alrud.com

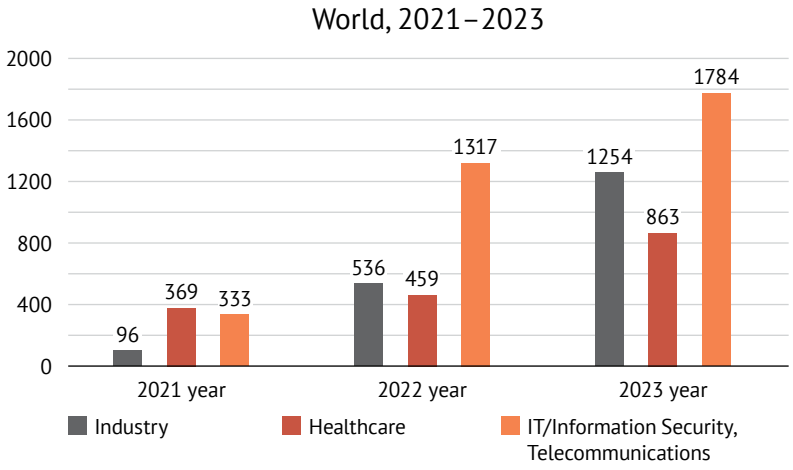
Data Protection: What Do Operators Need To Know in 2024?

ALRUD

Dear Readers,

According to a report by the International Association of Privacy Professionals (IAPP)[1], in recent years there has been a major increase in the number of requests for personal data on the Internet, and the teams of lawyers who deal with personal data protection issues are constantly expanding.

On 31 May 2024, Infowatch published a study titled 'Three-Year Study of Information Leaks in Industries[2], which showed that there has been a substantial and steady increase in the number of data leaks worldwide in such key industries as healthcare, IT and telecommunications, and industry. You can see the data from the Infowatch study in the chart below.



The authorities in Russia and the rest of the world have recently been paying more and more attention to data protection issues. This is evidenced by the numerous laws adopted in this regard, the increased activities of the Russian Federal Service for Supervision of Communications, Information Technology and Mass Media (Roskomnadzor), despite a moratorium on scheduled inspections, and the serious amendments that are expected to be introduced to broaden liability for violations of data protection laws.

For example, in a report that Roskomnadzor issued for 2023[3], we can see that a total of **RUB 266,324,329** in administrative fines were imposed last year compared with **RUB 109,579,160** in 2022[4]. This means that, despite the moratorium on scheduled inspections, Roskomnadzor more than doubled its efforts to hold individuals accountable for violations of legislation on the protection of personal data in 2023 compared with the previous period.

Russian data protection laws impose numerous requirements on operators, and companies must expend enormous resources and be highly vigilant in the processing of personal data to comply with them. As a result, internal teams and DPOs often have questions about which requirements are most critical and pose the greatest risk to business. The list of requirements may vary depending on the size of the business and the company's industry, business model, and other factors, however, there are issues that will be crucial for most operators. In this brochure, we have highlighted such issues for the current period and invite you to learn more about them.

Maria Ostashenko, Partner

Anastasia Petrova, Of Counsel

1. IAPP-EY Privacy Governance Report 2023 – Executive Summary
2. Three-Year Investigation into Information Leaks in Industries — Analytical Report (infowatch.ru)
3. gosdoklad_za_2023_03042024.pdf (rkn.gov.ru)
4. 2022_RKN_goskontrol.pdf

The importance of written consent

From the standpoint of law enforcers, consent remains one of the most important legal bases for data processing.

One of the most significant changes that took place at the end of 2023 was a multi-fold increase in fines for processing personal data without written consent when such consent must be obtained.

Moreover, in addition to the absence of consent, the failure to comply with the mandatory requirements of the law also constitutes an offence. The increased fines for this offence are as follows::

- **Up to 700,000 RUB** for the first offence instead of 150,000 RUB
- **Up to 1,500,000 RUB** for repeated offences instead of 500,000 RUB

The substantial increase in the amount of fines shows just how closely Roskomnadzor (the Russian data protection authority) is monitoring this issue. Companies are thus advised to double-check existing written consents for the processing of personal data and make the necessary changes to their forms if any inconsistencies with the law are found.

Finally, we would like to remind you of Roskomnadzor's ability to impose multiple fines based on the number of personal data subjects. For example, in response to reports from Roskomnadzor, five different court decisions were handed down with respect to one data controller in a single case based on the number of individuals whose rights were violated as a result of the illegal processing of personal data[1].

