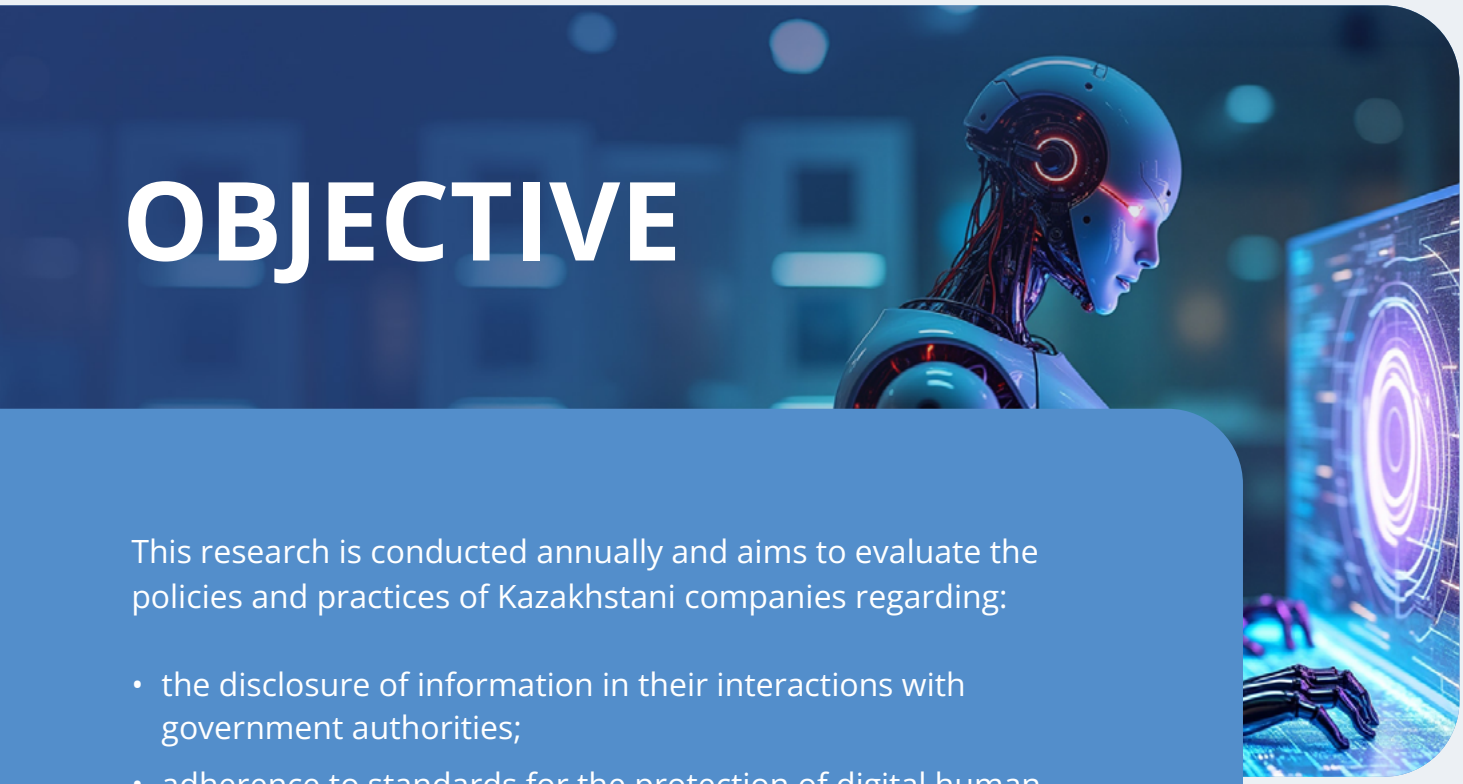
DRCQ

Digital Rights Rating

Digital Rights Compliance Ranking of Companies Developing and Implementing AI Technologies in Kazakhstan

2025

OBJECTIVE



This research is conducted annually and aims to evaluate the policies and practices of Kazakhstani companies regarding:

- the disclosure of information in their interactions with government authorities;
- adherence to standards for the protection of digital human rights;
- efforts to ensure users' rights to freedom of information and privacy;
- transparency in the use of artificial intelligence systems.

This year, the research focused on startups and companies whose operations are based on AI or involve the active use of algorithmic systems

RESEARCH PREPARED BY:

- Ruslan Dayirbekov
- Vadim Melyakov
- Elzhan Kabyshev
- Danila Bekturganov
- Diana Nurgaziyeva

RESEARCH ADVISOR:

Leandro Ucciferri,
World Benchmarking Alliance – Engagement Lead for Ranking Digital Rights (RDR)

CONTENTS

ABOUT US

The 2025 Digital Rights Compliance Ranking was prepared by legal experts from Digital Rights Center Qazaqstan (DRCQ) in collaboration with Ranking Digital Rights (RDR) and the World Benchmarking Alliance.

This research project was initiated by DRCQ to conduct an independent assessment of the public policies and practices of digital platforms in Kazakhstan. The study focuses on the disclosure of information in the context of interactions with government authorities, compliance with digital consumer human rights standards, and measures taken to ensure users' rights to freedom of information, privacy, and transparency in the use of artificial intelligence systems.

The 2025 research concentrates on Kazakhstani companies and startups involved in the development and application of AI technologies. This focus is due to the fact that AI has become a key driver of digital transformation in the country, affecting everyday life, public processes, access to information, and personal data security.

Moreover, on November 17, 2025, the Head of State signed the Law of the Republic of Kazakhstan "On Artificial Intelligence," which establishes fundamental principles for the functioning of AI systems and imposes new human rights obligations on owners, operators, and users of AI products, including ensuring transparency of algorithmic systems. Companies developing and implementing AI solutions must recognize their increased responsibility for algorithmic transparency, non-discrimination, and safeguarding users' privacy.

Upholding and protecting human rights is a competitive advantage and should be prioritized in line with the highest standards of the UN Guiding Principles on Business and Human Rights.

The companies selected for this research were chosen based on our four-stage methodology, which is detailed in the corresponding section of this report.

The DRCQ team consists of professional lawyers in cyber law (IT & IP Law), attorneys, telecom and communications experts, media lawyers, fintech and e-commerce lawyers, as well as technical specialists and financial analysts, covering a wide range of client needs.

"In 2025, we are evaluating, for the first time, companies that develop and implement AI-based solutions. For these companies, technological transparency and respect for human rights are not just elements of good practice—they are indicators of maturity and readiness to operate in the new digital reality. This is especially important in light of the Law on Artificial Intelligence adopted in Kazakhstan this year, which introduces new requirements for transparency, risk management, and accountability for AI developers and providers.

The ranking helps companies identify their strengths and areas for improvement, build sustainable compliance processes, meet the requirements of the new digital AI legislation, and strengthen user trust. Those who invest in these approaches today create a competitive advantage and set the standards for the development of responsible AI in Kazakhstan."

— **Ruslan Dayirbekov**, Director of DRCQ Law Firm

METHODOLOGY FOR SELECTING COMPANIES FOR THE "DIGITAL RIGHTS COMPLIANCE RANKING 2025"

The selection methodology is based on principles of transparency and aligns with the high international standards established in the Ranking Digital Rights methodology.

Our goal is to ensure that each company understands the criteria and selection process, can trust our assessment, and can subsequently improve its own transparency and strengthen trust among users and clients.

STAGE 1.

OPEN ONLINE VOTING AMONG SOCIAL MEDIA FOLLOWERS

In June, an online vote was conducted among followers of our official social media pages (Instagram, Telegram, Facebook, and LinkedIn). Participants selected from a range of public Kazakhstani AI startups and companies. Followers could also suggest additional companies and share their opinions in the comments.

STAGE 2.

VOTING AMONG PARTICIPANTS OF RELEVANT EVENTS VIA EMAIL SURVEY

An online survey was also carried out among an audience actively interested in digital rights and internet regulation, reached through participation in major events and forums such as Privacy Day and Qazaqstan IGF. This audience included representatives from various stakeholders, including businesses, academia, civil society, and government bodies.

STAGE 3.

FORMATION OF A POOL OF INDEPENDENT KAZAKHSTANI EXPERTS FOR SURVEY VOTING

To ensure professional competence in the company selection process, DRCQ established a pool of independent Kazakhstani experts. This pool includes public figures with significant contributions to the development of the business community, entrepreneurship, and the promotion of digital rights in Kazakhstan.

EXPERT "SURVEY":

Based on the results of the previous online voting stages, a survey was created and sent to the independent experts.

In the survey, leading professionals in the digital industry evaluated each company using a scoring system:

1 point — I do not believe this company should be included in the Ranking

2 points — Probably not

3 points — Some doubts, but the company could be considered

4 points — The company is suitable for consideration in the Ranking, though other options not on the list may also be considered

5 points — This company should definitely be included in the 2025 Ranking

Independent experts could also suggest additional companies through the survey form.

STAGE 4.

ANALYSIS OF RESULTS AND START OF WORK

After analyzing the final survey results, the following AI companies received the highest scores in the voting process:

- **CEREBRA AI**
- **FLOWSELL ME**
- **HR MESSENGER**
- **PRESIGHT AI KAZAKHSTAN**
- **PLEEP APP**
- **RE: CREATE AI**
- **VERIGRAM AI**

INFORMATION ON SELECTED COMPANIES

In 2025, Kazakhstan is experiencing a rapid “AI boom.” Private companies are increasingly integrating commercially available artificial intelligence systems into their business processes, and some are even developing their own. Government bodies are also actively implementing digital algorithms in public services and administrative processes. Companies and startups that develop and deploy AI solutions are becoming key intermediaries between technology and citizens, shaping how digital rights are realized or restricted in practice.

The renaming of the Ministry of Digital Development, Innovations, and Aerospace Industry (MDDIAI) to the Ministry of Artificial Intelligence and Digital Development of the Republic of Kazakhstan serves as both a symbolic and practical acknowledgment of AI’s priority at the state level. In the context of technology institutionalization, it is the business sector—from large companies to young startups—that gains unique opportunities and, simultaneously, the responsibility to establish standards of transparency and accountability.

At the same time, risks related to algorithmic opacity and the automated collection of sensitive data, including biometric and behavioral profiles, are increasing. Startups and companies pursuing rapid growth often bypass independent audits and public oversight, creating conditions for discrimination and violations of consumer rights.

Therefore, transparency and accountability of AI companies and startups have become critically important for protecting citizens’ fundamental digital rights. This is especially significant given the new requirements of the Law on Artificial Intelligence in Kazakhstan, which apply to operators, owners, and users of AI systems.

