Yandex Cloud

Customer actions to protect personal data in their clouds

When clients host their data in Yandex.Cloud, Yandex is obligated to fulfill legal requirements regarding personal data security. The customer remains the data owner and must perform all duties attributed to the data operator (such as acquiring consent to process personal data, inform Roskomnadzor about the processing of personal data, and form the threat model on their personal data information systems).

The actions of the data operator concerning personal data protection can be divided into:
— Creating the descriptive and procedural documents required by law.
— Implementing technical security measures for systems running on the cloud infrastructure.

Clients can fulfill these requirements on their own or request assistance from a Yandex.Cloud security partner:
— B-152 (in Russian),
— Card Security.

If a client appeals to a Yandex.Cloud partner for assistance, employees from the partner organization provide detailed instructions. If a client wishes to fulfill these requirements on their own, they can look at the following checklist:

1. Evaluate the business processes under which personal data is processed. Determine the objective of processing data, the contents of the personal data, the order in which personal data is processed, and where and how personal data is stored. Determine the legal grounds for processing personal data.

2. Assess any potential harm to personal data subjects and conduct threat modeling of the personal data security in the personal data information systems.

3. Determine the level of security of the personal data information system pursuant to the requirements of Resolution No. 1119 of the Russian Federal Government.

4. Appoint an employee to oversee the processing of personal data.

5. Design measures to fulfill the requirements of Order No. 21 of FSTEC of Russia. For example, the following security measures can be applied to implement level-3 security:
   — Configure authentication tools inside virtual machines (at the OS, DBMS, and software application level).
   — Control user access to virtual machines (at the OS, DBMS, and software application level).
   — Log security events (at the OS, DBMS, and software application level).
   — Provide anti-virus protection for virtual machines.
   — Perform vulnerability analyses and install security updates on OS, DBMS, and software applications.
   — Ensure that data is protected from disclosure and modification when transmitted over the internet.
   — Manage changes inside virtual machines.

6. Document and implement selected security measures and periodically monitor their implementation.

7. Develop a set of local documents (policies, regulations, and instructions) that regulate the processing and protection of personal data within the organization.

8. Publish personal data processing policies on the organization's websites and in mobile applications.

9. Have employees and third-parties sign forms of consent (when necessary) to the processing of their personal data.

10. If necessary, submit a notification to Roskomnadzor about personal data processing.

11. Keep documentation on personal data up-to-date.