicators



Telecom: P-indicators



E-commerce: P-indicators



The research process consisted of the following steps:

1. Compiling an inventory of publicly available documents of each service by the first expert;
2. Analyzing the documents and scoring each indicator by the first expert;
3. Validating obtained results by the second and third experts;
4. Interacting with the companies and their digital platforms, which is known as Company Engagement;
5. Performing the horizontal "verification": comparing the companies' results with each other in order to maintain a unified and objective approach and coordinating the final scores with the Ranking Digital Rights team.

Each indicator has a list of parameters, and companies receive a score (full, partial or zero) for each parameter met. The score takes into account the degree of disclosure for each indicator parameter based on one of the following possible answers:

"Yes" (full disclosure): the disclosure complies with the requirements of the specific indicator.

"Partial": the company has disclosed some but not all aspects of the indicator, or the disclosure is not complete enough to meet all the requirements of the indicator.

"No data on disclosure": researchers could not find information on the company's website that answers the element's question.

"No": information exists, but it does not specifically disclose the subject matter of the query on the parameter. This option is different from "No disclosure found," although both do not score favorably.

"Not Applicable": the element is not relevant to the company or service. Items marked as "Not Applicable" will not be counted in the scoring for or against the parameter.

Scoring

- Yes/full disclosure = 100
- Partial disclosure = 50
- No disclosure = 0
- No data on the disclosure = 0
- Not applicable - data are not included in scoring and averaging.

Company Engagement

Awarding the companies that gained the highest scores in the rating or took a nomination in the Company Engagement process, held as part of the presentation of the research results at the Qazaqstan IGF 2024 Forum.

As part of the research project, the Digital Rights Rating team contacted the selected companies and invited them to review preliminary findings of the report and provide feedback. Publicly available contact information on official websites was also used to reach the companies. Official letters from DRCQ were sent to e-mail addresses and via feedback forms.

The process of interacting with the companies under consideration, called the Company Engagement, is undoubtedly the key to the rating methodology. We aim for our research to be not only an assessment, but also a tool to encourage companies to comply with international standards regarding respect for digital human rights, including users' rights to information and privacy. For companies, it is a unique opportunity to get an independent assessment of their efforts on digital rights, learn about their strengths and identify areas for improvement.

For companies' customers, this dialog is an important signal that the company is open to criticism, committed to improving its practices and respectful of the rights of its users.

Through this rating, the Digital Rights Rating team offers roadmaps for companies that prioritize respect for and protection of human rights to build and operate online platforms and digital services in line with the UN Guiding Principles on Business and Human Rights.

Companies that provided feedback on preliminary ranking results:

- **Freedom Bank**
- **Freedom Telecom**
- **Kcell/Activ**
- **Yandex Go Delivery**

In the Fintech sector, representatives from Freedom Bank responded to the call and were presented with preliminary results with explanations of the indicators. The bank representatives reviewed the data and expressed their willingness to strengthen compliance measures and take into account recommendations of the Ranking. Specifically, Freedom Bank received a positive score of 29.4 in the corporate governance sector compared to 61.5 for Halyk and 64.9 for Jusan. However, in terms of corporate governance indicators, Freedom Bank lagged behind Halyk and Jusan banks on certain subindicators, such as:

- G3.1: Does the company provide clear information on staff training on freedom of expression and information?
- G3.2: Does the company provide clear information on staff training on privacy issues?
- G5.1: Is the company a member of one or more multi-stakeholder initiatives to explore all possible ways in which users' basic rights, freedom of expression and information, privacy and non-discrimination may be impacted as a result of the company's activities?

It is worth noting that Freedom Bank scored the highest among FinTech companies in the category of Privacy Compliance. The bank received the nomination in Privacy Compliance for the above-mentioned indicators and active participation in the Company Engagement process.

> *"By developing digital services and using big data, we significantly simplify the interaction between the client and the bank. At the same time, we realize that while processing huge amounts of data, our priority task resides in ensuring its secure storage. To maintain a high level of privacy, we invest significant financial and human resources and adhere to international standards for digital rights compliance. Freedom Bank's recognition as the best Privacy Compliance company in the FinTech sector emphasizes our commitment to transparency and protection of users' rights,"* Aidos Zhumagulov, the member of Freedom Bank's Board of Directors, said when commenting on the company's results in the Ranking.

