Practical impact of the recently amended Federal Law on Personal Data: Significant challenge for business or normal compliance routine?

July 25, 2022

ALRUD

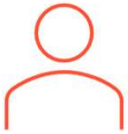
Key provisions of the amended Federal Law on Personal Data

ALRUD

1. Extraterritorial application

The Federal Law on Personal Data will apply to the processing of personal data of Russian citizens conducted on the basis of:

agreements between such citizens and foreign authorities, legal entities or individuals.



consent to the processing of personal data.

ALRUD

2. Definition of personal data processing

- Proposal was to exclude 'provision of access' from the notion of 'transfer'.
- This would have required an independent legal basis for processing.
- The amended law excluded this proposal and kept the original definition.

The Draft Law

(previous version)

.... transfer (distribution, provision), provision of access or performance of logical and (or) arithmetic operations.....

ALRUD

3. New criteria for appropriate consent by data subject

Current version	Amended version
Consent to the processing of personal data must be specific, informed and conscientious.	Consent to the processing of personal data must be specific, substantive, informed, conscientious and unambiguous.

ALRUD

4. “Data Controller – Data Processor” interaction

Data controller and a **foreign** data processor now both bear liability for violating the law:

New mandatory provisions for the assignment of personal data processing

- List of personal data.
- Processor's obligation to comply with data localization requirements.
- Obligation to implement necessary technical and organizational measures under Art. 18.1.
- Requirements for security measures under Art. 19.

New data processor’s obligations

- Observing data confidentiality.
- Obligation to provide documents of compliance with the responsibilities of data processor vis-à-vis data controller.
- Obligation to notify data controller of any data incidents.

ALRUD

5. New rules for cross-border data transfer

- Mandatory notification of the data protection authority ("DPA") by the controller, with the intention to transfer data abroad:

Transfer to adequate jurisdiction	**Transfer to inadequate jurisdiction**
During the notification consideration a transfer is not prohibited	During the notification consideration a transfer is prohibited

- Cross-border data transfer may be restricted to protect the constitutional order, morality, state security, defense or economic interests.

! China, India, Ivory Coast and Kyrgyzstan are now included in the proposed list of adequate jurisdictions.

ALRUD

6. Cross-border data transfer notification

1. Name and contact details of the data controller and its data protection officer ("DPO").
2. Legal basis and purpose of the transfer and further processing.
3. Categories and list of transferred data, categories of data subjects.
4. List of countries for data transfer.
5. Date of the assessment of the implemented by the data recipients data protection measures.

Data controller must also obtain information from a data recipient on the personal data regulations of the inadequate jurisdiction, if data is transferred to its territory.

Notification review period: 10 days

ALRUD

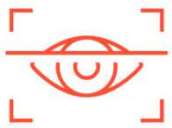
7. New guarantees for data subjects

Data controllers must conduct a due diligence review and ensure that the following contractual clauses are not included in agreements with data subjects:

- Contractual clauses that restrict personal data subjects' freedom.
- Contractual clauses establishing cases for processing minors' personal data, unless cases provided by the law.
- Contractual clauses allowing the omission of the personal data subject, as a condition for the conclusion of an agreement.

ALRUD

8. Restrictions on biometric data processing



Unlawfulness of refusal to provide services: if data subject fails to provide biometric personal data, or refuses to give her/his consent to biometric data processing (if provision of biometric data is not mandatory under a federal law).

Ban on the processing of underage persons' personal data was removed from the law, however, the debate is ongoing.

9. New terms for responses to data subject's requests

Within **10** business days of receipt of a data subject's request, the controller is obliged to stop processing her/his personal data, or to take measures on data clarification, blocking, or destruction.

Within **10** business days of receipt of a data subject's request, the controller is obliged to provide her/him with access to information about the processing of data subject's personal data.

ALRUD

10. New rules on privacy policy

Privacy policy must now include:

1. Purposes of processing, processing operations, categories and list of personal data.
2. Categories of data subjects.
3. Terms of processing, data retention and procedures for erasure.