Inspections by Roskomnadzor

Roskomnadzor was granted new grounds for unscheduled inspections in late 2023. This will allow for more frequent inspections despite an ongoing moratorium.

These grounds involve the existence of three or more discrepancies between the information posted on the data controller's website and the information that the data controller has previously included:

- ☑ In the notification of intent to start processing personal data
- ☑ In the notification of intent for the cross-border transfer of personal data

To avoid an unscheduled inspection, it is important for personal data controllers to regularly check their own websites to ensure compliance. Roskomnadzor may conduct independent monitoring activities to identify violations without the cooperation of the data controller. Alternatively, it may do so after receiving an anonymous complaint from a third party.

Please be aware that during the moratorium, Roskomnadzor also has the right to check the personal data controller as part of:

1. Website control measures without interacting with the data controller
2. Preventive visits
3. Unscheduled inspections (based on a specific list of grounds and with the agreement of the prosecutor's office)

1. See: Synergy University Case (decisions of the justice of the peace of Judicial District No. 383 of the Meshchansky Judicial District of Moscow in the following cases: N 5-119/2020, N 5-120/2020, N 5-121/2020, N 5-122/2020 and N 5-123/2020)

Requirements for online resources

The accelerated pace of external monitoring and the new statutes of information and personal data legislation introduced in 2023 have elevated website compliance issues to among the top trends for 2024.

In addition to general compliance issues, such as ensuring the legal basis for processing personal data, as well as the processing of Russians citizens' personal data in databases on the territory of Russia (localization requirement), companies that own websites should pay close attention to the following specific aspects that are applicable to websites:

- The use of recommendation technologies (profiling): Roskomnadzor may block a website if the owner fails to inform users about the use of such algorithms and/or fails to publish rules for their application.
- Compliance with user authorization requirements: website owners have seen their available options for user authorization restricted to four methods (via telephone, the Gosuslugi service, the unified biometric system or a system that meets the requirements of the law).
- The use of foreign services: in particular Google Analytics, CAPTCHA and similar tools that are used to process personal data on websites. The use of these services trigger the need to comply with the rules of cross-border transfer and localization requirements, as well as grounds for Roskomnadzor to request proof of compliance by the data controller.
- The use of cookies: the processing of cookies involves the processing of personal data, which must be described in the data controller's policy. A legal basis for the processing of personal data, such as user consent, must also be provided.
- Marketing mailings: the appropriate individual consents must be obtained prior to sending marketing mailings to users. Consent to marketing communications may not be included within the consent to the processing of personal data or within the privacy policy. Consent to marketing communications must be presented to users separately.
- Compliance with content requirements: certain information may not be posted in general or for certain audiences (e.g., children or the resulting requirements for age labelling of website content).

The 'extraterritorial' principle of the application of the personal data law

The 'extraterritorial' principle is a relatively new concept in personal data legislation. It is part of the legislation of many states, and its inclusion in Russian legislation reflects the legislators' intention to extend the reach of national law to data controllers who use the data of Russian citizens in their businesses. The need for this principle arises from the evolution of the digital economy and the necessity to regulate Internet resources – primarily foreign ones – that target the Russian market.

The 'extraterritorial' principle in Russia means that Russian personal data legislation extends to data controllers who conclude agreements with Russian users and/or obtain consent to process personal data from Russian users. Foreign data processors (persons acting on behalf of data controllers) are liable to the subjects of personal data along with the data controller.

In practice, this means that foreign persons processing the personal data of Russian citizens should consider the scope of applicability of Russian personal data legislation and the extent of liability for compliance with it. They should then pay regular attention to compliance and keep abreast of changes.

Localization trend

In 2024, the digital industry in the Russian Federation will continue to focus on localization and ensuring the independence of domestic information and the security of IT solutions.

