

Newsletter

Media and Data Protection Laws in 2021: What's New?

January 27th, 2021

Dear Ladies and Gentlemen,

We would like to inform you that several laws, that will have a significant impact on IT and data protection regulation, were adopted at the end of 2020 ("**Amendments**").

1. Further rules for blacklisting Internet resources

The first amendment to Russian law is aimed at securing guarantees, for citizens' rights, to freely search, access and disseminate information. It introduces the status of the **owner of an Internet resource, who is** involved in violations of the fundamental human rights of Russian citizens.

The Prosecutor General, in consultation with the Russian Foreign Ministry, may assign this status to the owner of an Internet resource that, inter alia, discriminates against materials from the Russian media. Such a decision can be made if the Internet resource limits access to socially-important information on the basis of nationality, language, or in connection with the imposition of sanctions against Russia, or its citizens. An owner of Internet resource must be notified of such decision.

In case the owner of Internet resource does not stop censoring, or in some way restricts the access to accounts of Russian media outlets, the Federal Service for Supervision of Communications, Information Technology, and Mass Media ("**Roskomnadzor**") is entitled to **restrict fully, or partially, access** to such Internet resource.

This amendment came into force on January 10th 2021.

2. New monetary fines

New amendments entail considerable fines for failure to delete prohibited information, upon the request of Roskomnadzor.

The fines imposed on **(i)** hosting providers, or any person enabling other persons to publish information on the Internet, for failure to restrict access to prohibited information and **(ii)** owners of the websites, or Internet resources, for non-deletion of prohibited information, may be up to **4,000,000** Roubles (approx. EUR 43,500, USD 53,000) for the first offence and up to **10% of the company's annual turnover**, from the preceding calendar year, (but not less than 4,000,000 Roubles) for a subsequent offence.

If prohibited information contains propaganda of extremism, child pornography, or drugs, liability is increased for up to **8,000,000** Roubles (approx. EUR 87,000, USD 106,000) for the first offence, or up to **20% of the company's annual turnover** from the preceding calendar year (but not less than 8,000,000 Roubles) for the subsequent offence.

This amendment was elaborated due to the fact that Russian laws do not prescribe any liability for hosting providers, owners of websites and information resources who fail to restrict access or delete information, the dissemination of which is prohibited in Russia.

This amendment came into force on January 10th 2021.

3. Information on security and State officials

This amendment introduces a **ban** on the **publication of information** about the activities and private lives of security and State officials and their relatives. Under the current legislation, such a prohibition was provided only in case of a threat to the officials' lives.

The authors of this amendment point out that the practice of unauthorized publication on the Internet, of information about the activities and private lives of security and State officials and

their relatives, is expanding, which negatively affects their ability to fulfill their functions.

We believe that in connection with this amendment, the court may recognize such information as prohibited and oblige the sites to remove it.

This amendment came into force on January 10th 2021.

4. Social media register

According to the amendments, **social networks** are defined as websites, information systems, or software, that simultaneously fall under the following criteria:

- used for provision and dissemination of information by creating users' personal pages in Russian, official languages of Russian republics and other languages of Russian national groups;
- contain advertising aimed at attracting the attention of consumers in the territory of the Russian Federation;
- more than **500,000 Internet users** from the territory of the Russian Federation visit **the site daily**.

If such resource is considered a social network, it will be **included in the register**, which Roskomnadzor is authorized to maintain.

Within **3 days** after the social network receives notification of the inclusion into the register from Roskomnadzor, the hosting provider, or other person enabling the placement of social network on the Internet, must **identify the owner of the social network** and provide information about it to Roskomnadzor.

If a resource is included in the social network register, such resource becomes obliged to **identify and restrict access to illegal content**. It includes child pornography, the propaganda of drugs and suicide, advertising of online casinos, remote sale of alcohol, and information expressing "obvious disrespect" to society and the State.

Moreover, the following information shall be **posted on the social network** by its owner:

- name, email address and an electronic form for sending requests about any illegal content;
- annual reports on the results of the consideration of requests and monitoring activities;
- terms of use of the social network.

This amendment will enter into force on February 1st 2021.

5. Unified Biometric System

The new law determines the use of the **Unified Biometric System ("UBS")** for remote identification to receive a wide range of **financial and State services**. Currently, only the banks with a basic license are entitled to use UBS to open bank accounts and issue facilities. After the UBS Draft Law enters into force, biometric data (voice recordings, personal images, etc.) can be used for **identification** by State bodies, local government bodies, financial organizations, individual entrepreneurs, notaries public, etc.

This amendment came into force on January 1st 2021, however, certain provisions of the amendment will enter into force on January 1st 2022.

6. Publicly-available personal data

The new law significantly changes the legal landscape with regard to the use of publicly-available personal data.

According to the new law, data controllers making personal data publicly available, for their further use by third parties, shall:

- obtain individuals' specific consents, which shall not be bundled with any other consents;
- enable individuals to choose the types of their personal data to be made publicly available and set out restrictions on the use of such personal data;
- enable individuals to revoke their consents, for making the data publicly available, with immediate effect;
- set out the rules, for use of the publicly-available data with a view to individuals' consents, and post such rules on their relevant web-resources.

When it comes to the third parties who intend using publicly-available personal data, such third parties may either:

- rely on the consent obtained by the controller, making the data publicly available, considering the rules of such use defined by that controller;
- rely on the consent provided by an individual to Roskomnadzor, via a dedicated web-based platform to be set up under the law, but also considering the rules of data use defined by Roskomnadzor;

- ensure on their own, that they have appropriate legal grounds for the use of such publicly-available personal data.

The new requirements will enter into force gradually on March 1st and July 1st 2021.

Conclusion

The Amendments are aimed at more detailed regulation of IT and data protection in Russia. They eliminate legal gaps and tighten existing

liability for offenses committed in the digital space.

Thus, the Russian authorities will have more mechanisms of influence on websites, news media, social media and video hostings. We believe that upcoming significant fines and potential blacklistings will change the peculiarities of ensuring compliance with the Russian laws, including for companies without a presence in Russia.

We hope that the information provided herein will be useful for you. If any of your colleagues would also like to receive our newsletters, please send them the link to complete a [Subscription Form](#). If you would like to learn more about our [Telecommunications, Media and Technology Industry](#), please let us know in reply to this email. We will be glad to provide you with our materials.

Note: Please be aware that all information provided in this letter was taken from open sources. Neither ALRUD Law Firm, nor the author of this letter, bear any liability for consequences of any decisions made in reliance upon this information.

If you have any questions, please, do not hesitate to contact ALRUD Partner

Sincerely,
ALRUD Law Firm



**Maria
Ostashenko**

Partner

Commercial, Intellectual
Property, Data Protection &
Cybersecurity, TMT

E: mostashenko@alrud.com