In the Telecom sector, Freedom Telecom and Kcell JSC provided feedback to the research team and expressed their willingness to see preliminary results of the Digital Rights Compliance Ranking and to receive explanations on the Ranking methodology and scoring system.

Based on the aggregate results, Kcell JSC was determined to be the best company in this sector. Kcell received the highest scores in the G-sector of corporate governance, with voluminous, yet clear enough public documents on corporate ethics, risk management system and annual report. In order to provide more detailed feedback, the Digital Rights Rating team was invited to the Kcell/Activ office in Almaty to familiarize managers and employees of the company's legal and technical departments with the research in general, and with the specific results for Kcell/Activ. After the meeting, the company's legal department received tables with the results for all indicators.

> *"The rapid penetration of various online services, digital services, IT solutions, products and technologies into our lives has equated the digital rights of citizens and users with basic and fundamental rights, such as the right to freedom, personal integrity, education, etc.*
>
> *Therefore, being recognized as a leader in the Telecom sector in the Digital Rights Compliance Ranking is not only an assessment of our efforts to ensure the security of corporate resources and digital assets, but also an incentive for us to further improve our services, their security, and the fault tolerance of all systems and services of the company,"* Daniyar Ibrayev, the Chief Security Officer of Kcell JSC, said.

Freedom Telecom demonstrated lower results in the Ranking compared to Beeline and Kcell. This situation is due to the fact that such key public documents as the "User Agreement" and "Privacy Policy" were not available on the company's official website at the time of the research. Availability and accessibility of these documents are integral elements of transparent interaction with users and ensuring their digital rights, which, in turn, significantly reduced the possibility of scoring a higher final score.

Nevertheless, the telecom operator's resource included the "Public Agreement for Provision of Services to Individuals" and the "Code of Ethics and Business Conduct". Since according to the rating methodology we are obliged to take into account all public documents, the company was evaluated based on these sources.

Freedom Telecom received favorable scores on corporate governance (G) and respect for freedom of expression and information rights (F), but scored virtually no points in the Privacy (P) section. User privacy is a fundamental indicator that, along with corporate governance and respect for freedom of expression, reflects a company's responsibility to society and its commitment to international digital human rights standards.

The Digital Rights Rating research team recommends that companies always make the most complete and detailed forms of documents such as "User Agreement", "Privacy Policy", and "Personal Data Processing Policy" publicly available on their resources. At the same time, it is also important that the information in these documents is presented in a user-friendly form in the state language and the language of international communication.

Яндекс Go

Yandex Go Delivery has the highest score on aggregate indicators in the E-commerce sector. It is also noteworthy that Yandex Go Delivery has the highest score in the Privacy (P) section of its sector.

Yandex Delivery representatives reached out to Digital Rights Rating's research team. During the interaction, the team presented the company with the methodology of the Digital Rights Compliance Ranking as well as detailed the assessment criteria and analysis mechanisms. In addition, the management of the service was presented with the preliminary results of the research. The discussion of the results allowed to draw the company's attention to the best practices used by large international services in the field of E-commerce.

The Digital Rights Rating team provided recommendations to companies in the area of digital human rights compliance, along with their adherence to international standards, which will help them improve their existing approaches and strengthen their commitment to the protection of users' digital rights.

We express our sincere gratitude to the companies that responded to our invitation to dialog and participated in such an important process as Company Engagement. This engagement format plays a pivotal role not only in increasing the transparency of our research, but also in enabling companies to improve their digital human rights practices and policies.

Participation in the Company Engagement brings significant benefits for all parties: users gain confidence in the reliability of companies in terms of protecting their rights and data, companies strengthen the trust of customers and their reputation, as a result of which the digital economy of Kazakhstan as a whole becomes more sustainable and oriented towards international standards.

General Conclusions

1. The good news is that the majority (six) of the companies reviewed have some form of mention that the organization respects and respects human rights, including the right to freedom of expression and information, as well as the right to privacy. However, more often than not, this is reflected in insufficiently clear wording.

2. Only Kcell JSC was found to have a document explicitly titled "Kcell JSC Policy on Freedom of Expression in Telecommunications".

3. No company has a clear and transparent description of policies on the development and use of algorithmic systems and automatic content curation. And this is particularly important given the current context in which these technologies are evolving.

4. Most of the companies' policies state that top management and senior and middle managers are involved in one way or another in the process of controlling how the company respects the rights of employees and customers to freedom of expression and privacy. In addition, many of the companies surveyed clearly reflect in their policies the procedures for filing complaints about violations of the above rights.