CEREBRA AI

Cerebra AI — a Kazakhstani AI project created by Almaty A.I. Lab, which has been developing machine learning and computer vision technologies since 2018. Cerebra AI's solutions are applied in medicine for the automatic analysis of brain CT scans, helping doctors detect strokes and traumatic brain injuries faster, reducing diagnosis time and improving accuracy.

FLOWSELL.ME

Flowsell.me — a Kazakhstani IT startup developing solutions for automating customer interactions in the service sector. The platform helps businesses retain and recover clients through mass messaging, notifications, appointment confirmations, and feedback collection via messengers, enhancing communication efficiency and sales.

HR MESSENGER

HR Messenger — a Kazakhstani startup that created a chatbot service to automate HR processes, including recruitment, employee onboarding, and internal communications. The company aims to optimize HR department operations, reduce recruiter workload, and strengthen the HR brand by handling routine tasks and providing analytics on employee engagement.

PRESIGHT AI

Presight AI — a UAE-based company specializing in big data analytics and AI-driven solutions. In 2025, Presight AI opened a regional office in Astana, becoming part of Kazakhstan's digital transformation initiatives. The company is part of the G42 group and develops smart city technologies, including the Intelli City system. In Kazakhstan, Presight AI participates in modernizing the city surveillance system, replacing the existing "Sergek" platform.

PLEEP APP

Pleep App — a Kazakhstani startup that developed an intelligent chatbot for automating sales and customer communication. Unlike standard bots, Pleep mimics human interaction, responds instantly to inquiries, and can conduct phone dialogues. The solution operates 24/7 and aims to increase conversion rates through personalized responses, objection handling, and sequential follow-up communications.

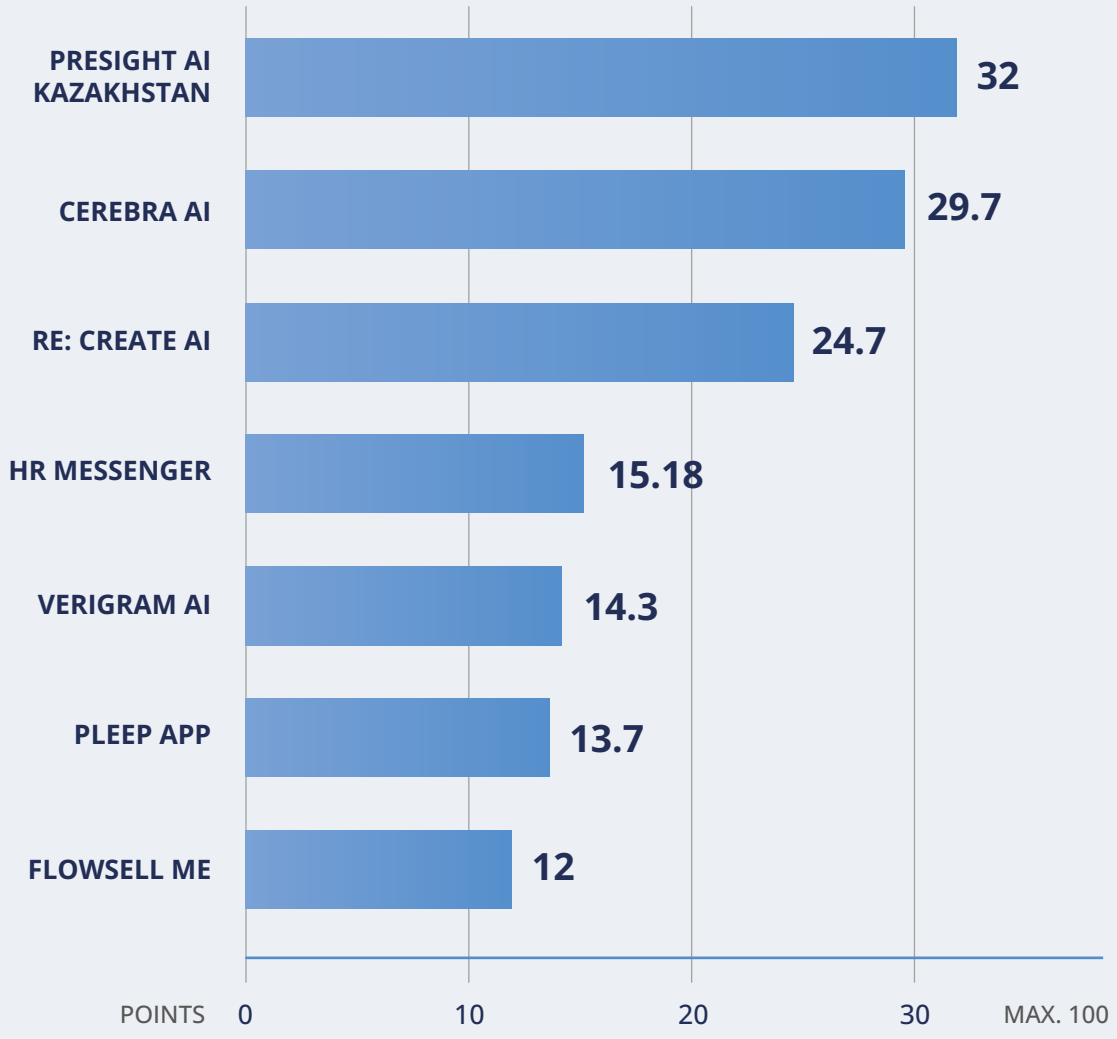
RE:CREATE AI

RE:CREATE AI — a Kazakhstani startup and graduate of the first AI'preneurs accelerator cohort at Astana Hub. The project offers a search engine for trends and content scenarios on Instagram, TikTok, and YouTube, helping experts, entrepreneurs, and small businesses discover and adapt viral content formats for their own promotion based on reach and engagement data.

VERIGRAM AI

Verigram AI — a Kazakhstani company founded in 2017, developing AI, computer vision, and machine learning technologies. The company provides services for document, facial, and object recognition, as well as intelligent video analytics systems. It also implements OCR and biometric technologies to improve customer service quality and prevent fraud.

TOTAL SCORE OF THE COMPANIES



METHODOLOGY

To assess the public positions and policies of companies regarding the protection of digital human rights, we used the official websites and web resources of the companies and their parent groups. All publicly available company documents were collected and archived for the period from July to September 2025 and were reviewed as part of the research project until the end of September 2025.

The indicators used to evaluate companies are based on the 2020 Ranking Digital Rights corporate reporting methodology. Detailed descriptions of the indicators and sub-indicators are available on our website on the Methodology page, as well as in Annex 1 of this report.

The research questions were grouped under three main indicators.

“G. CORPORATE GOVERNANCE”

Indicators in this category are designed to demonstrate the presence of clearly defined governance processes within a company that ensure respect for human rights, including freedom of expression and privacy. To achieve high scores in this category, the company’s publicly disclosed information should at a minimum reflect—and ideally exceed—the UN Guiding Principles on Business and Human Rights and other human rights standards aimed at protecting freedom of expression and privacy, as established by the Global Network Initiative (GNI).

Additionally, to score highly, a company should demonstrate that it conducts regular independent audits, provides employee training programs on data protection, and engages in consultations with relevant stakeholders. For companies implementing artificial intelligence technologies, Category G further assesses the extent of their responsibility in the development and use of algorithmic systems. Specifically, it examines whether the company has clear and publicly stated commitments to uphold human rights in its AI activities, and whether the organization’s leadership conducts impact assessments of algorithms concerning non-discrimination and user privacy.

G–INDICATORS

CORPORATE GOVERNANCE

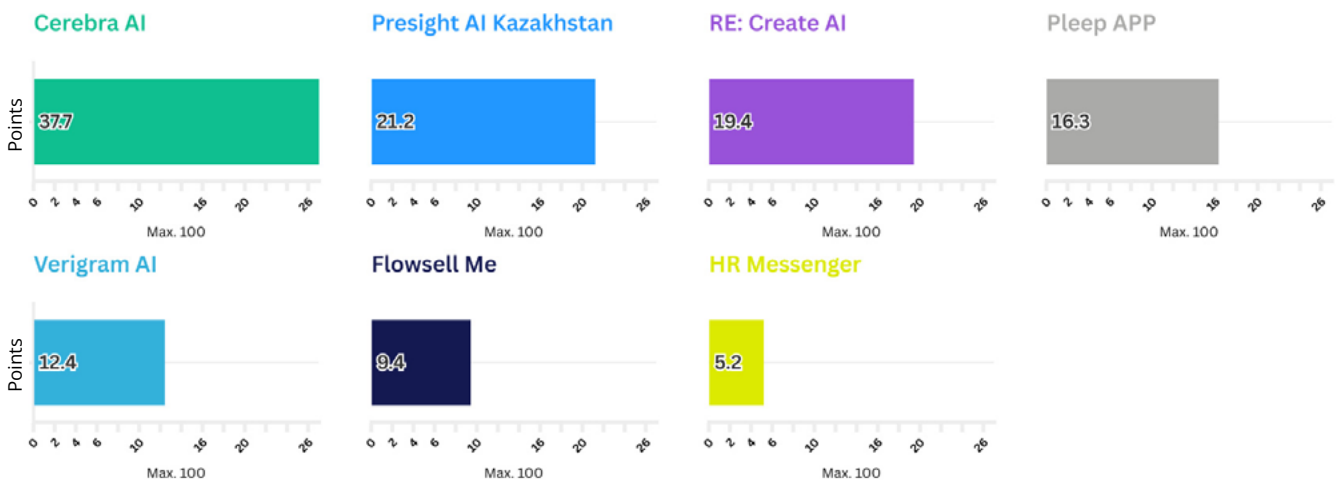
“F. FREEDOM OF EXPRESSION AND INFORMATION”

The points earned in this category indicate that the company has demonstrated a respectful approach to the rights to freedom of expression and information in accordance with international human rights standards. The company’s published policies clearly outline the measures taken to prevent human rights violations, except in cases where such actions are lawful, proportionate, and pursue a legitimate aim. AI technologies, which are increasingly used in the operations of private companies, are inherently prone to discriminatory outcomes or information distortion, as they are trained on datasets that reflect existing societal biases and inequalities.

As a result, the outputs of AI systems—such as hiring or content-moderation algorithms, credit-scoring tools, or facial-recognition technologies—may be unfair, discriminatory, or inaccurate for certain groups of people, thereby undermining the right to equality and access to reliable information. Moreover, AI models often generate information that sounds credible but is in fact false or fabricated, creating additional risks of user misinformation.

