Russia Introduces New Requirements for Processing of Publicly Disclosed Personal Data

19 April 2021

On 1 March 2021, Federal Law No. 519-FZ on Amendments to the Federal Law on Personal Data dated 30 December 2020 (the "Law") came into force. The Law places additional burdens on companies operating in Russia to obtain consents from individuals whose personal data will be posted on a publicly available website, for example, while creating a profile on a social media or a webpage dedicated for a particular person.

Starting from 1 March 2021, if a data subject's personal data is posted on a publicly available resource, the operator of that resource (the "data operator") must obtain a specific consent from the data subject to allow for public disclosure of that individual's data ("Special Consent"). This is additional to general data processing consent, which is still required under pre-existing data protection law.

If a data subject does not grant Special Consent, the data operator must restrict access to that individual's personal data on the relevant publicly available resource. Further, if the data subject places any conditions or restrictions in the Special Consent on the use of his or her personal data, the data operator must disclose those conditions or restrictions, and as a general rule, third parties must abide by those restrictions in their processing of that data.

The Law is likely to have a substantial impact on a wide range of businesses. Most directly, it would apply to data operators, which include not only social media companies but also companies that publish personal data of their employees or others on their websites. The Law also applies to anyone who uses publicly available personal data for various purposes, ranging from companies that target advertisements to individuals based on publicly available personal information to businesses that conduct due diligence on third parties in part by reviewing publicly available information.

The way the Law will be interpreted and enforced remains to be seen. According to the position of the Russian Ministry of the Digital Development, Connection and Mass Media, on the jurisdictional reach of personal data legislation, the provisions of the Law would extend to any data operator that targets its activities to Russia. The same

approach may apply to a third party that uses personal data published on Russian-based publicly available resources in connection with Russian-related activities. Although extraterritorial application of the Law may be difficult, Russian data protection regulators could take measures to restrict access to alleged violators' websites from Russia.

Below is a summary of the principal provisions of the Law.

Special Consent. In order to publish personal data on a publicly available resource such as a social network or a website, the operator of that resource must obtain a Special Consent from the data subject. The form of the Special Consent must comply with the requirements of the Federal Service for Oversight of Communications, Information Technologies and Mass Media ("Roskomnadzor"). Those requirements are currently being registered with the Ministry of Justice of the Russian Federation, but it is expected that the Special Consent will have to include, in particular, the following:[1]

- the purposes for which the personal data is being published;
- the categories of personal data being published, with the data subjects having a right to determine which specific personal data elements they agree to be published;
- the conditions or restrictions, if any, that the data subjects impose on the publication of their personal data (as discussed in more detail below);
- the time limit of the Special Consent, which cannot be indefinite and cannot be automatically extended; and
- a link to the data operator's publicly available resource where the personal data will be published.

The Special Consent can be given to the data operator directly or, after 1 July 2021, through the information system to be launched by Roskomnadzor.

Transfer of Publicly Disclosed Personal Data. The data operator can transfer publicly disclosed personal data only if the data subject explicitly agrees to such transfer in the Special Consent. "Transfer" in this context means making the personal data available to any other person or entity. In other words, if the data subject does no explicitly agree to the data transfer, the data operator must make the data subject's user profile or website

[1] The draft Order of Roskomnadzor on the Approval of Requirements on the Content of Consent to the Processing of Personal Data Permitted by the Data Subject for Dissemination (the "Draft Order of Roskomnadzor") is available at https://regulation.gov.ru/projects#npa=113086.

housing the personal data unavailable to anyone other than the data subject and the data operator. The only exception is when the transfer is required to promote state, social or other public interests provided by law.

A data subject may completely prohibit any transfer of personal data or place conditions on such transfer in the Special Consent. For example, a data subject may allow the transfer only for the purposes of receiving certain types of communications but not others (e.g., news but not advertising). To allow an unconditional and unrestricted transfer of personal data, the data subject must clearly state that there are no conditions or restrictions in the Special Consent. If the Special Consent is silent on this topic, it will be presumed that transfer of personal data is prohibited.

The restrictions may apply to all personal data or specific categories or types of personal data as indicated by the data subject. Information on the restrictions and conditions imposed on publishing, transfer or other processing of publicly available personal data must be disclosed by the data operator (for example, in the data subject's user profile) within three business days of the receipt of the Special Consent setting out those restrictions and conditions. According to the logic of the law, if the data operator provided the information on relevant restrictions and conditions, but a third party nevertheless used the personal data in violation of them, the liability for the breach would be on the third party.

Termination of Transfer of Personal Data. A data subject may at any time revoke the Special Consent or change the terms of the Special Consent. If the data subject revokes the consent to data transfer, the data operator must make the data subject's personal data publicly unavailable (e.g., by making the user profile or webpage containing that data private).

If the terms of a data subject's Special Consent are violated, the data subject can file a legal claim. This could be the case, for example, if a data subject prohibited the use of his publicly disclosed data for advertising purposes but nonetheless received customized advertising offerings based on his data.

The person or entity processing personal data must terminate the transfer of personal data within three business days upon receipt of the data subject's request or within the period ordered by the court.[2] Failure to comply with this requirement may lead to the

[2] If no period is prescribed by the court order, the transfer of personal data must be terminated within three business days after the court order comes into force.

imposition of an administrative fine on a company of up to RUB 100,000 (approx. USD 1,300) and/or on company officers of up to RUB 20,000 (approx. USD 260).[3]

* * *

Please do not hesitate to contact us should you have any questions.

LONDON / NEW YORK

Jane Shvets
jshvets@debevoise.com

NEW YORK

Jeremy Feigelson
jfeigelson@denevoise.com

MOSCOW

Anna V. Maximenko
avmaximenko@debevoise.com

Elena Klutchareva
emklutchareva@debevoise.com

Nikolay Kiselev
nskiselev@debevoise.com

[3] Article 13.11 (1) of the Administrative Offences Code of the Russian Federation.