Privacy policy cannot contain any supplemental obligations of data controller apart from statutory ones.

Risk-oriented approach to the implementation of global policies and additional safeguards.

Privacy policy must also be published on all the webpages where personal data is collected.

ALRUD

11. New rules on data processing notification

List of exemptions from filing a processing notification to the DPA is significantly limited.

Any change must be communicated to the DPA no later than the 15th day of the month following the change.

If processing is terminated, data controller shall notify the DPA within 10 business days.

ALRUD

New obligations and responsibilities in terms of cybersecurity

ALRUD

12. New data controller's obligations on data security

Interaction with the State control system on computer attacks ("GosSOPKA") in accordance with the procedure to be established by the Federal Security Service (FSS).

Harm assessment shall be conducted in accordance with the requirements to be established by the DPA.

13. Data breach notification

Two-step notification procedure with the DPA:

Within 24 hours*:

- Reasons;
- Suspected harm to data subjects;
- Measures taken to mitigate the consequences of the breach; and
- Contact person.

Within 72 hours*:

- Results of the internal investigation; and
- Individuals responsible for the breach.

* *as of the moment that controller, the DPA or any concerned person detects data breach.*

ALRUD

14. New obligations for CII subjects and “others”

Provisions of Presidential Decree No. 250

- Responsibility of the CEO and her/his deputy for information security in the company*.
- Mandatory incorporation of a department responsible for information security*.
- Involvement of third parties for implementation of information security measures.
- Mandatory evaluation of the security level of the information systems.
- Implementation of organizational and technical measures provided by FSS and Federal Service for Technical and Export Control (“FSTEC”).
- Development of information security level monitoring

** Presidential Decree No. 250 of May 1, 2022 "On Additional Measures to Ensure Information Security of the Russian Federation".*

** Governmental Decree No. 1272 of July 15, 2022 "On approval of a model regulation on the deputy responsible for ensuring information security and a model regulation on a subdivision that ensures information security”.*

X5Group

Яндекс

АЛРОСА

Билайн

ALRUD

15. Upcoming restrictions for CII subjects

As of 2025

Prohibition of use of information protection tools of unfriendly states for all CII subjects*

Prohibition of use of foreign software at significant CII facilities, for CII subjects with State corporate participation**

** Decree No. 250 of the President of the Russian Federation of 01.05.2022 "On Additional Measures for Ensuring Information Security of the Russian Federation".*
***Decree No. 166 of the President of the Russian Federation of 30.03.2022 "On measures to ensure technological independence and security of critical information infrastructure of the Russian Federation".*

ALRUD

Recommendations and deadlines for compliance

ALRUD

16. Deadlines for compliance

September 1, 2022

- Revise all data processing agreements, consent form templates, contracts, and policies.
- Update and publish privacy policy on all webpages collecting personal data.
- File a processing notification if no exemptions are met.
- Implement the policy regarding GosSOPKA once the FSS issues the rules

March 1, 2023

- Prepare templates for cross-border transfer notification, assess the counterparties, and adopt local policies.
- Conduct harm assessment when the DPA issues guidelines.

ALRUD

17. Check-list for data controllers

Arrange for the immediate detection of a data breach and for timely filing a notification with the DPA in the event of a data breach.

Audit data transfers and arrange for filing a notification with the DPA in the case of a cross-border data transfer before the transfer.

Arrange for timely procedures for handling and responding to data subjects' and the DPA's requests.

Arrange for tracking of data processing activities and timely notification of the DPA of any changes in data processing activities.

ALRUD

Thank you for your attention!

ALRUD

Contact details

Anastasia Petrova
Of Counsel
E: APetrova@alrud.com

ALRUD Law Firm
Skakovaya st., 17, bld. 2, 6th fl.
Moscow, Russia, 125040
T: +7 495 234 96 92
E: info@alrud.com