F–INDICATORS

FREEDOM OF EXPRESSION AND INFORMATION



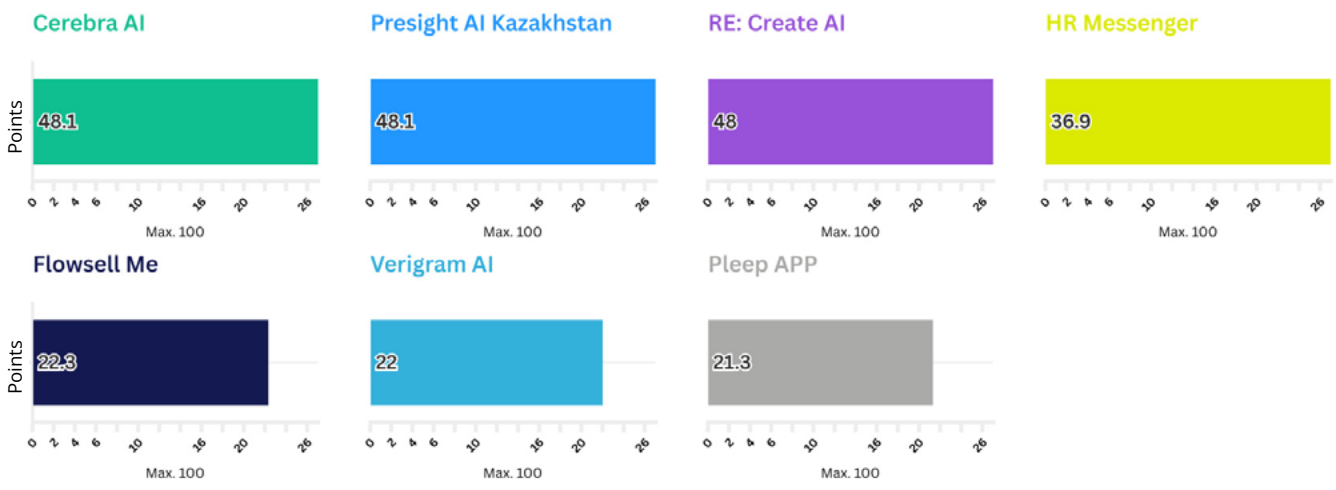
“P. PRIVACY”

The indicators in this category reflect the extent to which companies demonstrate their commitment to users’ rights to privacy and digital security in accordance with international human rights standards. They show how transparent companies are in their policies on the processing of personal data—including its collection, use, storage, and transfer to third parties—as well as how effectively they ensure users’ information security.

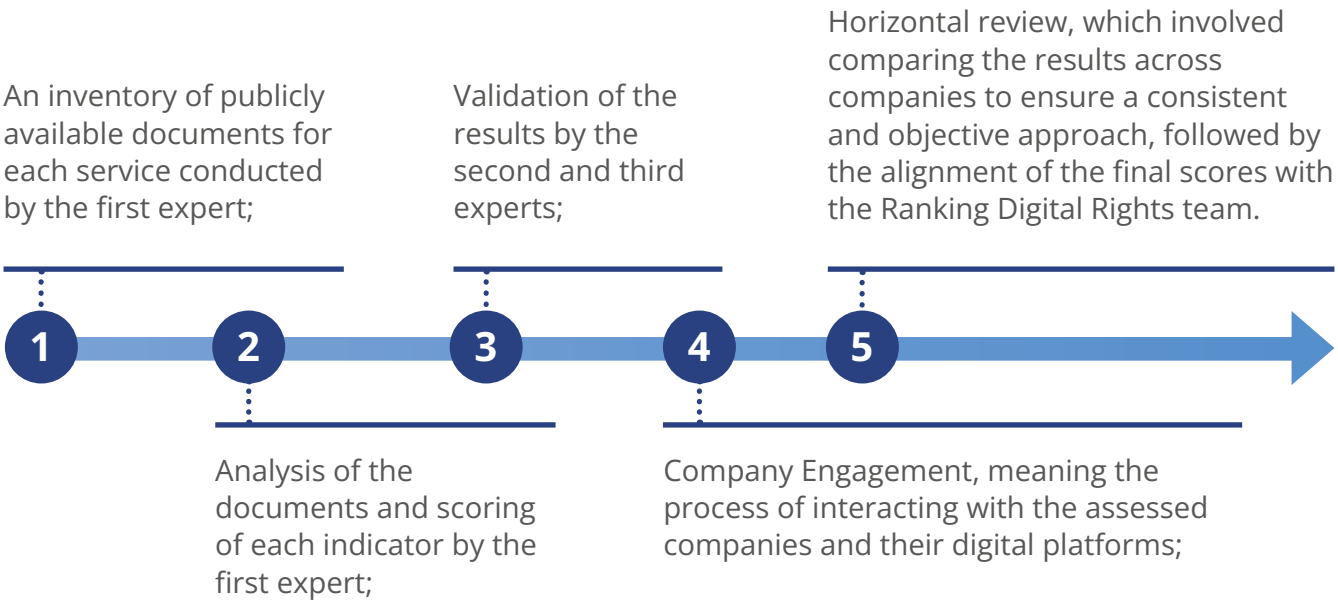
Additionally, the assessment considers whether companies take measures to minimize the risk of data breaches, whether they provide users with opportunities to control their own information, whether they clearly explain their privacy-protection mechanisms, and whether they conduct cybersecurity training for employees. The development and deployment of artificial intelligence systems involve significant risks to customer privacy, as these technologies often rely on large-scale collection and analysis of personal data. As a result, companies risk violating fundamental privacy principles such as purpose limitation in data collection and the requirement for user consent.

P–INDICATORS

PRIVACY



The research process consisted of the following stages:



Each indicator includes a set of parameters, and companies receive a score (full, partial, or zero) for each parameter they meet. The assessment reflects the extent to which the company discloses information for each parameter, based on one of the following possible responses:

- **"Yes"** (full disclosure): The company's disclosure fully meets the requirement of the indicator.
- **"Partial"**: The company has disclosed some, but not all, aspects of the indicator, or the disclosure is not sufficiently detailed to meet all requirements.
- **"No disclosure found"**: Researchers were unable to locate information on the company's website that addresses the element in question.
- **"No"**: Relevant information exists, but it does not address the specific parameter being evaluated. This option differs from "No disclosure found," although both do not result in a positive score.
- **"Not applicable"**: The element does not apply to the company or the service. Elements marked as "Not applicable" are excluded from the scoring process and do not count for or against the final score

SCORES

- Yes / full disclosure = **100**
- Partial disclosure = **50**
- Information not disclosed = **0**
- No disclosure found = **0**
- Not applicable – this element is excluded from both the scoring and the calculation of average values.

KEY FINDINGS

1. Most companies do not articulate clear public commitments to respecting human rights, including in the development and use of algorithmic systems. The only exception is Presight AI, which does declare in its public annual report its commitment to the ethical use of artificial intelligence and the implementation of privacy-management standards such as ISO 27701:2019; however, these commitments are not reflected in its core policies

2. Almost all companies publicly disclose policies regulating their interaction with users and content on their websites. The exception is HR Messenger, which publishes only a privacy policy.

3. The mechanisms for updating policies or the procedures for notifying users of upcoming or implemented changes are insufficiently disclosed. None of the reviewed companies maintains a public archive of previous versions of policies or a changelog documenting amendments.

4. Standalone policies governing the use of algorithmic systems are absent across all companies. However, it is worth noting that Cerebra AI includes a subsection titled “Use of Artificial Intelligence (AI) and Liability Provisions” within its Terms of Use, which partially describes the use of AI and algorithms for service provision and other purposes. Pleep App also outlines procedures for the use of its AI assistant in its Public Offer.

5. Although all companies operate or provide services in Kazakhstan, a significant portion of their official documents is available only in Russian or English, without an option to access them in the state language.

6. All companies ensure basic accessibility of their privacy policies. Moreover, each of the reviewed companies scored the highest in the indicators under the Privacy section.

7. It is worth noting separately that the privacy policies of most of the companies reviewed are described in sufficient detail and written in clear, understandable language.

8. Cerebra AI, Presight AI, and HR Messenger present the purposes, categories, and methods of processing users' personal data in structured table formats, which align with high international standards. Cerebra AI and Verigram AI explicitly note in their documents that their privacy policies incorporate the requirements of the European General Data Protection Regulation (GDPR). The privacy policy of the RE:Create AI startup is also highly detailed and discloses many aspects required by the RDR methodology.

9. All policies mention the possibility of transferring personal data to third parties, but most do not disclose the specific list of partners. Only HR Messenger explicitly identifies the business partners with whom the company shares user data.

10. Only RE:Create AI and Presight AI indicate that they exercise due diligence when transferring personal data to third parties. These companies are also the only ones that explicitly state that, in the event of a personal data breach, they will notify the competent authority within 72 hours.

11. The startup Cerebra AI claims compliance with the international medical standard HIPAA, which, among other requirements, obliges organizations to notify users in case of a breach of their medical data privacy. However, the startup's website does not provide a description of the specific provisions or rules of this standard.

12. It was found that publicly available company documentation does not provide detailed and transparent information on how they respond to requests from government authorities (judicial and non-judicial) or private third parties, including the media, regarding account restrictions or the provision of personal data. Despite statements about data sharing "in accordance with the law," there are no clear indications of which data is shared or whether users are informed about such transfers.

13. None of the companies publish a transparency report regarding data privacy.

14. Information on data obtained automatically through big data inference or algorithmic predictions is presented only partially. For example, Flowsell.me, Presight AI, Cerebra AI, and HR Messenger describe the use of automatically collected data for personalizing user experiences and marketing purposes.

15. Verigram AI and Presight AI stand out by clearly stating that only authorized personnel have access to users' personal information, and that compliance with security protocols is ensured through disciplinary and organizational measures. The other reviewed companies provide only general statements about implementing cybersecurity measures.

