

## Newsletter

### *Data Protection guidelines: to-do list if you are not ready to submit the notification on cross-border data transfer before 1 March 2023*

February 27, 2023

Dear Ladies and Gentlemen,

As a result of major data protection reforms that took place in 2022 in Russia, companies are required to comply with new cross-border data transfer rules that take effect on 1 March 2023. The new rules require data controllers to review their data flows, aggregate information about foreign data importers and adapt internal regulations on cross-border data transfer within their companies.

Considering the tight deadline and that many companies are not quite ready to file the notification before 1 March 2023, we have prepared the below to-do list for those who are not ready to submit the notification in time.

#### After 1 March 2023

In the event of continued data transfers abroad and/or changes in cross-border data processing (i.e., new purposes, legal basis, foreign jurisdictions where data is to be transferred), data controllers **must submit a notification of intent** to make such a transfer.

The requirements for the notification of intent are as follows.

Filing a notification of intent to transfer data abroad	Required and recommended actions
<p>The notification must include:</p> <ul style="list-style-type: none"> <li>(i) The contact details of the <b>DPO</b></li> <li>(ii) The registration number in the <b>register of Russian data controllers</b></li> <li>(iii) The purpose and legal basis of the data transfer</li> <li>(iv) A list and categories of the data to be transferred and categories of the data subjects</li> <li>(v) <b>A list of foreign countries</b> to which the data is to be transferred</li> <li>(vi) <b>The assessment date of the foreign data importers' compliance</b> with ensuring the confidentiality and security of the personal data during processing</li> </ul> <p>Before filing the notification, it is also required to:</p> <ul style="list-style-type: none"> <li>(i) Collect information on technical and organizational measures implemented by foreign data importers!</li> </ul>	<ul style="list-style-type: none"> <li>(i) Appoint a DPO</li> <li>(ii) Complete a data mapping exercise with respect to cross-border data flows</li> <li>(iii) Make an entry in the register of Russian data controllers, or amend registration with respect to cross-border data transfers</li> <li>(iv) Collect and assess information on measures taken to protect personal data by foreign importers and the regulation of data protection in any inadequate jurisdiction (if you transfer, or plan to transfer data to such inadequate jurisdictions) and prepare the form of the document confirming the assessment</li> <li>(v) Prepare a template of <b>the notification of intent</b> to transfer data abroad</li> <li>(vi) Before transferring data to foreign recipients, ensure that agreements with them <b>include the obligation of data recipients to</b></li> </ul>

<p>(ii) Collect information regarding the data protection regulation of inadequate jurisdictions to which the personal data is transferred</p> <p>Transfers to inadequate jurisdictions may be carried out upon expiration of the 10 business day period for the Federal Service for Supervision of Communications, Information Technology and Mass Media (Roskomnadzor) to consider a notification of intent to make a cross-border data transfer. Transfers to adequate jurisdictions is not restricted during such consideration.</p> <p>If Roskomnadzor restricts or prohibits the transfer of personal data after considering the notification, the data controller must ensure the deletion of the transferred personal data by foreign data importers.</p>	<p>delete data at the request of the data controller in the event that Roskomnadzor bans or restricts a cross-border data transfer</p> <p>(vii) Prepare a template of a document to confirm the data deletion by data importers that complies with the requirements on data deletion, which can be added as an annex to agreements with foreign data importers<sup>1</sup></p>
---	--

Before filing the notification of intent to transfer data abroad, make sure that none of the following grounds exist for the prohibition or restriction of cross-border data:

Prohibition	Restriction
<ul style="list-style-type: none"> <li>Foreign data importers do not have data protection measures and do not specify the conditions for the termination of data processing</li> <li>The activities of a foreign data importer are prohibited on the territory of the Russian Federation based on a court decision</li> <li>A foreign data importer is included in the list of undesirable organizations in Russia<sup>2</sup></li> <li>The cross-border data transfer and further data processing are incompatible with the purposes of personal data collection</li> <li>The cross-border data transfer is not carried on a statutory legal basis<sup>3</sup>.</li> </ul>	<ul style="list-style-type: none"> <li>The content and scope of the personal data planned for cross-border transfer does not correspond to the purpose of the cross-border transfer of personal data;</li> <li>The categories of personal data subjects whose data are to be transferred do not correspond to the purpose of the cross-border data transfer.</li> </ul>

If Roskomnadzor decides to prohibit/restrict a cross-border data transfer, the respective data controller may re-submit the notification of intent to transfer data abroad if the reasons for such prohibition/restriction are eliminated.

The decision by Roskomnadzor to prohibit/restrict a cross-border data transfer may be appealed out of court and/or in court.

---

### Possible sanctions for the failure to comply with cross-border data transfer rules

---

Transferring data abroad without the respective notifications may potentially lead to a ban or restriction of cross-border data transfers for a particular data controller.

<sup>1</sup> The requirements for the confirmation of personal data deletion are stipulated in Roskomnadzor's [Order No. 179 dated 28 October 2022 "On the Approval of Requirements for the Confirmation of the Destruction of Personal Data"](#).

<sup>2</sup> Please see the list of such organization [here](#).

<sup>3</sup> E.g., a data subject's consent, execution of contract with a data subject, compliance with the requirements of Russian legislation.

In addition, a data controller may face administrative liability in the form of an administrative fine of up to 100 000 RUB (approx. 1,350 USD or 1,263 EUR) per violation.

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 let us know by sending us his/her email address in response to this message. If you would like to learn more about our [Data protection and Cybersecurity](#) practice, 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



**Maria  
Ostashenko**

**Partner**

Commercial, Intellectual Property, Data  
Protection and Cybersecurity

Sincerely,  
[ALRUD Law Firm](#)

E: [mostashenko@alrud.com](mailto:mostashenko@alrud.com)