5. It has been discovered that none of the public documents clearly and transparently reflect the process for responding to requests from public authorities or private third parties (e.g. the media) to restrict user accounts or request their personal data. Companies note that they may share their users' personal data with the authorities "in accordance with the laws of the Republic of Kazakhstan", but there is no clarity on the scope of the data shared and whether the user is then notified that their data has been shared.

6. It is also worth noting that neither company publishes the number of such requests from local or foreign government agencies or private third parties.

7. Of all the reviewed companies, only Yandex Go has a clearly stated policy on targeted advertising. And there is also a mention that such advertising can be disabled at the user's request.

8. Only Yandex publishes a Transparency report on data privacy on a regular basis. However, even this company reflects mostly the data on the Russian Federation, while it should also reflect the data on the Republic of Kazakhstan.

9. It is also important to point out that many of Yandex's public documents, directly or generally reflecting the company's policy with respect to the "Yandex Go Delivery" service in Kazakhstan, refer to the legislation of the Russian Federation, not Kazakhstan.

10. At the time of the research, the homepage of Freedom Telecom's website featured an image with the CEO of Freedom Holding Corp. Timur Turlov and his quote: "The UN Human Rights Council has adopted a resolution that equates access to the Internet with basic human rights. Our strategic goal is to realize this right for every citizen of the Republic of Kazakhstan". This approach was welcomed by the research team. All participants in the digital economy sector should strive both in their policies and in practice to comply with the highest international standards in relation to digital human rights.

11. Most of the selected companies scored high on the sub-indicator "F1a - Access to Terms of Service". Their public documents and policies were easy to find on the main pages of their official websites and were presented in an understandable manner. Also, to receive a high score on this indicator, all company policies should be available in the state and Russian languages. Only Satu.kz was found not to have some of their terms of service fully reflected in the state language.

12. Only Jusan Bank, Yandex Go and OLX maintain public archives of previous versions of their terms of service policies and make it possible to review past versions of the user agreement or privacy policy.

13. Most companies in their privacy policies at least partially disclose what data they collect about users and how they obtain that data.

14. Only Kcell JSC explicitly states the names of third party organizations to whom the company may share users' personal data. The other companies only mention them in general terms, such as "Partners", "Third Party", "Authorized Bodies" and suchlike.

15. Halyk and Jusan banks, as well as Yandex Go and Kcell/Activ, have high scores in the G-section of Corporate Governance section, including in the context of the companies' approach to respecting human rights and training their employees to respect privacy and users' rights to freedom of expression and information.

16. According to the sub-indicator "P15. Data Leaks" in the Privacy section, companies are required to reflect in their policies a clear procedure for responding to personal data leaks and to promptly report leaks to the relevant government authorities. None of the policies of the companies under study explicitly state that in case of leaks they will notify the relevant authority without delay. Nevertheless, Freedom Bank, Beeline, Kcell/Activ and Yandex Go make a general statement in their documents that they take all necessary cybersecurity measures to protect personal data.

17. Freedom Bank received the highest score among companies in the Fintech sector in the P-section of Privacy. As to the Telecom sector, the leader of the Privacy is Beeline, while in the E-commerce sector, Freedom Bank has received the highest score in the Privacy section.

Recommendations

In order to increase transparency of companies' activities and strengthen high standards of digital rights compliance, DRCQ experts, based on the obtained data and analysis results, have developed a set of universal recommendations for companies and services operating in the digital economy sector. The recommendations will allow digital platforms to independently assess compliance with the proposed standards and identify areas for improvement.

Freedom of Expression and Information

1. The company's obligations to respect human rights and protect users' rights to freedom of expression and access to information should be clearly and understandably stated in its public policies. We recommend paying attention to international standards and be guided in this matter by the following international documents: Universal Declaration of Human Rights; International Covenant on Civil and Political Rights; UN Guiding Principles on Business and Human Rights.

2. Companies should publicly inform users when they receive requests from government authorities to remove content, user accounts or restrict access to information. It is important to explain how such requests are assessed by companies (including senior management) for legality, proportionality and reasonableness, and what the company's policy is regarding responding to such requests.

3. There should be clear rules for customer complaints and mechanisms in place to allow users to file complaints and challenge decisions regarding content restriction or account blocking. These mechanisms should be understandable, accessible, and focused on ensuring fair and timely treatment of issues that arise.