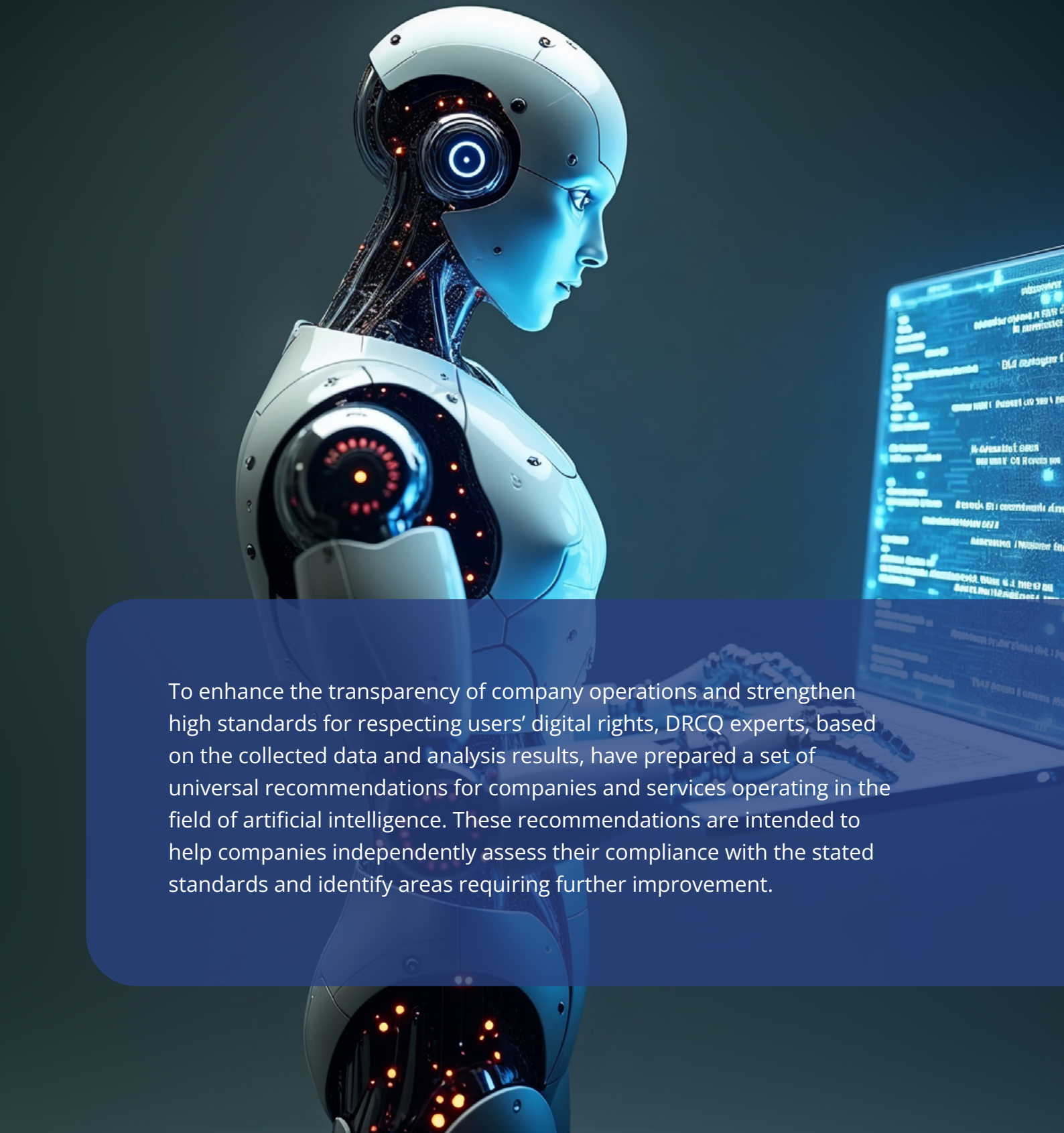
16. It should be noted that Presight AI is the only company that provides clear information on the mechanism for submitting complaints regarding violations of user privacy. One of its policy sources includes a separate section, "Filing a Complaint", which describes the procedure for submitting a complaint and provides contact details.

17. Cerebra AI, Presight AI, and RE:Create AI are the top three companies in terms of points scored in the Privacy category.

18. Since most of the reviewed companies are relatively new and essentially startups, almost all scored very low in the Corporate Governance category.

19. In the Freedom of Expression and Information category, the same three companies that scored highest in Privacy also received high scores.

RECOMMENDATIONS



To enhance the transparency of company operations and strengthen high standards for respecting users' digital rights, DRCQ experts, based on the collected data and analysis results, have prepared a set of universal recommendations for companies and services operating in the field of artificial intelligence. These recommendations are intended to help companies independently assess their compliance with the stated standards and identify areas requiring further improvement.

FREEDOM OF EXPRESSION AND INFORMATION

1. Clearly and transparently state in public policies the company's commitments to respecting human rights and protecting users' rights to freedom of expression and access to information. It is recommended to refer to international standards, including: the Universal Declaration of Human Rights; the International Covenant on Civil and Political Rights; and the UN Guiding Principles on Business and Human Rights.

2. Companies should openly inform users when they receive requests from government authorities to remove content, suspend user accounts, or restrict access to information. It is important to explain how such requests are assessed by the company (including senior management) for legality, proportionality, and legitimacy, as well as the company's policy on complying with such requests.

3. Clearly define procedures for submitting user complaints and implement mechanisms that allow users to file complaints and challenge decisions regarding content restrictions or account suspensions. These mechanisms should be understandable, accessible, and designed to ensure fair and timely resolution of issues.

4. Conduct regular risk assessments with the involvement of independent auditors to evaluate compliance with digital and consumer human rights.

5. Ensure transparency of content moderation policies and the use of algorithmic systems for evaluating content or user behavior. Companies should publish detailed algorithm-use policies, including measures to guarantee non-discriminatory and fair access to content for users.

6. All public company documents should be published in the languages of the markets where services are offered (i.e., at minimum, in Kazakh and Russian).

7. When making any changes to policies, it is important to directly notify all users of the updates via email or a notification in their personal account.

CORPORATE GOVERNANCE

1. Senior management should regularly oversee how the company's policies and practices impact freedom of expression and information, as well as privacy.
2. Clearly designate, at the senior management level, an individual or committee responsible for oversight and reporting on digital consumer rights and their compliance.
3. Adopt a strategic policy that requires adherence to the principle of "Privacy by Design" when developing new company products or services.
4. Implement systematic training programs aimed at increasing staff awareness of user rights, personal data protection, and the ethical use of artificial intelligence. This will help raise awareness and strengthen internal processes for human rights compliance. Employees should also be informed about who to contact and the procedures to follow if their own rights are violated.
5. For companies using artificial intelligence technologies, it is important to establish mechanisms for risk assessment, monitoring, and accountability in the development and use of AI systems.

PRIVACY

1. Provide users with easily accessible and effective tools to control the collection, use, and transfer of their personal data, in accordance with local legislation and the international GDPR standard (such tools may include user controls for deletion, correction, access to data, etc.).
2. Ensure that users can control the use of their data for targeted advertising. Users should also be able to easily opt out of targeted advertising or limit data collection for these purposes.

3. Publicly disclose in the privacy policy the names of third-party legal entities (including advertising partners and subcontractors) to which users' personal data is or may be transferred.
4. Regularly publish a Transparency Report regarding data privacy on company platforms. This report should detail how the company responds to requests from government authorities, law enforcement agencies, or other parties. Typically, the report should include:
    a. How many times government authorities requested user data.
    b. What data was requested (e.g., contact information, messages, IP addresses).
    c. How many requests the company approved or rejected, and why.
    d. How often the company deletes or restricts content, for example, in response to government requests.
5. Clearly indicate whether user data is collected for machine learning and subsequent use in algorithmic systems, including AI assistants, chatbots, etc. It is important to disclose: the purposes of using data in these processes; potential impacts on users (e.g., personalization, automated decisions); and measures to prevent discrimination and bias.
6. Provide detailed information on data deletion procedures and retention periods, including deletion upon user request or once the purpose of data collection is achieved.
7. Immediately notify users in the event of a data breach and promptly inform the competent government authority.
8. Publish (on the website, in the app, and on social media) practical materials that educate users on how to protect themselves from cybersecurity risks associated with the company's products or services.
9. Strive to minimize data collection, limiting it to the information strictly necessary to provide services.
10. Strengthen internal controls over employee access to users' personal data. Implement an internal data management system where access to user information is granted only to authorized personnel.

LEGISLATION

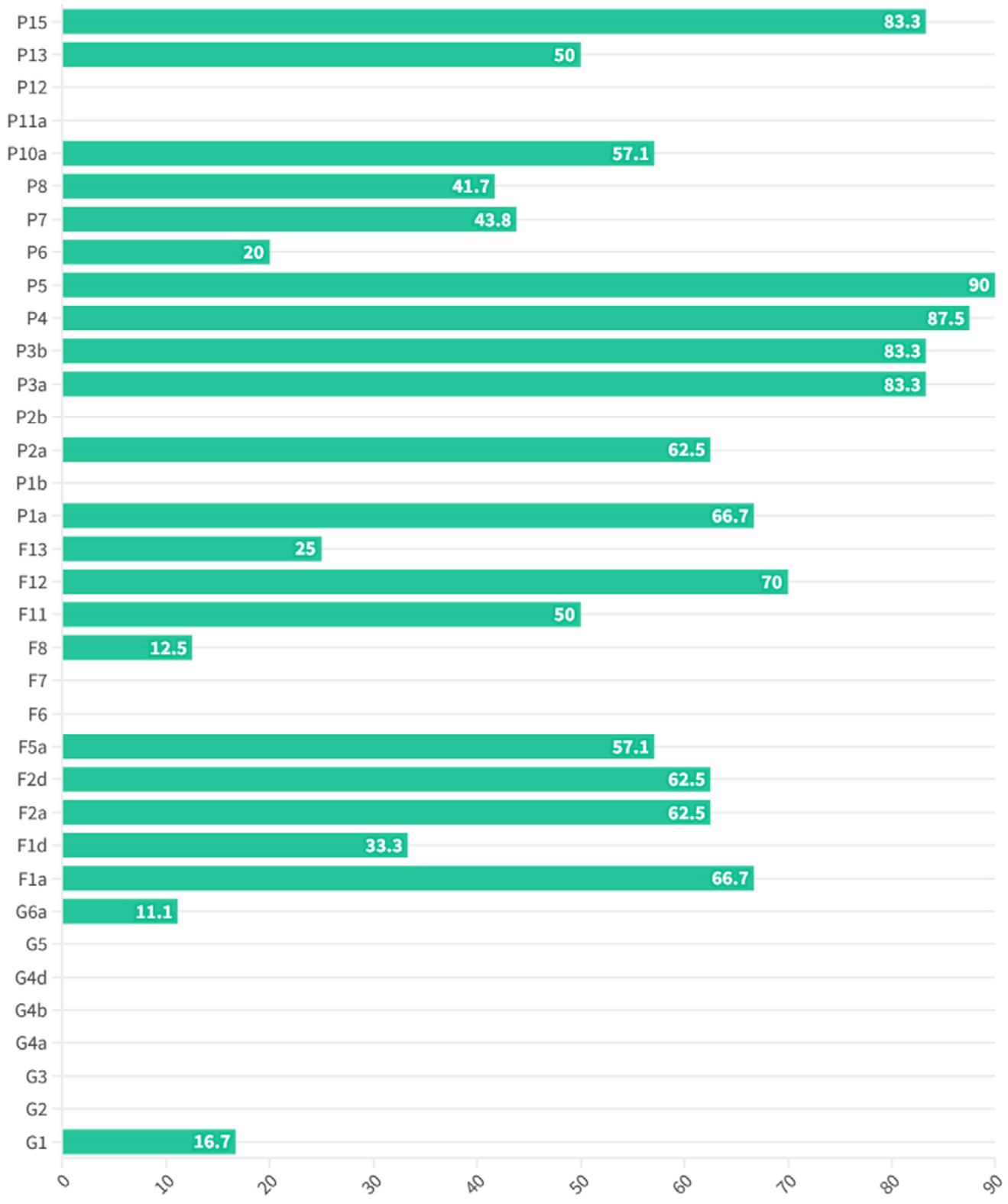
In the work of the project, we were guided by the following normative legal acts:

