

Approved

by the General Director of First Genetics JSC

Kuznetsov N.A.

Order dated 05/22/2025 No. 6



REGULATION
"First Genetics" JSC (Moscow)
On the processing and protection of personal data of employees (other persons)

1. General Provisions

1.1. This Regulation is a local regulatory act of First Genetics JSC (hereinafter referred to as the Company), adopted taking into account the requirements of, in particular, Chapter 14 of the Labor Code of the Russian Federation, Federal Law No. 152-FZ dated July 27, 2006 "On Personal Data" (hereinafter referred to as the "the Law on Personal Data").

1.2. The Regulation establishes:

- the purpose, procedure and conditions for processing personal data;
- the categories of subjects whose personal data are processed, categories (lists) of personal data processed, methods, terms of their processing and storage, the procedure for destroying such data upon achieving the processing goals or upon the occurrence of other legal grounds;
- provisions concerning the protection of personal data, procedures aimed at identifying and preventing violations of Russian legislation in the field of personal data, and eliminating the consequences of such violations.

1.3. The Regulation uses terms and definitions in accordance with their meanings defined in the Law on Personal Data.

1.4. The Regulation comes into force from the moment of its approval by the General Director and is valid until it is cancelled by order of the General Director or until a new Regulation is introduced.

1.5. Amendments to the Regulation are made by order of the General Director. Amendments come into force from the moment the relevant order is signed.

2. Categories of personal data subjects

2.1. The subjects whose personal data are processed by the Company in accordance with the Regulation include:

- candidates for employment with the Company;
- employees of the Company;
- former employees of the Company;
- family members of the Company's employees - in cases where, in accordance with the law, information about them is provided by the employee;
- other persons whose personal data the Company is obliged to process in accordance with labor legislation and other acts containing labor law standards.

3. Purposes of personal data processing, categories (lists) of personal data processed

3.1. According to the Regulation, personal data are processed for the purpose of applying and enforcing labor legislation within the framework of labor and other directly related relationships, including:

- assisting in employment;
- maintaining personnel and accounting records;
- assisting employees in obtaining education and career advancement;
- processing awards and incentives;
- provision by the Company of working conditions, guarantees and compensations established by law;
- filling out and submitting to authorized bodies the required reporting forms;
- ensuring the personal safety of employees and the safety of property;

- exercising control over the quantity and quality of work performed.

3.2. In accordance with the purpose specified in paragraph 3.1 of the Regulation, the following personal data are processed in the Company:

- last name, first name, patronymic (if any), as well as the previous last name, first name, patronymic (if any), date and place of their change (in case of change);
- gender;
- date (day, month, year) and place of birth;
- photograph;
- citizenship information;
- type, series, number of the identity document, name of the issuing authority, date of issue;
- insurance number of an individual personal account ("SNILS");
- individual taxpayer number ("INN");
- address and date of registration at the place of residence (place of stay), address of actual residence;
- contact telephone number, email address and (or) information on other methods of communication;
- details of certificates of state registration of acts of civil status and the information contained therein;
- information on marital status, family composition (degree of kinship, last name, first name, patronymic (if any), date (day, month, year) and place of birth);
- information on education and (or) qualifications or availability of special knowledge (including the name of the educational and (or) other organization, year of graduation, level of education, qualifications, details of the document on education, training);
- information on proficiency in foreign languages;
- information on attitude to military service, military registration and details of military registration documents (series, number, date of issue of the document, name of the authority that issued it);
- information on work experience, as well as information on previous places of work, periods and length of service;
- information contained in documents granting the right to stay and work in the territory of the Russian Federation (for foreign citizens staying in the Russian Federation);
- information contained in a temporary residence permit, a temporary residence permit for the purpose of obtaining an education (for foreign citizens temporarily residing in the Russian Federation), a residence permit (for foreign citizens permanently residing in the Russian Federation);
- information on income, obligations under enforcement documents;
- bank account numbers, bank card numbers;
- information on the state of health (for certain categories of employees);
- information on the presence (absence) of a criminal record and (or) the fact of criminal prosecution or the termination of criminal prosecution on rehabilitating grounds (for certain categories of employees);
- other personal data contained in documents, the submission of which is required by law, if the processing of this data corresponds to the purpose of processing provided for in paragraph 3.1 of the Regulation;
- other personal data that the employee wished to provide about himself and the processing of which corresponds to the purpose of processing provided for in paragraph 3.1 of the Regulation.