4. Regular risk assessments on digital and consumer human rights should be conducted with the involvement of independent auditors.

Corporate Governance

1. Mechanisms should be put in place to monitor compliance with international human rights standards. For example, conduct regular audits, keep reports and be sure to involve the company's senior management in this process.

2. Companies should organize regular training for their employees, especially those who work directly with customers or with their personal data. This will help raise awareness and strengthen internal processes to respect human rights. Employees themselves should also be made aware of who they can complain to and the procedure to follow if their rights have been violated.

Privacy

1. It is recommended to develop detailed privacy policies that specifically explain what user data is collected, how it is used, where and how much it is stored, and whether it is shared with third parties. Policies should be written in clear language.

Separately, it is recommended to disclose the names of third-party organizations to whom users' personal data may be shared.

2. Ensure that users can control how their data is used in targeted advertising. In addition, users should be able to easily disable targeted advertising or limit data collection for these purposes. It is recommended to provide access to clear privacy settings where users can choose the level of ad personalization, including opting out of data collection for such purposes.

3. Publish Transparency Reports on their sites on a regular basis. Such reports allows companies to describe how they deal with requests from the government, law enforcement, or other parties.

Such report typically shows:

- How many times government agencies requested user data
- What data were requested (e.g., contact information, messages, IP addresses)
- How many requests the company has approved or denied and why
- How often the company, for example, removes content or restricts access to content, at the request of government authorities.

4. Companies should clearly indicate whether they collect user data for machine learning and its further use in algorithmic systems, including AI assistants, chatbots, etc.

5. Disclose in detail the procedures for revoking and destroying user data upon request or when the purposes of collecting that data have been achieved.

6. Promptly notify users of the facts of their data leakage, as well as promptly notify the authorized state agency.

7. Publish practical materials to educate users on how to protect themselves from cybersecurity risks associated with the company's products or services.

8. Minimize the collection of user data, limiting it to the information that is necessary for the provision of services.

Legislation

When implementing the project, we were guided by the following laws and regulations:

- UN Guiding Principles on Business.
- Universal Declaration of Human Rights.
- International Covenant on Civil and Political Rights (ICCPR).
- International Covenant on Economic, Social and Cultural Rights.
- Entrepreneurial Code of the Republic of Kazakhstan dated October 29, 2015, No. 375-V ZRC.
- Law of the Republic of Kazakhstan "On Personal Data and Their Protection" dated May 21, 2013, No. 94-V.
- Law of the Republic of Kazakhstan "On Access to Information" dated November 16, 2015, No. 401-V ZRC.
- Law of the Republic of Kazakhstan "On Informatization" dated November 24, 2015, No. 418-V ZRC.
- Law of the Republic of Kazakhstan "On Communications" dated July 5, 2004, No. 567.
- Law of the Republic of Kazakhstan "On Online Platforms and Online Advertising" dated July 10, 2023, No. 18-VIII ZRC.
- Order of the Minister of Digital Development, Innovation and Aerospace Industry of the Republic of Kazakhstan "On Approval of the Rules of Information Content of Internet Resources of State Bodies and Requirements to Their Content", dated April 2, 2021, No. 114/NK
- Decree of the Government of the Republic of Kazakhstan "On Approval of Unified Requirements in the Field of Information and Communication Technologies and Information Security" dated December 20, 2016, No. 832
- Law of the Republic of Kazakhstan "On Amendments and Additions to Certain Legislative Acts of the Republic of Kazakhstan on Information and Communications" dated December 28, 2017, No. 128-VI ZRC.
- Law of the Republic of Kazakhstan "On Amendments and Additions to Certain Legislative Acts of the Republic of Kazakhstan on Stimulating Innovations, Development of Digitalization, Information Security and Education" dated July 14, 2022, No. 141-VII ZRC.

- Law of the Republic of Kazakhstan "On Amendments and Additions to Certain Legislative Acts of the Republic of Kazakhstan on Implementation of the Address of the Head of State dated March 16, 2022" dated November 5, 2022, No. 157-VII ZRC
- Law of the Republic of Kazakhstan "On Amendments and Additions to Certain Legislative Acts of the Republic of Kazakhstan on Digital Assets and Informatization" dated February 6, 2023 No. 194-VII ZRC
- Law of the Republic of Kazakhstan "On Amendments and Additions to Certain Legislative Acts of the Republic of Kazakhstan on Defense and Aerospace Industry, Information Security in the Sphere of Informatization" dated March 18, 2019, No. 237-VI ZRC.