- UN Guiding Principles on Business and Human Rights
- Universal Declaration of Human Rights
- International Covenant on Civil and Political Rights
- International Covenant on Economic, Social and Cultural Rights
- Entrepreneurship Code of the Republic of Kazakhstan (No. 375-V ZRK, 29 October 2015)
- Law of the Republic of Kazakhstan “On Artificial Intelligence” (No. 230-VIII, 17 November 2025)
- Law of the Republic of Kazakhstan on Amendments and Additions to Certain Legislative Acts concerning Artificial Intelligence and Digitalization (2025)
- Law of the Republic of Kazakhstan “On Personal Data and their Protection” (No. 94-V, 21 May 2013)
- Law of the Republic of Kazakhstan “On Access to Information” (No. 401-V ZRK, 16 November 2015)
- Law of the Republic of Kazakhstan “On Informatization” (No. 418-V ZRK, 24 November 2015)
- Law of the Republic of Kazakhstan “On Communications” (No. 567, 5 July 2004)
- Law of the Republic of Kazakhstan “On Online Platforms and Online Advertising” (No. 18-VIII, 10 July 2023)

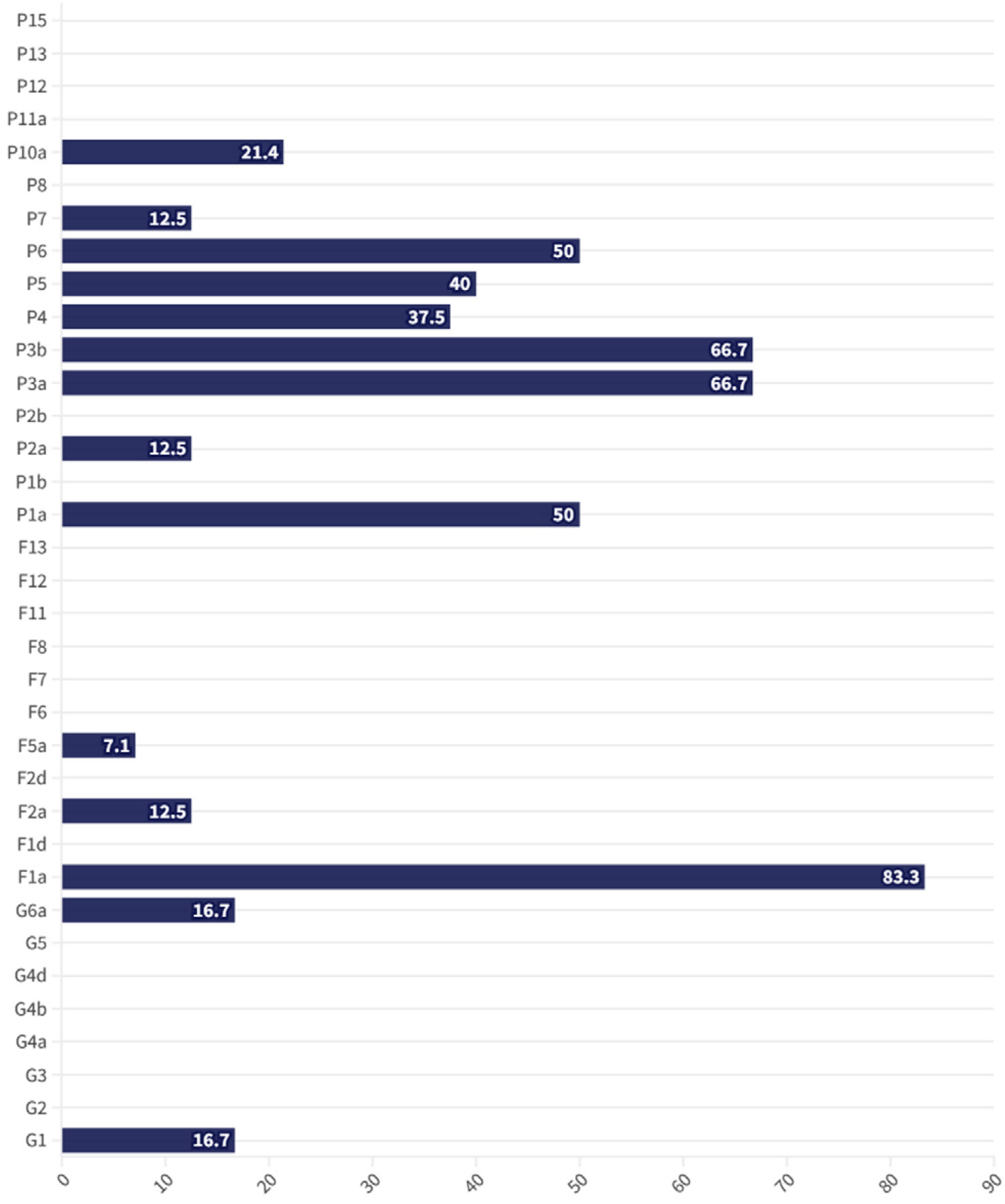
- Order of the Minister of Digital Development, Innovations and Aerospace Industry of the Republic of Kazakhstan No. 114/NQ (2 April 2021) "On Approval of the Rules for Information •Content of Internet Resources of Public Authorities and Requirements for their Content"
- Order of Acting Minister of Digital Development, Innovations and Aerospace Industry of the Republic of Kazakhstan No. 601/NQ (27 September 2024) "On Approval of the Rules for Digital Transformation of Public Administration"
- Resolution of the Government of the Republic of Kazakhstan No. 832 (20 December 2016) "On Approval of Unified Requirements in the Field of Information and Communication Technologies and Information Security"
- Resolution of the Government of the Republic of Kazakhstan No. 592 (24 July 2024) "On Approval of the Concept for the Development of Artificial Intelligence for 2024–2029"
- Resolution of the Mazhilis of the Parliament of the Republic of Kazakhstan No. 794-VIII (24 September 2025) on the Law "On Artificial Intelligence"
- Law of the Republic of Kazakhstan on Amendments and Additions to Certain Legislative Acts on Information and Communications (No. 128-VI, 28 December 2017)
- Law of the Republic of Kazakhstan on Amendments and Additions to Certain Legislative Acts on Innovation Stimulation, Digitalization, Information Security and Education (No. 141-VII, 14 July 2022)
- Law of the Republic of Kazakhstan on Amendments in Connection with the Address of the Head of State (No. 157-VII, 5 November 2022)
- Law of the Republic of Kazakhstan on Amendments and Additions to Certain Legislative Acts on Digital Assets and Informatization (No. 194-VII, 6 February 2023)
- Law of the Republic of Kazakhstan on Amendments and Additions Regarding Defense, Aerospace Industry and Information Security (No. 237-VI, 18 March 2019)