3.3. The Company does not process special categories of personal data related to race, nationality, political views, religious or philosophical beliefs, intimate life, except in cases stipulated by the legislation of the Russian Federation.

4. Procedure and conditions for personal data processing

4.1. Before starting to process personal data, the Company is obliged to notify Roskomnadzor of its intention to process personal data.

4.2. The legal basis for processing personal data is the Labor Code of the Russian Federation, other regulatory legal acts containing labor law standards, Federal Law No. 152-FZ dated July 27, 2006 "On Personal Data", Federal Law No. 402-FZ dated December 6, 2011 "On Accounting", Resolution of the Government of the Russian Federation No. 719 dated November 27, 2006 "On Approval of the Regulation on Military Registration".

4.3. Personal data is processed in compliance with the principles and conditions stipulated by the legislation in the field of personal data and these Regulations.

4.4. Personal data is processed in the Company in the following ways:

- non-automated processing of personal data;

- automated processing of personal data with or without transfer of the received information via information and telecommunications networks;
- mixed processing of personal data.

4.5. The processing of personal data in the Company is carried out with the consent of the personal data subject to the processing of his/her personal data, unless otherwise provided by the legislation in the field of personal data.

4.5.1. The processing of personal data permitted by the personal data subject for distribution is carried out in compliance with the prohibitions and conditions stipulated by Art. 10.1 of the Law on Personal Data.

Consent to the processing of such personal data is drawn up separately from other consents to the processing of personal data. Consent is provided by the personal data subject in person or in the form of an electronic document signed with an electronic signature, using the information system of Roskomnadzor.

4.5.2. The processing of biometric personal data is permitted only with the written consent of the personal data subject. Exceptions are situations stipulated by Part 2 of Art. 11 of the Law on Personal Data.

4.6. The Company does not carry out cross-border transfer of personal data.

4.7. Personal data shall be processed by collecting, recording, systematizing, accumulating, storing, clarifying (updating, changing), retrieving, using, depersonalizing, blocking, deleting, destruction of personal data, including by means of computer technology.

4.7.1. The Company shall collect, record, systematize, accumulate and clarify (update, change) personal data by means of:

- obtaining original documents or their copies;
- copying original documents;
- entering information into accounting forms on paper and electronic media;
- creating documents containing personal data on paper and electronic media;
- entering personal data into personal data information systems.

4.7.2. The Company shall use the following information systems:

- corporate e-mail;
- electronic document management system;
- user workstation support system;
- reference information system;
- personnel management system;
- remote access control system;
- information portal.

4.8. Transfer (distribution, provision, access) of personal data of personal data subjects is carried out in cases and in the manner stipulated by the legislation in the field of personal data and the Regulation.

5. Personal data processing and storage periods

5.1. The processing of personal data in the Company shall be terminated in the following cases:

- upon detection of the fact of unlawful processing of personal data. The processing termination period shall be within three working days from the date of detection of such fact;
- upon achievement of the purposes of their processing (with some exceptions);
- upon expiration of the validity period or upon revocation by the subject of personal data of consent to the processing of their personal data (with some exceptions), if, in accordance with the Law on Personal Data, their processing is permitted only with consent;
- upon application by the subject of personal data to the Company with a request to terminate the processing of personal data (except for the cases stipulated by Part 5.1 of Article 21 of the Law on Personal Data). The processing termination period shall be no more than 10 working days from the date of receipt of the request (with the possibility of extension for no more than five working days if notification of the reasons for the extension is sent).

5.2. Personal data shall be stored in a form that allows identification of the subject of personal data for no longer than required by the purposes of their processing. Exceptions are cases when the storage period of personal data is established by federal law, an agreement to which the subject of personal data is a party (beneficiary or guarantor).

5.3. Personal data on paper media are stored in the Company for the storage periods of documents for which these periods are provided for by the legislation on archival affairs in the Russian Federation (Federal Law dated October 22, 2004 No. 125-FZ "On Archival Affairs in the Russian Federation", the List of standard

management archival documents generated in the course of activities of state bodies, local governments and organizations, indicating the periods of their storage (approved by the Order of Rosarchive dated December 20, 2019 No. 236)).

5.4. The storage period of personal data processed in personal data information systems corresponds to the storage period of personal data on paper media.