Annex 1

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?

G3. Internal implementation

Elements:

1. Does the company clearly disclose that it provides employee training on freedom of expression and information issues?
2. Does the company clearly disclose that it provides employee training on privacy issues?
3. Does the company clearly disclose that it maintains an employee whistleblower program through which employees can report concerns related to how the company treats its users' freedom of expression and information rights?
4. Does the company clearly disclose that it maintains an employee whistleblower program through which employees can report concerns related to how the company treats its users' privacy rights?

G4(a). Impact assessment: Governments and regulations

Elements:

1. Does the company assess how laws affect freedom of expression and information in jurisdictions where it operates?
2. Does the company assess how laws affect privacy in jurisdictions where it operates?
3. Does the company assess freedom of expression and information risks associated with existing products and services in jurisdictions where it operates?
4. Does the company assess privacy risks associated with existing products and services in jurisdictions where it operates?
5. Does the company assess freedom of expression and information risks associated with a new activity, including the launch and/or acquisition of new products, services, or companies, or entry into new markets or jurisdictions?
6. Does the company assess privacy risks associated with a new activity, including the launch and/or acquisition of new products, services, or companies, or entry into new markets or jurisdictions?
7. Does the company conduct additional evaluation whenever the company's risk assessments identify concerns?
8. Do senior executives and/or members of the company's board of directors review and consider the results of assessments and due diligence in their decision-making?
9. Does the company conduct assessments on a regular schedule?
10. Are the company's assessments assured by an external third party?

G4(b). Impact assessment: Processes for policy enforcement

Elements:

1. Does the company assess freedom of expression and information risks of enforcing its terms of service?
2. Does the company conduct risk assessments of its enforcement of its privacy policies?
3. Does the company assess discrimination risks associated with its processes for enforcing its terms of service?
4. Does the company assess discrimination risks associated with its processes for enforcing its privacy policies?
5. Does the company conduct additional evaluation whenever the company's risk assessments identify concerns?
6. Do senior executives and/or members of the company's board of directors review and consider the results of assessments and due diligence in their decision-making?
7. Does the company conduct assessments on a regular schedule?
8. Are the company's assessments assured by an external third party?
9. Is the external third party that assures the assessments accredited to a relevant and reputable human rights standard by a credible organization?

G5. Stakeholder engagement and accountability

Elements:

1. Is the company a member of one or more multi-stakeholder initiatives that address the full range of ways in which users' fundamental rights to freedom of expression and information, privacy, and non-discrimination may be affected in the course of the company's operations?
2. If the company is not a member of one or more such multi-stakeholder initiatives, is the company a member of any organizations that engages systematically and on a regular basis with non-industry and non-governmental stakeholders on freedom of expression and privacy issues?
3. If the company is not a member of one of these organizations, does the company disclose that it initiates or participates in meetings with stakeholders that represent, advocate on behalf of, or are people whose rights to freedom of expression and information and to privacy are directly impacted by the company's business?

G6(a). Remedy

Elements:

1. Does the company clearly disclose it has a grievance mechanism(s) enabling users to submit complaints if they feel their freedom of expression and information rights have been adversely affected by the company's policies or practices?
2. Does the company clearly disclose it has a grievance mechanism(s) enabling users to submit complaints if they feel their privacy has been adversely affected by the company's policies or practices?
3. Does the company clearly disclose its procedures for providing remedy for freedom of expression and information-related grievances?
4. Does the company clearly disclose its procedures for providing remedy for privacy-related grievances?
5. Does the company clearly disclose timeframes for its grievance and remedy procedures?
6. Does the company clearly disclose the number of complaints received related to freedom of expression?
7. Does the company clearly disclose the number of complaints received related to privacy?
8. Does the company clearly disclose evidence that it is providing remedy for freedom of expression grievances?
9. Does the company clearly disclose evidence that it is providing remedy for privacy grievances?

G6(b). Process for content moderation appeals

Elements:

1. Does the company clearly disclose that it offers affected users the ability to appeal content-moderation actions?
2. Does the company clearly disclose that it notifies the users who are affected by a content-moderation action?