ANNEX 1

CEREBRA AI. RDR INDICATORS

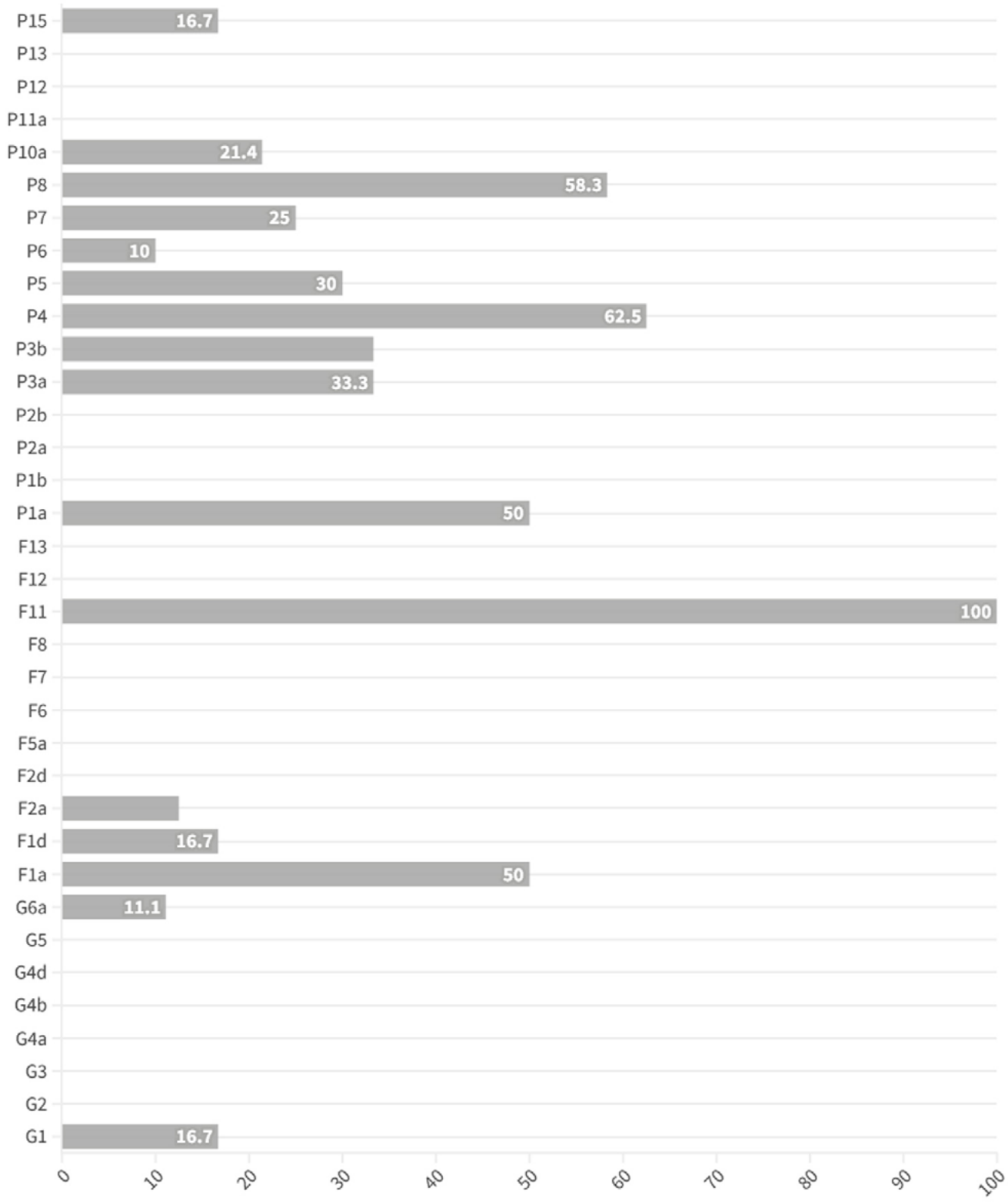


FLOWSELL ME. RDR INDICATORS

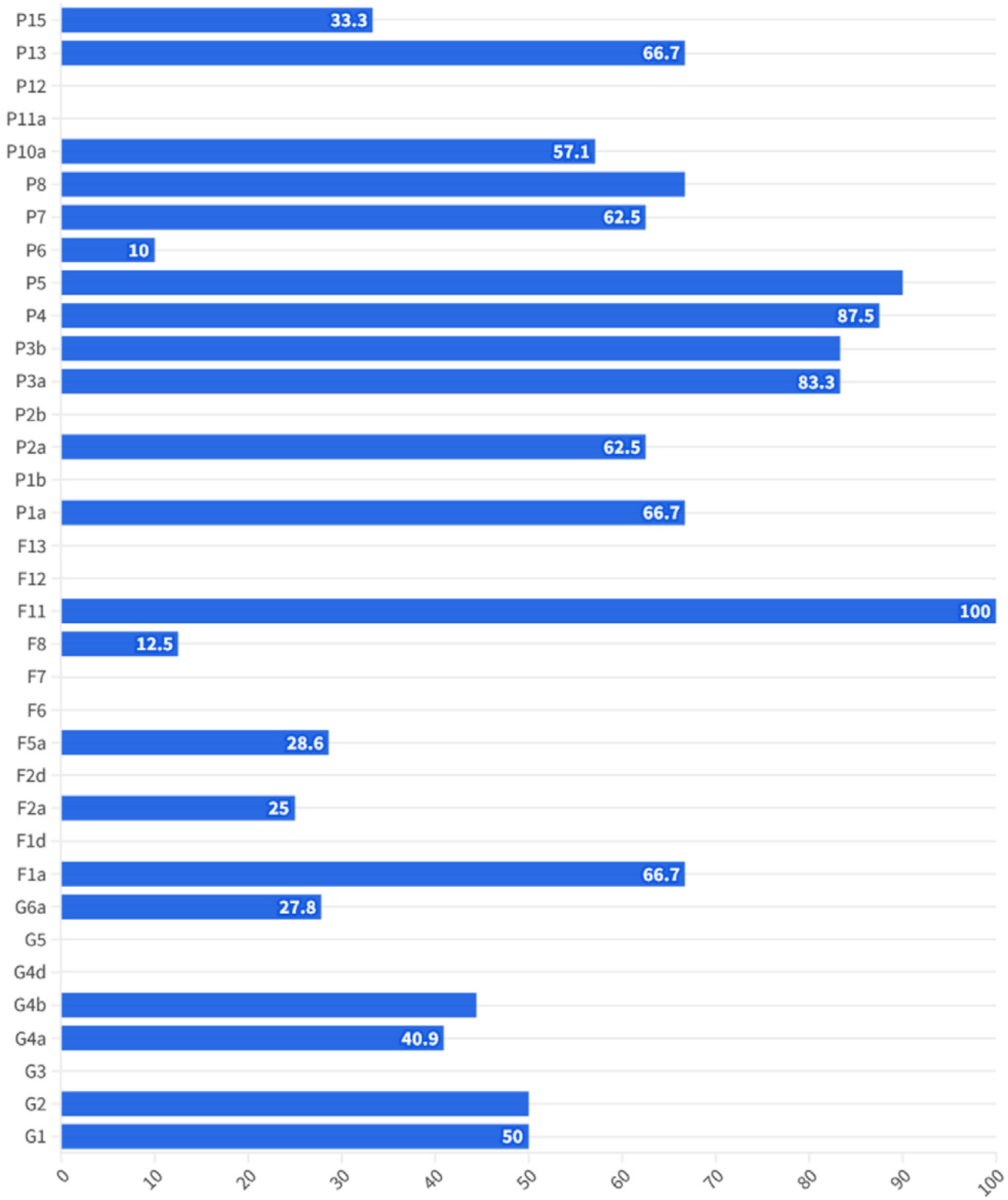


HR MESSENGER. RDR INDICATORS

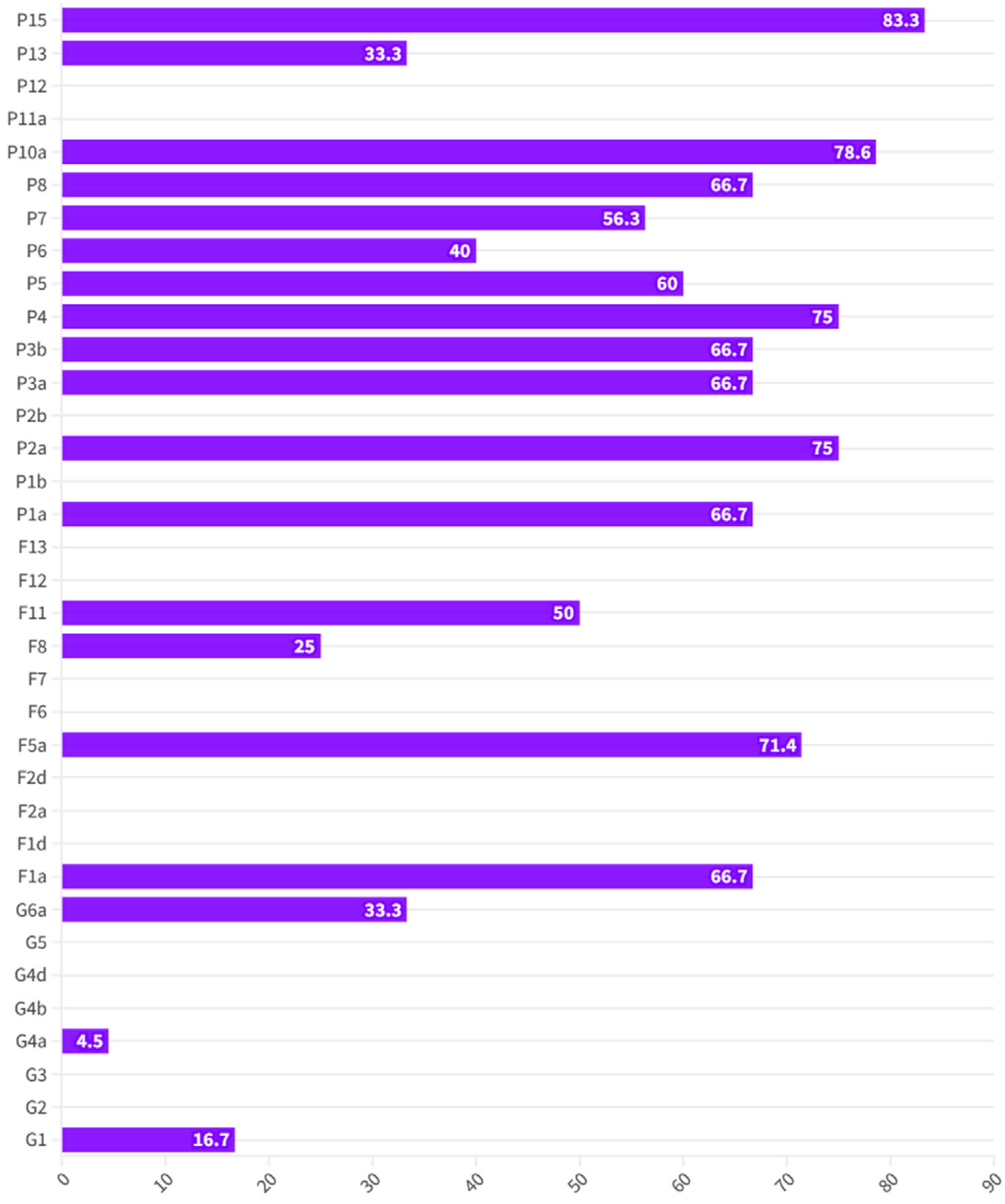
PLEEP APP. RDR INDICATORS



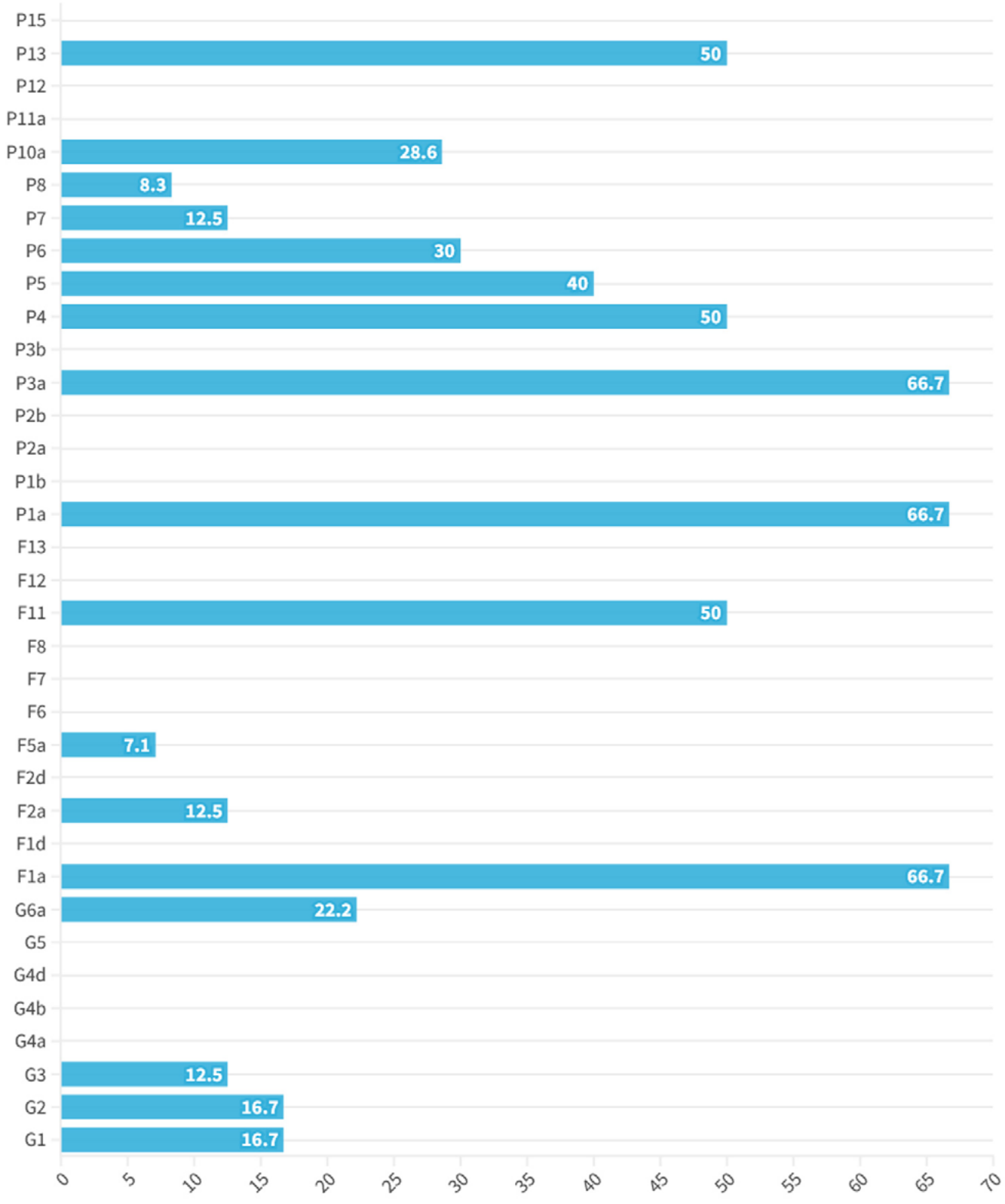
PRESIGHT AI KAZAKHSTAN. RDR INDICATORS



RE:CREATE AI. RDR INDICATORS



VERIGRAM AI. RDR INDICATORS



G1. COMMITMENT POLICY

PARAMETERS:

1. Does the company adopt clear, publicly stated commitments to respect human rights, including the right to freedom of expression and access to information?
2. Does the company adopt clear, publicly stated commitments to respect human rights, including the right to privacy?
3. Does the company adopt clear, publicly stated commitments to respect human rights in the development of algorithmic systems?

G2. MANAGEMENT OVERSIGHT AND SUPERVISION

PARAMETERS:

1. Does the company provide clear information that the Board of Directors exercises formal oversight over how the company's activities affect freedom of expression and access to information?
2. Does the company provide clear information that the Board of Directors exercises formal oversight over how the company's activities affect privacy?
3. Does the company provide clear information that the company's activities affecting freedom of expression and access to information are overseen by an executive committee, a designated team, a targeted program, or a senior-level responsible officer?
4. Does the company provide clear information that the company's activities affecting privacy are overseen by an executive committee, a designated team, a targeted program, or a senior-level responsible officer?
5. Does the company provide clear information that the company's activities affecting freedom of expression and access to information are overseen by an executive committee, a designated team, a targeted program, or a responsible officer from management-level staff?

6. Does the company provide clear information that the company's activities affecting privacy are overseen by an executive committee, a designated team, a targeted program, or a responsible officer from management-level staff?

G3. APPLICATION IN INTERNAL POLICY

PARAMETERS:

1. Does the company provide clear information about employee training on freedom of expression and access to information?
2. Does the company provide clear information about employee training on privacy?
3. Does the company provide clear information about whistleblower programs and mechanisms through which employees can report issues related to how the company respects users' freedom of expression and informational rights?
4. Does the company provide clear information about whistleblower programs and mechanisms through which employees can report issues related to how the company respects users' right to privacy?

G4(A). IMPACT ASSESSMENT: GOVERNMENT AUTHORITIES AND REGULATIONS

PARAMETERS:

1. Does the company assess how local laws affect the protection of freedom of expression and information in the jurisdictions where it operates?
2. Does the company assess how local laws affect privacy protection in the jurisdictions where it operates?
3. Does the company assess risks to freedom of expression and information regarding existing products and services in the jurisdictions where it operates?

4. Does the company assess privacy risks regarding existing products and services in the jurisdictions where it operates?
5. Does the company evaluate potential threats to freedom of expression and information arising from new business activities, including the launch or creation of new products, services, or companies, as well as entry into new markets or jurisdictions?
6. Does the company assess privacy risks associated with new business activities, including the launch or creation of new products, services, or companies, as well as entry into new markets or jurisdictions?
7. Does the company conduct additional expert review in cases where risk assessments reveal problematic issues?
8. Do senior executives and/or board members review the results of risk assessments and comprehensive evaluations, and consider them in decision-making?
9. Are such assessments conducted on a regular basis?
10. Are risk assessments performed by an independent third-party organization?
11. Is the independent third-party organization conducting the assessment a reputable entity accredited according to relevant authoritative human rights standards?

G4(B). IMPACT ASSESSMENT: POLICY IMPLEMENTATION PROCESSES

PARAMETERS:

1. Does the company assess risks related to ensuring freedom of expression and access to information when applying its Terms of Service?
2. Does the company assess risks related to ensuring privacy when applying its Terms of Service?
3. Does the company evaluate discriminatory risks associated with its mechanisms for enforcing Terms of Service?
4. Does the company evaluate discriminatory risks associated with its mechanisms for enforcing privacy policies?

5. Does the company carry out additional expert review procedures when risk assessments reveal problematic areas?
6. Do senior management and/or board members review the results of risk assessments and comprehensive evaluations and take them into account in decision-making?
7. Does the company conduct such reviews on a regular basis?
8. Are these reviews conducted by an independent third-party organization?
9. Is the independent third-party organization performing the review a credible entity accredited according to a recognized human rights standard?

G4(D). IMPACT ASSESSMENT: ALGORITHMIC SYSTEMS