This trend is being driven by several factors:

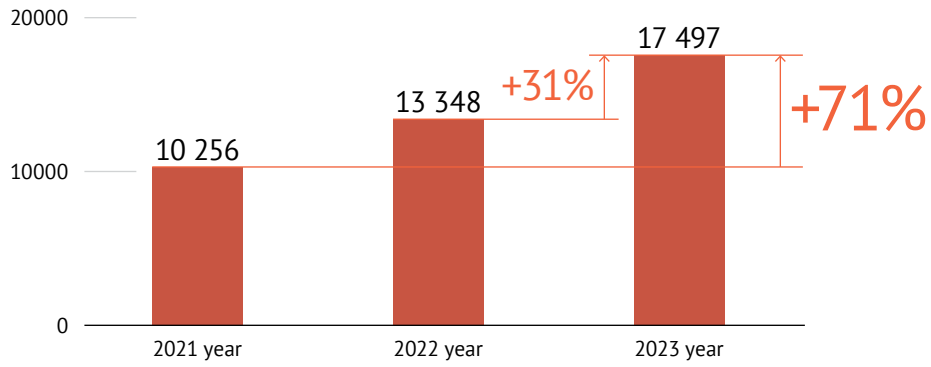
- External: the imposition of the 12th package of EU sanctions, which restricts the use of European software and the use of IT services
- Internal: the focus on the sovereign segment of the Internet, new rules for hosting providers and the import substitution of software and information security tools (the ban on the purchase of foreign software and related services as part of government procurements for use at significant critical information infrastructure ("CII") facilities, ban on the use by CII entities of information security tools from unfriendly countries, ban on the use by CII entities of "untrusted" hardware and software systems when a Russian analogue exists and probable ban on the use of foreign software at any significant CII facilities).

It should be noted that Federal Law No. 152-FZ dated 27 July 2006 "On Personal Data" requires that the personal data of Russian citizens be processed using databases located on the territory of the Russian Federation when collecting such data. Failure to comply with this legal requirement is subject to the following fines:

- **Up to 6,000,000 RUB** for the first offence
- **Up to 18,000,000 RUB** for repeated offences. A fine for a repeated offence may be imposed with no limit on the number of times.

As a result, we anticipate that localization trends will intensify in the near future. It is thus crucial for companies to assess the extent to which existing localization and import substitution restrictions and requirements apply to them, as well as to analyse the potential applicability of newly introduced requirements and restrictions.

Legal disputes involving personal data in Russia[1]



The number of legal disputes involving personal data in Russia increased by 71% over two years

1. https://mosdigitals.ru/media/za-poslednie-dva-goda-v-rossii-kolichestvo-sudebnykh-del-po-personalnym-dannym-vyroslo-na-71

Cross-border data transfer

The rules on the cross-border transfer of personal data, which came into force on 1 March 2023, remain in effect in 2024.

As a reminder, data may only be transmitted across borders after submitting a special notification to Roskomnadzor. This notification must be preceded by an assessment of the recipient of the personal data abroad in terms of its compliance with confidentiality and personal data protection measures.

Roskomnadzor may prohibit or restrict the cross-border transfer of personal data. In practice, this does not happen often, but it is important to recognize the risks of restricting cross-border transfer processes in relation to certain data controllers. In some cases, this could result in the interruption of business processes.

In practice, notifications about the cross-border transfer of personal data raise many questions, including how to comply with the requirements for assessing the foreign data recipient and whether a second notification is required when the data processing procedures change in terms of data volume.

Another aspect of cross-border transfers that data controllers should pay attention to is the use of foreign services to collect data from websites and applications and to create reports with information that is useful for business. For example, this could include using the well-known Google Analytics service. Roskomnadzor believes the use of such services is indicative of cross-border transfers and entails the need for compliance with the relevant requirements to notify the regulator and assess the recipient of the data abroad.

One of the key considerations is that a data controller may only notify Roskomnadzor of a cross-border transfer if it is registered in the register of personal data controllers.

There is currently a trend towards increased regulatory control over cross-border transfers by data controllers.

Anonymous data

The year 2024 could be a pivotal one for the regulation of anonymous personal data if a draft law[1] that sets out the fundamental principles for the entire industry is adopted.

At present, there are no established transparent rules for private businesses to follow with regard to the anonymization of data. In most cases, Roskomnadzor rules that anonymous data remains personal data with all the resulting legal limitations on the processing of such information.

The new draft law proposes establishing a general framework for the regulation of anonymization with numerous specific issues to be further resolved at the level of bylaws.

The changed proposed in the draft law would impose the following new requirements on companies: transferring anonymous data sets to a state information system, complying with the prescribed procedure for the use of such data, and other obligations. In addition, businesses would be directly responsible for anonymizing data with the relevant costs borne by the companies themselves. Further legal amendments are expected to be made in this area to facilitate the growth of artificial intelligence technologies.