3. Does the company clearly disclosee a timeframe for notifying affected users when it takes a content-moderation action?
4. Does the company clearly disclose when appeals are not permitted?
5. Does the company clearly disclose its process for reviewing appeals?
6. Does the company clearly disclose its timeframe for reviewing appeals?
7. Does the company clearly disclose that such appeals are reviewed by at least one human not involved in the original content-moderation action?
8. Does the company clearly disclose what role automation plays in reviewing appeals?
9. Does the company clearly disclose that the affected users have an opportunity to present additional information that will be considered in the review?
10. Does the company clearly disclose that it provides the affected users with a statement outlining the reason for its decision?
11. Does the company clearly disclose evidence that it is addressing content moderation appeals?

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?

F1(c). Access to advertising targeting policies

Elements:

1. Are the company's advertising targeting policies easy to find?
2. Are the advertising targeting policies available in the primary language(s) spoken by users in the company's home jurisdiction?
3. Are the advertising targeting 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 targeting 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 targeting policy?

F1(d). Access to algorithmic system use policies

Elements:

1. Are the company's algorithmic system use policies easy to find?
2. Are the algorithmic system use policies available in the primary language(s) spoken by users in the company's home jurisdiction?
3. Are the algorithmic system use policies presented in an understandable manner?

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?

F2(b). Changes to advertising content policies

Elements:

1. Does the company clearly disclose that it directly notifies users about changes to its advertising content 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 made available through its app store to notify users when the apps change their advertising content policies?
6. (For personal digital assistant ecosystems): Does the company clearly disclose that it requires skills made available through its skill store to notify users when the skills change their advertising content policies?

F2(c). Changes to advertising targeting policies

Elements:

1. Does the company clearly disclose that it directly notifies users about changes to its advertising targeting 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 made available through its app store to directly notify users when the apps change their advertising targeting policies?
6. (For personal digital assistant ecosystems): Does the company clearly disclose that it requires skills made available through its skill store to notify users when the skills change their advertising targeting policies?

F2(d). Changes to algorithmic system use policies

Elements:

1. Does the company clearly disclose that it directly notifies users about changes to its algorithmic system use 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?

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

F3(b). Advertising content rules and enforcement

Elements:

1. Does the company clearly disclose what types of advertising content it does not permit?
2. Does the company clearly disclose whether it requires all advertising content be clearly labelled as such?
3. Does the company clearly disclose the processes and technologies it uses to identify advertising content or accounts that violate the company's rules?

F3(c). Advertising targeting rules and enforcement

Elements:

1. Does the company clearly disclose whether it enables third parties to target its users with advertising content?
2. Does the company clearly disclose what types of targeting parameters are not permitted?
3. Does the company clearly disclose that it does not permit advertisers to target specific individuals?
4. Does the company clearly disclose that algorithmically generated advertising audience categories are evaluated by human reviewers before they can be used?
5. Does the company clearly disclose information about the processes and technologies it uses to identify advertising content or accounts that violate the company's rules?

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?

F5(a). Process for responding to government demands to restrict content or accounts

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?

F5(b). Process for responding to private requests for content or account restriction

Elements:

1. Does the company clearly disclose its process for responding to requests to remove, filter, or restrict content or accounts made through private processes?
2. Do the company's explanations clearly disclose the basis under which it may comply with requests made through private processes?
3. Does the company clearly disclose that it carries out due diligence on requests made through private processes before deciding how to respond?
4. Does the company commit to push back on inappropriate or overbroad requests made through private processes?
5. Does the company provide clear guidance or examples of implementation of its process of responding to requests made through private processes?

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?
10. Can the data be exported as a structured data file?

F7. Data about private requests for content or account restriction

Elements:

1. Does the company break out the number of requests to restrict content or accounts that it receives through private processes?
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 reasons for removal associated with the requests it receives?
5. Does the company clearly disclose the private processes that made requests?
6. Does the company list the number of requests it complied with?
7. Does the company publish the original requests or disclose that it provides copies to a public third-party archive?
8. Does the company report this data at least once a year?
9. Can the data be exported as a structured data file?
10. Does the company clearly disclose that its reporting covers all types of requests that it receives through private processes?

F9. Network management (telecommunications companies)

Elements:

1. Does the company clearly disclose a policy commitment to not prioritize, block, or delay certain types of traffic, applications, protocols, or content for reasons beyond assuring quality of service and reliability of the network?
2. Does the company engage in practices, such as offering zero-rating programs, that prioritize network traffic for reasons beyond assuring quality of service and reliability of the network?
3. If the company does engage in network prioritization practices for reasons beyond assuring quality of service and reliability of the network, does it clearly disclose its purpose for doing so?