PARAMETERS:

1. Does the company assess freedom of expression and information risks related to its policies and activities in the area of algorithmic systems?
2. Does the company assess privacy risks related to its policies and activities in the area of algorithmic systems?
3. Does the company evaluate discriminatory risks related to the development and use of algorithmic systems?
4. Does the company carry out additional expert review procedures when risk assessments reveal problematic areas?
5. Do senior management and/or board members review the results of assessments and comprehensive evaluations and take them into account in decision-making?
6. Does the company conduct such reviews on a regular basis?
7. Are these reviews conducted by an independent third-party organization?
8. Is the independent third-party organization performing the review a credible entity accredited according to a recognized human rights standard?

G5. STAKEHOLDER ENGAGEMENT AND ACCOUNTABILITY

PARAMETERS:

1. Is the company a member of one or more multistakeholder initiatives aimed at examining ways in which company activities may affect users' fundamental rights, including freedom of expression and information, privacy, and non-discrimination?
2. If the company is not a member of any such multistakeholder initiatives, is it a member of any organizations that systematically and continuously engage with non-industry and non-government stakeholders on freedom of expression and privacy issues?
3. If the company is not a participant in any such organizations, does it provide information on organizing or participating in meetings with stakeholders, human rights defenders, or directly affected individuals whose rights to freedom of expression, information, and privacy are directly related to the company's activities?

G6(A). LEGAL REMEDIES

PARAMETERS:

1. Does the company provide clear information on the existence of complaint mechanisms allowing users to submit complaints if they believe company policy or practice has negatively affected their freedom of expression and information rights?
2. Does the company provide clear information on the existence of complaint mechanisms allowing users to submit complaints if they believe company policy or practice has negatively affected their privacy?
3. Does the company provide clear information on the procedures for remedies in case of complaints related to freedom of expression and information?
4. Does the company provide clear information on the procedures for remedies in case of privacy-related complaints?

5. Does the company provide clear information on the timeframes for complaint handling and the procedures for legal remedies?
6. Does the company provide clear information on the number of complaints received related to freedom of expression?
7. Does the company provide clear information on the number of complaints received related to privacy?
8. Does the company provide clear information on the provision of remedies for complaints related to freedom of expression?
9. Does the company provide clear information on the provision of remedies for complaints related to privacy violations?

F1(A). ACCESS TO TERMS OF SERVICE

PARAMETERS:

1. Is it easy to find the company's Terms of Service?
2. Are the Terms of Service available in the primary language(s) spoken by users in the jurisdictions where the company operates?
3. Are the Terms of Service presented in a clear and understandable manner?

F1(D). ACCESS TO ALGORITHMIC SYSTEMS POLICY

PARAMETERS:

1. Is it easy to find the company's policy on the use of algorithmic systems?
2. Is the policy on algorithmic systems available in the primary language(s) spoken by users in the jurisdictions where the company operates?
3. Is the policy on algorithmic systems presented in a clear and understandable manner?

F2(A). CHANGES TO TERMS OF SERVICE

PARAMETERS:

1. Does the company provide clear information that it directly notifies users of all changes to its Terms of Service?
2. Does the company clearly explain the method it uses to directly notify users of changes?
3. Does the company clearly indicate the timeframe within which it notifies users of changes before they take effect?
4. Does the company maintain a public archive or log of changes made?

F2(D). CHANGES TO ALGORITHMIC SYSTEMS POLICY

PARAMETERS:

1. Does the company provide clear information that it directly notifies users of changes to its algorithmic systems policy?
2. Does the company clearly explain the method it uses to directly notify users of these changes?
3. Does the company disclose the timeframe in which users are notified of changes before they take effect?
4. Does the company maintain a public archive or log of changes made?

F5(A). PROCESS FOR RESPONDING TO GOVERNMENT REQUESTS

PARAMETERS:

1. Does the company provide accessible information about its process for responding to non-judicial government requests?
2. Does the company provide accessible information about its process for responding to court orders?
3. Does the company provide accessible information about its process for responding to requests from foreign government authorities?
4. Does the company clearly explain the legal basis on which it may comply with government requests?
5. Does the company clearly explain that it exercises due diligence before responding to government requests?
6. Does the company commit to resisting unlawful or excessively broad government requests?
7. Does the company provide accessible guidance or examples of how its process for responding to government requests is implemented?