6. Procedure for blocking and destruction of personal data

6.1. The Company blocks personal data in the manner and under the conditions stipulated by the legislation in the field of personal data.

6.2. Upon achieving the goals of personal data processing or in the event of loss of the need to achieve these goals, personal data are destroyed or anonymized. An exception may be provided for by federal law.

6.3. Illegally obtained personal data or those that are not necessary for the purpose of processing are destroyed within 7 working days from the date of submission of supporting information by the subject of personal data (his/her representative).

6.4. Personal data, the processing of which is terminated due to its illegality and the legality of the processing of which cannot be ensured, are destroyed within 10 working days from the date of detection of the fact of illegal processing.

6.5. Personal data shall be destroyed within 30 days from the date of achieving the processing purpose, unless otherwise provided by an agreement to which the personal data subject is a party (beneficiary or guarantor), or another agreement between him/her and the Company, or if the Company has no right to process personal data without the consent of the personal data subject on the grounds provided for by federal laws.

6.5.1. Upon reaching the maximum storage periods for documents containing personal data, personal data shall be destroyed within 30 days.

6.6. Personal data shall be destroyed (if their preservation is not required for the purposes of processing personal data) within 30 days from the date of receipt of the personal data subject's revocation of consent to their processing. Otherwise, may be provided by an agreement to which the personal data subject is a party (beneficiary or guarantor), or another agreement between him/her and the Company. In addition, personal data shall be destroyed within the specified period if the Company has no right to process them without the consent of the personal data subject on the grounds provided for by federal laws.

6.7. The selection of tangible media (documents, hard drives, flash drives, etc.) and (or) information in information systems containing personal data that are subject to destruction is carried out by the Company's divisions processing personal data.

6.8. The destruction of personal data is carried out by a commission created by the order of the General Director.

6.8.1. The commission compiles a list indicating the documents, other tangible media and (or) information in information systems containing personal data that are subject to destruction.

6.8.2. Personal data on paper media are destroyed using a shredder. Personal data on electronic media are destroyed by mechanically violating the integrity of the media, preventing the personal data from being read or restored, as well as by deleting data from electronic media using methods and means of guaranteed removal of residual information.

6.8.3. The commission confirms the destruction of personal data specified in paragraphs 6.4, 6.5, 6.6 of the Regulation, in accordance with the Requirements for confirmation of the destruction of personal data approved by the Order of Roskomnadzor dated October 28, 2022 No. 179, namely:

- an act on the destruction of personal data - if the data is processed without the use of automation;
- an act on the destruction of personal data and unloading from the event log in the personal data information system - if the data is processed using automation tools or simultaneously with and without the use of such tools.

The act can be drawn up on paper or in electronic form signed with electronic signatures.

The forms of the act and the unloading from the log, taking into account the information that must be contained in the specified documents, are approved by the order of the General Director.

6.8.4. After drawing up the act on the destruction of personal data and unloading from the event log in the personal data information system, the commission transfers them to the general department for subsequent storage. Acts and log downloads are stored for three years from the moment of destruction of personal data.

6.8.5. Destruction of personal data not specified in paragraph 6.8.3 of the Regulation is confirmed by an act, which is drawn up immediately after the destruction of such data. The form of the act is approved by order of the General Director.

7. Protection of personal data. Procedures aimed at preventing and detecting violations of legislation, eliminating the consequences of such violations

7.1. Without the written consent of the personal data subject, the Company does not disclose to third parties or distribute personal data, unless otherwise provided by federal law.

7.1.1. It is prohibited to disclose and distribute personal data of personal data subjects by telephone.

7.2. In order to protect personal data, the following are appointed (approved) by orders of the General Director of the Company:

- an employee responsible for organizing the processing of personal data;
- a list of positions for which personal data is processed;
- a list of personal data to which employees holding positions involving the personal data processing have access;
- the procedure for access to premises where personal data is processed;
- the procedure for transferring personal data within the Company;
- a form of consent to the processing of personal data, a form of consent to the processing of personal data permitted by the personal data subject for distribution;
- the procedure for protecting personal data when processing them in personal data information systems;
- the procedure for conducting internal investigations and inspections;
- other local regulations adopted in accordance with the requirements of legislation in the field of personal data.

7.3. Employees who hold positions that involve the processing of personal data are allowed to do so after signing a non-disclosure agreement.