For businesses, your best strategy in 2024 is to stay informed about legislative changes regarding data anonymization and the use of anonymous data.

1. Bill No. 992331-7 "On Amendments to the Federal Law "On Personal Data"" (https://sozd.duma.gov.ru/bill/992331-7#D97CDA3F-60FD-489B-B8D7-1A94A87991AC)

Personal data breaches

Several draft laws were submitted in late 2023 to significantly increase liability for data protection violations, both administrative and criminal[1]. This year will be pivotal in terms of the finalization of these draft laws.

The draft laws are currently undergoing being discussed and undergoing the approval process. Please note that the final versions may still change. However, businesses are already facing a number of pressing issues.

- What requirements would a company have to meet to avoid administrative liability and the imposition of large fines considering the new statutes?
- What legal mechanisms should be put in place to mitigate risks?
- How can business owners and employees avoid criminal liability given the uncertain enforcement of laws?

One of the potential amendments to the draft law is the introduction of a mechanism to compensate individuals affected by data breaches. Individuals whose personal data has been compromised will be able to request compensation from a company via the Gosuslugi service. If two-thirds of the individuals affected agree with the amount offered by the offender, this will be considered a mitigating factor when determining the offender's administrative liability (including the use of lower rates when determining turnover-based fines).

In light of the upcoming regulatory requirements, companies are encouraged to conduct an internal audit of their personal data processing processes, develop and introduce a procedure to timely respond to data breaches, assess and comply with information security requirements that will help prevent various incidents, and consider compensatory measures. These and other measures will help businesses avoid large fines of up to 500 million RUB and potential negotiable penalties.

Notification of a personal data breach

The regulation requiring data controllers to notify Roskomnadzor about a data breach came into force in 2022. In accordance with the current legislation, data controllers are required to notify Roskomnadzor about a data breach within 24 hours (and with a further notification within 72 hours on measures taken to remedy the incident).

The provisions remain highly relevant, including with regard to the potential introduction of an amended fine. While the current fine for failure to provide notification about an incident is a relatively small amount for a company of up to 5,000 RUB, the proposed amendments would significantly increase this fine. If companies are held liable, the fine could be as much as 1,000,000 to 3,000,000 RUB for a single offence[2].

1. Bill No. 502104-8 "On Amendments to the Code of the Russian Federation on Administrative Offences" (https://sozd.duma.gov.ru/bill/502104-8) / Bill No. 502113-8 "On Amendments to the Criminal Code of the Russian Federation" (https://sozd.duma.gov.ru/bill/502113-8)
2. Aforementioned bill. Bill No. 502104-8 "On Amendments to the Code of the Russian Federation on Administrative Offences" (https://sozd.duma.gov.ru/bill/502104-8)

Personal liability of management and imposition of criminal liability

Whereas in previous years the legislative trend towards greater liability for data protection mainly concerned companies as data controllers, in early 2024 legislators went beyond the mechanism of "impersonal" liability.

As a result, a new draft law[1] submitted by the Central Bank of Russia on the dismissal of persons responsible for information security at financial organizations for data breaches and other violations is under discussion.

Furthermore, a draft law on imposing criminal liability for illegal trafficking and data breaches of personal data is another manifestation of this trend. This draft law calls for up to 10 years in prison for individuals found guilty of such violations.

These initiatives are reflective of attempts to move towards a mechanism of individual liability for violations of personal data and information security laws. Legislators clearly intend to make sure management is paying increased attention to compliance with existing regulations.

1. The bill was not published. Link to source: https://iz.ru/1636949/natalia-ilina/10-let-bez-prava-top-menedzherov-bankov-diskvalifitciruiut-za-utechki-dannykh

Key Contacts

Maria Ostashenko
Partner

Commercial, Intellectual Property,
Data Protection and Cybersecurity

MOstashenko@alrud.com

Anastasia Petrova
Of Counsel

Data Protection and Cybersecurity,
Labour law

APetrova@alrud.com

Elizaveta Kostyuchenko
Associate

Intellectual Property,
Data Protection and Cybersecurity

EKostyuchenko@alrud.com

Victoria Shvetsova
Associate

Data Protection and Cybersecurity

VShvetsova@alrud.com

Skakovaya str., 17, bld. 2, 6th fl., Moscow, Russia, 125040
E-mail: info@alrud.com | www.alrud.com | Тел. +7 495 234-9692

ALRUD