F6. DATA ON GOVERNMENT REQUESTS TO RESTRICT CONTENT OR ACCOUNTS

PARAMETERS:

1. Does the company provide data on the number of such requests received, broken down by country?
2. Does the company provide data on the number of accounts affected by such requests?
3. Does the company indicate the number of content items or URLs affected?
4. Does the company provide a list of categories/topics related to the received requests?
5. Does the company indicate the total number of requests coming from various official authorities?
6. Does the company indicate the number of content or account restriction requests received from officials via informal channels?
7. Does the company indicate the number of requests it has fulfilled?
8. Does the company disclose information about the original requests or inform about providing corresponding copies to a third-party public archive?
9. Does the company publish this data at least once a year?
10. Can this data be exported in a structured file format?

F7. DATA ON PRIVATE REQUESTS TO RESTRICT CONTENT OR ACCOUNTS

PARAMETERS:

1. Does the company provide data on the number of private requests received to restrict content or accounts?
2. Does the company provide data on the number of accounts affected by such requests?

3. Does the company indicate the number of content items or URLs affected by such requests?
4. Does the company provide data on the reasons for content removal related to these requests?
5. Does the company provide accessible information on the private requests received?
6. Does the company indicate the number of requests it has fulfilled?
7. Does the company disclose information about the original requests or inform about providing corresponding copies to a third-party public archive?
8. Does the company publish this data at least once a year?
9. Can this data be exported in a structured file format?
10. Does the company provide accessible information stating that the reporting includes all types of private requests?

F8. USER NOTIFICATION ABOUT CONTENT AND ACCOUNT RESTRICTIONS

PARAMETERS:

1. For companies hosting user-generated content on their platforms. Does the company provide accessible information that users whose content is restricted are notified about it?
2. Does the company provide accessible information that it notifies users when they attempt to access restricted content?
3. Does the company indicate in its notification the reason for content restriction (legal or other grounds) in an accessible manner?
4. Does the company provide accessible information that it notifies users in case their account is restricted?

F11. USER IDENTIFICATION POLICY

PARAMETERS:

1. Does the company require verification of users' identities using a government-issued identity document or through other types of identification data that can be used for offline identification?

F12. ALGORITHMIC CONTENT CURATION, RECOMMENDATION, AND/OR RANKING SYSTEMS

PARAMETERS:

1. Does the company provide accessible information on the use of algorithmic systems for curation, recommendation, and/or ranking of content available to users on its platform?
2. Does the company explain in an accessible way how it uses algorithmic systems for curation, recommendation, and/or ranking of content, and which variables influence these systems?
3. Does the company explain in an accessible way the options available to users to control the variables considered by the algorithmic system for curation, recommendation, and/or ranking of content?
4. Does the company disclose in an accessible way information on the use of algorithmic systems for automatic curation, recommendation, and/or ranking of content by default?
5. Does the company explain in an accessible way that users have the option to consent to automatic curation, recommendation, and/or ranking of content?

F13. AUTOMATED SOFTWARE AGENTS ("BOTS")

PARAMETERS:

1. Does the company clearly disclose the rules governing the use of bots on its platform?
2. Does the company provide accessible information that users must clearly label any content and accounts created, disseminated, or managed via a bot?
3. Does the company explain in an accessible way the process for enforcing the bot policy?
4. Does the company provide accessible information on the volume and nature of user content and accounts restricted for violating the company's bot policy?

P1(A). ACCESS TO PRIVACY POLICY

PARAMETERS:

1. Is it easy to find the company's privacy policy?
2. Is the company's privacy policy published in the main language(s) spoken by users in the country of its national jurisdiction?
3. Is the policy presented in a clear and easily understandable format?

P1(B). ACCESS TO ALGORITHMIC SYSTEMS DEVELOPMENT POLICY

PARAMETERS:

1. Is it easy to find the company's algorithmic systems development policy?
2. Is the company's algorithmic systems development policy published in the main language(s) spoken by its users?
3. Are the provisions of the algorithmic systems development policy presented clearly?

P2(A). CHANGES TO PRIVACY POLICY

PARAMETERS:

1. Does the company provide clear information that it directly notifies users about changes to the privacy policy?
2. Does the company explain clearly how it directly notifies users about changes?
3. Does the company publish, in an accessible manner, the timeframes within which it directly notifies users about changes to the privacy policy before they take effect?
4. Does the company maintain a public archive or record of changes made?

P2(B). CHANGES TO ALGORITHMIC SYSTEMS DEVELOPMENT POLICY

PARAMETERS:

1. Does the company provide clear information that it directly notifies users about changes to the algorithmic systems development policy?
2. Does the company explain clearly how it directly notifies users about changes?

3. Does the company publish, in an accessible manner, the schedule according to which it directly notifies users about changes to its policy before they take effect?
4. Does the company maintain a public archive or record of changes made?

P3(A). COLLECTION OF USER DATA

PARAMETERS:

1. Does the company clearly disclose which user data it collects and how?
2. Does the company clearly disclose how it collects each type of user data?
3. Does the company explain clearly that it limits the collection of user data strictly to what is necessary for providing its services?

P3(B). USER DATA OBTAINED THROUGH INFERENCE

PARAMETERS:

1. Does the company clearly disclose which user data it collects and how?
2. Does the company clearly disclose how it collects each type of inferred user data?
3. Does the company explain clearly that it limits the collection of inferred user data strictly to what is necessary for providing its services?

P4. PROVISION OF USER DATA TO THIRD PARTIES

PARAMETERS:

1. Does the company clearly explain which user data it shares and with whom, providing a breakdown by data type?
2. Does the company clearly explain which types of third parties it shares user data with, with a breakdown by data type?
3. Does the company clearly explain that it may provide user information in response to government or judicial requests?
4. Does the company clearly disclose the names of all third parties with whom it shares user data, with a breakdown by data type?

P5. PURPOSES OF COLLECTING, INFERRING, AND SHARING USER DATA

PARAMETERS:

1. Does the company clearly explain the purposes for which it collects user data, with a breakdown by data type?
2. Does the company clearly explain the purposes for which it infers user data, with a breakdown by data type?
3. Does the company clearly explain whether it correlates information about users across different company services? If yes, for what purpose?
4. Does the company clearly explain the purposes for sharing user data with third parties, with a breakdown by data type?
5. Does the company clearly explain that it limits the use of user data to the purposes for which the data were collected or inferred?

P6. STORAGE OF USER DATA

PARAMETERS:

1. Does the company clearly explain how long it retains user data, with a breakdown by data type?
2. Does the company clearly explain which anonymized user data it stores?
3. Does the company clearly explain its processes for anonymizing user data?
4. Does the company clearly state that it deletes all user data after users delete their accounts?
5. Does the company clearly disclose the timeframes for deleting all user data after users delete their accounts?

P7. USER CONTROL OVER THEIR DATA

PARAMETERS:

1. Does the company clearly explain whether users can control the collection of their personal information, with a breakdown by each type of user data collected?
2. Does the company clearly explain whether users can delete their personal information, with a breakdown by each type of user data collected?
3. For each type of user information derived (through automated collection) from collected data, does the company clearly explain users' ability to control the output of such data?
4. For each type of user information derived from collected data, does the company clearly explain users' ability to delete such information?

5. Does the company clearly explain that it allows users to control the use of their personal data for targeted advertising?
6. Does the company clearly state that targeted advertising is disabled by default?
7. Does the company clearly explain that it allows users to control the use of their data in algorithmic systems development?
8. Does the company clearly explain whether it uses or does not use user data for algorithmic systems development by default?

P8. USER ACCESS TO THEIR DATA

PARAMETERS:

1. Does the company clearly disclose that users can request a copy of their personal data?
2. Does the company clearly disclose which user information users can obtain?
3. Does the company clearly disclose the possibility for users to receive their personal data in a structured format?
4. Does the company clearly disclose the possibility for users to access all public and private information held about them?
5. Does the company clearly disclose that users can access the list of advertising audience categories assigned to them?
6. Does the company clearly disclose that users can obtain all the information the company can derive about them?

P10(A). RESPONSE PROCESS FOR GOVERNMENT REQUESTS FOR USER INFORMATION

PARAMETERS:

1. Does the company clearly report on its process for responding to non-judicial government requests?
2. Does the company clearly report on its process for responding to judicial orders?
3. Does the company clearly report on its process for responding to requests from foreign governments?
4. Does the company clearly explain the legal basis on which it may comply with government requests?
5. Does the company clearly explain that it exercises due diligence before responding to government requests?
6. Does the company commit to resisting unlawful or overly broad government requests?
7. Does the company provide, in an accessible manner, guidance or examples illustrating its process for responding to government requests?

P11(A). GOVERNMENT REQUESTS FOR USER DATA

PARAMETERS:

1. Does the company provide data on the number of such government requests received, with a breakdown by country?
2. Does the company provide data on the number of government requests for stored user information and real-time communications access?
3. Does the company provide data on the number of accounts affected by such requests?

4. Does the company provide data on the nature of the request: content, non-content, or both?
5. Does the company specify the legal channels or processes through which law enforcement and national security authorities make requests?
6. Does the company include data on government requests made pursuant to court orders?
7. Does the company provide data on the number of government requests fulfilled, with a breakdown by category?
8. Does the company provide data on the types of government requests it is legally prohibited from disclosing?
9. Does the company provide such data at least annually?
10. Can the data provided by the company be exported as a structured data file?

P12. USER NOTIFICATION OF THIRD-PARTY REQUESTS

PARAMETERS:

1. Does the company clearly state that it notifies affected users when a request from government authorities (including courts or law enforcement) for user information is received?
2. Does the company clearly state that it notifies affected users when a private request for user information is received?
3. Does the company clearly disclose the circumstances under which user notification is not possible, and specify the types of government requests it cannot notify users about under applicable law?

P13. SECURITY REVIEW

PARAMETERS:

1. Does the company clearly disclose the existence of employee access restriction and control systems for user information?
2. Does the company clearly disclose the existence of a security department that conducts security reviews of the company's products and services?
3. Does the company clearly disclose information about security audits of its products and services conducted with the involvement of third-party contractors?

P15. DATA BREACH

PARAMETERS:

1. Does the company clearly disclose that in the event of a data breach it will promptly notify the relevant authorities?
2. Does the company clearly explain the process for notifying affected individuals in such cases?
3. Does the company clearly disclose the steps that will be taken to mitigate the consequences of a data breach for users?

DRCQ

For a detailed audit and personalized recommendations aimed at enhancing company transparency, upholding high standards of digital user rights, and strengthening user trust and loyalty towards web services, you can contact the experts of the DRCQ Team.

CONTACTS

Email: kz@drc.law
T.: +7 775 007 81 99
https://drcq.law/
https://digitalrights.kz/