7.4. Personal data storage media are stored in cabinets that are locked with a key. The Company's premises where they are located are equipped with locking devices. Keys to cabinets and premises are issued against signature.

7.5. Access to personal information contained in the Company's information systems is provided using individual passwords.

7.6. The Company uses certified anti-virus software with regularly updated databases.

7.7. The Company's employees who process personal data periodically undergo training in the requirements of legislation in the field of personal data.

7.8. The job descriptions of the Company's employees who process personal data include, in particular, provisions on the need to report any cases of unauthorized access to personal data.

7.9. The Company conducts internal investigations in the following situations:

- in case of unlawful or accidental transfer (provision, distribution, access) of personal data, resulting in the violation of the rights of personal data subjects;
- in other cases, stipulated by the legislation in the field of personal data.

7.10. The employee responsible for organizing the processing of personal data carries out internal control:

- over compliance by employees authorized to process personal data with the requirements of the legislation in the field of personal data, local regulations;
- over compliance of the said acts with the requirements of the legislation in the field of personal data.

Internal control is carried out in the form of internal audits.

7.10.1. Internal scheduled audits are carried out on the basis of an annual plan approved by the General Director.

7.10.2. Internal unscheduled audits are carried out by decision of the employee responsible for organizing the processing of personal data. The basis for them is information about a violation of the legislation in the field of personal data, received orally or in writing.

7.10.3. Based on the results of the internal audit, a report is issued to the General Director. If violations are identified, the document provides a list of measures to eliminate them and the corresponding deadlines.

7.11. An internal investigation is conducted if a fact of illegal or accidental transfer (provision, distribution, access) of personal data is revealed, resulting in a violation of the rights of personal data subjects (hereinafter referred to as an incident).

7.11.1. In the event of an incident, the Company shall notify Roskomnadzor within 24 hours:

- about the incident;
- its presumed causes and the harm caused to the rights of the subject (several subjects) of personal data;
- measures taken to eliminate the consequences of the incident;
- a representative of the Company who is authorized to interact with Roskomnadzor on issues related to the incident.

When sending a notification, a representative must be guided by the Procedure and conditions for interaction between the Federal Service for Supervision of Communications, Information Technology and Mass Media and operators in the context of maintaining a register of incidents in the field of personal data, approved by Order of Roskomnadzor dated November 14, 2022 No. 187.

7.11.2. Within 72 hours, the Company is obliged to do the following:

- notify Roskomnadzor of the results of the internal investigation;
- provide information about the persons whose actions caused the incident (if any).

When sending a notification, a representative must also be guided by the Procedure and conditions for interaction between the Federal Service for Supervision of Communications, Information Technology and Mass Media and operators in the context of maintaining a register of incidents in the field of personal data, approved by Order of Roskomnadzor dated November 14, 2022 No. 187.

7.12. If the personal data subject (his/her representative) provides confirmed information that the personal data are incomplete, inaccurate or outdated, changes will be made to them within 7 business days. The Company will notify the personal data subject (his/her representative) in writing of the changes made and notify (by e-mail) of them to third parties to whom the personal data were transferred.

7.13. The Company will notify the personal data subject (his/her representative) of the elimination of violations regarding the illegal processing of personal data. Roskomnadzor will also be notified if it has sent a request from the personal data subject (his/her representative) or has made a request itself.

7.13.1. In the event of destruction of personal data that was processed illegally, the notification will be sent in accordance with paragraph 7.13 of the Regulation.

7.14. In the event of destruction of personal data that was illegally obtained or is not necessary for the stated purpose of processing, the Company shall notify the subject of the personal data (his/her representative) of the measures taken in writing. The Company shall also notify third parties to whom such personal data were transferred by e-mail.

8. Liability for violation of the rules governing the processing of personal data

8.1. Persons guilty of violating the provisions of the Russian Federation legislation in the field of personal data when processing personal data shall be subject to disciplinary and financial liability in the manner established by the Labor Code of the Russian Federation and other federal laws. In addition, they shall be subject to administrative, civil or criminal liability in the manner established by federal laws.

8.2. Moral damage caused to the subject of personal data due to the violation of his rights, violation of the rules for personal data processing, as well as failure to comply with the requirements for their protection established by the Law on Personal Data, shall be subject to compensation in accordance with the legislation of the Russian Federation. Compensation for moral damage is carried out regardless of compensation for property damage and losses incurred by the subject of personal data.