ASSIGNMENT FOR PROCESSING PERSONAL DATA

One Party, acting as the Data Controller under the Federal Law of the Russian Federation No. 152-FZ "On Personal Data" dated July 27, 2006 (hereinafter referred to as the "Law"), hereby instructs the other Party (hereinafter referred to as the "Receiving Party") to process personal data.

The Receiving Party is designated as the Data Processor, acting on behalf of the Data Controller (hereinafter referred to as the "Controller").

The processing of personal data by the Receiving Party on behalf of the Controller is carried out for the purpose of proper fulfillment of the Agreement. Prior to assigning the processing of personal data, the Controller must obtain consent from the data subjects for the processing and transfer of their personal data to a third party (the Receiving Party). The list of purposes for which personal data is transferred to the third party, as well as the specific actions (operations) to be performed with the personal data on behalf of the Controller, shall be communicated by the Controller to the Receiving Party in the form provided by the Controller.

Assignment

Purpose of Personal Data Processing	Actions (Operations) with Personal Data	List of Personal Data Assigned for Processing
Here, specify the purposes for which the personal data is being transferred to the third party (e.g., to ensure information interaction, such as the functioning of IT infrastructure).	*For example: collection; recording; systematization; accumulation; storage; updating (amendment, modification); retrieval; transfer (provision, distribution, access); use; blocking; deletion; destruction.*	*Other personal data: surname, first name, patronymic; position; department; address; email address; IP address of workstation; mobile phone number; work phone number; photo.*

The Receiving Party, when processing personal data on behalf of the Data Controller, may perform the following actions (operations), whether using automated means or without such means: collection, recording, systematization, accumulation, storage, updating (amendment, modification), retrieval, use, transfer (provision, access), anonymization, blocking, deletion, and destruction.

The list of necessary actions (operations) with personal data to be performed under the assignment is specified by the Data Controller in the Assignment. The Assignment is considered accepted and agreed upon by the parties from the date the Data Controller sends the Assignment

to the Receiving Party's email address, as indicated in the Agreement in the contact details for electronic communication.

Upon receiving the Assignment for personal data processing, the Receiving Party is required to send the Data Controller a confirmation of receipt within two (2) business days. The failure of the Receiving Party to send a confirmation of receipt of the Assignment does not constitute grounds for refusing to fulfill the obligations agreed upon by the Parties in this document.

Collection of Personal Data by Assignment

1. In cases where the assignment involves the processing of personal data through their collection from data subjects based on their consent for the processing of personal data (Clause 1, Part 1, Article 6 of the Law), the Data Controller is obligated to provide the Receiving Party with the form of such consent.

2. Upon request by the Data Controller and no later than 10 days, the Receiving Party shall provide confirmation that consent for the processing of personal data has been obtained from the data subjects whose personal data were collected.

3. The Parties agree that the confirmation of obtaining consent for the processing of personal data shall be the written consents signed by the data subjects.

4. In the event of the termination of the Assignment or the contract, the Receiving Party shall provide confirmation of having obtained all consents for the processing of personal data from the data subjects whose personal data were collected throughout the entire term of this Agreement.

Measures for Compliance with Legal Requirements

5. When processing personal data under the assignment, the Receiving Party is obligated to adhere to the principles established in Article 5 of the Law, maintain the confidentiality of personal data, and ensure their security.

6. The Receiving Party, in processing personal data, is required to take the necessary and sufficient measures to fulfill the obligations prescribed by the legislation of the Russian Federation, as outlined in Article 18.1 of the Law:

6.1. Appoint a person responsible for organizing the processing of personal data;

6.2. Issue documents that define the policy regarding the processing of personal data, and internal regulations on personal data processing in accordance with Clause 2, Part 1, Article 18.1 of the Law;

6.3. Conduct internal control and/or audits to ensure compliance of personal data processing with the Law and the regulatory legal acts adopted pursuant to it, as well as the

requirements for personal data protection, the Receiving Party's policy on personal data processing, and internal regulations;

6.4. Assess the potential harm that may be caused to personal data subjects in case of a violation of the Law, and evaluate the correlation between this harm and the measures taken to ensure compliance with the obligations prescribed by the Law;

6.5. Familiarize employees directly involved in the processing of personal data with the provisions of the legislation of the Russian Federation on personal data, including the requirements for personal data protection, the documents defining the policy regarding personal data processing, internal regulations on personal data processing, and/or provide training for these employees.

