ALRUD

Newsletter

Data Protection checklist: how to prepare for new requirements

September 8, 2022

Dear Ladies and Gentlemen,

This summer, a major reform relating to personal data, in Russia, has been instigated. New privacy regulations entered into force on September 1st, 2022. These introduced a number of new requirements to data processing activities. Part of the new requirements, including new cross-border data transfer rules, will come into force from March 1st, 2023. Amendments to the Law on Personal Data entail the need to examine the data processing activities, update most of the data processing documents, as well as to implement new cross-border data transfers, data breach procedures and monitoring and compliance measures, to implement policies establishing procedures for handling each new data subject's rights and guarantees, responsibilities of controllers and processors, etc. Please see our July Newsletter in which you will find our overview of the new law and its provisions.

In view of the upcoming changes, we have prepared the checklist below, answering the most frequent questions regarding implementation of the novelties of the Law on Personal Data and navigating data controllers' on compliance level, as well as relevant risks and actions that should be taken, in order to comply with the new requirements.

Aspect of data processing	Questions	Action needed
Interactions with data subjects	(i) Does the consent form that you use include details on the processing, such as the concrete purpose of processing, non-excessive list of personal data, details of data processors, relevant methods, terms of processing and clarifications regarding the consequences of not providing data? (ii) Do you use implicit opt-in consent mechanisms? (iii) Do your policies provide for a term of 10 days to respond to DSRs?	(i) Avoid generic and vague language for consents and revise the consent template. (ii) Avoid pre-ticked boxes and opt-out mechanisms and revise the consent template. (iii) Revise the consent templates. (iv) Make sure that policy describes proper rules for responding to requests of data subjects, update the policies and procedures of interactions with data subjects.
Privacy policy	(i) Does your privacy policy describe all categories of data subjects, and data, the	(i) Do data mapping and update the policy so that the details of the

		processing activities in respect of each processing purpose?		processing are disclosed, in respect of each purpose of processing.
	(ii)	Do you collect and process data online?	(ii)	Publish the privacy policy on each web page where personal data is collected.
Interactions with Roskomnadzor	(i)	Do you have procedures for investigations in the case of data breach and monitoring of potential data incidents?	(i)	Adopt, or update, the procedures of DPA notifications in the case of data breach and monitoring of potential data incidents.
	(ii)	Do your IT systems interact with the GosSOPKA?*	(ii)	Develop the procedure for interaction with the GosSOPKA
	(iii)	Do you have a policy, or procedures, for responding to requests of DPA?	(iii)	Make sure that the privacy policy, or separate policy, describes responding to requests of the Roskomnadzor.
Relations with the third party providers	(i)	Do you engage third party providers for collection of data? Do they localize personal data, when collecting?	(i)	Make sure that third party providers that collect data localize such data in Russia
	(ii)	Do data processing agreements include obligations to confirm the implementation of organizational and technical measures for data protection?	(ii)	Revise the agreements, with third parties, to include the new mandatory provisions.
Special categories of data	(i)	Do you collect biometric personal data when providing your services to data subjects?	(i)	Make sure that you provide services, despite any refusal of a data subject to provide consent to processing of biometric data (unless the data is necessary for provision of the services under the law).
	(ii)	Do you process data of minors?	(ii)	Revise consents and contracts if the biometric data, or data of minors, is processed.
Handling of security incidents	(i)	Do you have a person responsible for handling and	(i)	Appoint an official responsible for handling

** Hereinafter, such footnote means the action should be carried out under requirements, which are to be adopted by the relevant State authorities.*

	investigating personal data incidents? (ii) Do you have policies and procedures to detect, monitor and report security incidents?	and investigating personal data incidents. (ii) Adopt the policies describing the procedures, terms and responsibilities, with respect to monitoring and reporting security incidents in time, approve the form for incident reporting.
By March 1st. 2023		
Cross-border data transfers	(i) Have you appointed a DPO? (ii) Do you have accurate information about existing data flows and compliance with the cross-border data transfer rules? (iii) Is the information about cross-border data transfers in the registry of data controllers? (iv) Have you assessed the adequacy of the regulation of data protection, in the recipient jurisdiction, if personal data is / will be transferred to other jurisdictions? (v) Have you filed the notification of the cross-border transfer before March 1st 2023?	(i) Appoint DPO. (ii) Complete a data mapping exercise with respect to cross-border data flows, adopt internal guidance on measures, procedures and responsibilities, aimed at compliance with cross-border data transfer rules. (iii) Submit a notice on registration with Roskomnadzor, or notice of amendments of the information, in the register, with respect to cross-border data transfers. (iv) Collect and assess information, about measures taken to protect personal data, by the recipient data controller and the regulation of data protection in any inadequate jurisdiction (if you transfer, or plan, transfers to such inadequate jurisdictions) and develop the form of the document confirming the assessment. (v) Submit a cross-border transfer notification by March 1st 2023.
Assessment of potential data subject harm	(i) Have you assessed the harm that can be caused to data	(i) Develop and adopt the policy providing for the procedures to access potential harm to data subjects' rights, implement

		subjects' rights, in case of a data breach? *		the forms and procedures for hard assessment.
Data deletion	(i)	Do you have procedures of personal data deletion? *	(i)	Adopt, or update, the policy on the personal data deletion.
	(ii)	Have templates of documents, confirming the deletion of personal data, been developed?	(ii)	Develop templates for confirming any personal data deletion.

We hope that the information provided herein will be useful for you. If any of your colleagues would like to receive our newsletters, please send them the link to complete a Subscription Form. 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

E: mostashenko@alrud.com

Sincerely,
ALRUD Law Firm

Hereinafter, such footnote means the action should be carried out under requirements which are to be adopted by the relevant State authorities.