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?

F12. Algorithmic content curation, recommendation, and/or ranking systems

Elements:

1. Does the company clearly disclose whether it uses algorithmic systems to curate, recommend, and/or rank the content that users can access through its platform?
2. Does the company clearly disclosee how the algorithmic systems are deployed to curate, recommend, and/or rank content, including the variables that influence these systems?
3. Does the company clearly disclose what options users have to control the variables that the algorithmic content curation, recommendation, and/or ranking system takes into account?
4. Does the company clearly disclose whether algorithmic systems are used to automatically curate, recommend, and/or rank content by default?
5. Does the company clearly disclose that users can opt in to automated content curation, recommendation, and/or ranking systems?

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?

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 notifiesusers of changes prior to these changes coming into effect?
4. Does the company maintain a public archive or change log?

P3(a). Collection of user information

Elements:

1. Does the company clearly disclose what types of user information it collects?
2. For each type of user information the company collects, does the company clearly disclose how it collects that user information?

3. Does the company clearly disclose that it limits collection of user information to what is directly relevant and necessary to accomplish the purpose of its service?
4. (For mobile ecosystems): Does the company clearly disclose that it evaluates whether the privacy policies of third-party appsmade available through its app store disclose what user information the apps collect?

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?

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?

P7. Users' control over their own user information

Elements:

1. For each type of user information the company collects, does the company clearly disclose whether users can control the company's collection of this user information?
2. For each type of user information the company collects, does the company clearly disclose whether users can delete this user information?
3. For each type of user information the company infers on the basis of collected information, does the company clearly disclose whether users can control if the company can attempt to infer this user information?

4. For each type of user information the company infers on the basis of collected information, does the company clearly disclose whether users can delete this user information?
5. Does the company clearly disclose that it provides users with options to control how their user information is used for targeted advertising?
6. Does the company clearly disclose that targeted advertising is off by default?
7. Does the company clearly disclose that it provides users with options to control how their user information is used for the development of algorithmic systems?
8. Does the company clearly disclose whether it uses user information to develop algorithmic systems by default, or not?

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?

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?

P10(b). Process for responding to private requests for user information

Elements:

1. Does the company clearly disclose its process for responding to requests made through private processes?
2. Do the company's explanations clearly disclose the basis under which it may comply with requests made through private processes?
3. Does the company clearly disclose that it carries out due diligence on requests made through private processes before deciding how to respond?
4. Does the company commit to push back on inappropriate or overbroad requests made through private processes?
5. Does the company provide clear guidance or examples of implementation of its process of responding to requests made through private processes?

P11(a). 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?

P11(b). Data about private requests for user information

Elements:

1. Does the company list the number of requests it receives for user information that come through private processes?
2. Does the company list the number of requests for user information that come through private processes with which it complied?
3. Does the company report this data at least once per year?
4. Can the data reported by the company be exported as a structured data file?

P12. User notification about third-party requests for user information

Elements:

1. Does the company clearly disclose that it notifies users when government entities (including courts or other judicial bodies) demand their user information?
2. Does the company clearly disclose that it notifies users when they receive requests for their user information through private processes?
3. Does the company clearly disclose situations when it might not notify users, including a description of the types of government demands it is prohibited by law from disclosing to users?

P13. Security oversight

Elements:

1. Does the company clearly disclose that it has systems in place to limit and monitor employee access to user information?
2. Does the company clearly disclose that it has a security team that conducts security audits on the company's products and services?
3. Does the company clearly disclose that it commissions third-party security audits on its products and services?

P15. Data breaches

Elements:

1. Does the company clearly disclose that it will notify the relevant authorities without undue delay when a data breach occurs?
2. Does the company clearly disclose its process for notifying data subjects who might be affected by a data breach?
3. Does the company clearly disclose what kinds of steps it will take to address the impact of a data breach on its users?

DRCQ

Digital Rights Rating

Please contact DRCQ experts for a detailed audit and customized recommendations to improve the companies' transparency, raise the high standards of digital rights of users, and increase the loyalty and trust of web services by their users.

Contacts

Email: kz@drc.law

Tel.: +7 775 007 81 99

https://kz.drc.law/

https://digitalrights.kz/