Requirements for Personal Data Protection

7. The Parties are obligated to comply with the requirements for the protection of personal data being processed, in accordance with Article 19 of the Law:

7.1. Identify the security threats to personal data assigned for processing if they are to be processed in personal data information systems;

7.2. In cases where the assigned personal data is processed in personal data information systems, determine the level of protection for personal data during their processing in such systems and comply with the requirements set forth in the Resolution of the Government of the Russian Federation No. 1119 dated November 1, 2012, "On Approval of Requirements for the Protection of Personal Data During Their Processing in Personal Data Information Systems";

7.3. Assess the potential harm to the data subject during the processing of their personal data, which has been assigned for processing, in the event of security threats to the personal data;

7.4. Use information protection measures that have undergone the established conformity assessment procedure;

7.5. Evaluate the effectiveness of the measures taken to ensure the security of the personal data assigned for processing before the commissioning of the personal data information system;

7.6. Maintain records of machine-readable media containing personal data if the assigned personal data is recorded on them;

7.7. Detect incidents of unauthorized access to the personal data assigned for processing and take the necessary measures in response;

7.8. Restore personal data that has been modified or destroyed due to unauthorized access;

7.9. Establish rules for accessing personal data that is assigned for processing and processed in personal data information systems, as well as ensure the registration and accounting of all actions performed with the personal data in the personal data information system;

7.10. Monitor the measures taken to ensure the security of personal data and the level of protection of the personal data information systems in which the assigned personal data is processed.

8. When collecting personal data, including via the Internet, the Receiving Party is required to ensure the recording, systematization, accumulation, storage, updating (amendment, modification), and retrieval of personal data of citizens of the Russian Federation using databases located within the territory of the Russian Federation, except in cases provided by law.

Confirmation of the Receiving Party's Compliance with Obligations Established in the Agreement

9. Throughout the term of this Agreement, the Data Controller is entitled to request, and the Receiving Party is obligated to provide within 10 business days from the date of receiving the request, information (including documents) confirming the adoption of measures and compliance with the requirements established by this document and the legislation of the Russian Federation for the purpose of fulfilling the assignment.

10. In the event that there is an unauthorized or accidental transfer (provision, distribution, access) of personal data that results in a violation of the rights of personal data subjects, the Receiving Party is obligated, upon identifying such an incident, to notify the Data Controller:

10.1. Without undue delay / within 12 hours,

10.1.1 About the incident, including a list of personal data, categories of personal data subjects, the number of data subjects affected by the incident;

10.1.2 About the presumed causes that led to the violation of the rights of personal data subjects;

10.1.3 About the presumed harm caused to the rights of personal data subjects;

10.1.4 About the measures taken to eliminate the consequences of the incident;

10.1.5 About the person authorized by the Receiving Party to respond to and investigate the incident;

10.2. Within 48 hours, provide the results of the internal investigation of the identified incident, as well as information about the individuals whose actions caused the incident (if available).

Destruction of Personal Data

11. Upon request from the Data Controller, the Receiving Party must destroy the specific personal data identified by the Controller, or all personal data assigned to it for processing, within 15 calendar days from the date of receiving the request, provided that the processing of such data is not required under the legislation of the Russian Federation.

12. The Data Controller has the right, throughout the term of this Agreement, to request copies of documents from the Receiving Party, as well as documents containing records of events in the Receiving Party's personal data information systems, confirming the destruction of the personal data transferred to it for processing. Copies of such documents must be provided no later than 5 business days from the date of receiving the corresponding request.

13. If it is not possible to destroy the personal data within 15 calendar days from the receipt of the request, the Receiving Party shall block such personal data and ensure their destruction within a period not exceeding 6 months. The fact of blocking must be reported to the Data Controller within 15 calendar days from the date of receiving the request.

14. If it is not possible to destroy the personal data as requested due to the necessity of processing it in compliance with the requirements of the legislation of the Russian Federation, the Receiving Party shall provide a reasoned justification for the inability to destroy or block the personal data within 15 calendar days from the date of receiving the request from the Controller.

Subcontracting of Personal Data Processing

15. The Data Controller permits the Receiving Party to subcontract the processing of personal data to third parties (hereinafter referred to as "Subcontractors").

16. The subcontracting of personal data processing is possible under the following conditions:

16.1. Notification of the Data Controller via the email address specified in the Agreement about the possibility of subcontracting the processing of personal data to a Subcontractor at least 15 (fifteen) business days before the actual engagement of the Subcontractor. The notification must include the name of the third party, its Taxpayer Identification Number (INN), location address, contact phone number, and email address;

16.2. The engagement of Subcontractors for the processing of personal data shall be carried out by their properly documented accession to the Agreement and only under the condition of their unconditional acceptance of all provisions of the Agreement in its current version;

16.3. Before commencing the execution of the Agreement, Subcontractors are required to implement all security measures (legal, organizational, and technical) necessary for the processing of personal data as stipulated in the Agreement.

Liability of the Parties

17. In accordance with Part 5 of Article 6 of the Law, the Data Controller bears sole responsibility to the personal data subjects whose personal data is processed, while the Receiving Party, processing personal data under the assignment, is responsible to the Data Controller.

18. If the rights of the personal data subjects, whose personal data were assigned to the Receiving Party, are violated, resulting in damage to the Data Controller, the Receiving Party is obligated to compensate such damage within 30 (thirty) calendar days from the date of receiving the relevant written demand.