

PERSONAL DATA PROTECTION AND PROCESSING POLICY

of SKET-Group Limited Liability Company
(hereinafter referred to as "SKET-Group LLC")

1. General Provisions

1.1. This Policy of SKET-Group Limited Liability Company regarding the processing of personal data (hereinafter referred to as the "Policy") has been developed in compliance with the requirements of Clause 2, Part 1, Article 18.1 of Federal Law No. 152-FZ dated July 27, 2006, "On Personal Data" (hereinafter referred to as the "Personal Data Law"), to ensure the protection of human and civil rights and freedoms when processing their personal data, including the rights to privacy, personal, and family secrets.

1.2. The Policy applies to all personal data processed by SKET-Group Limited Liability Company (hereinafter referred to as the "Operator" or "SKET-Group LLC").

1.3. The Policy governs relations in the field of personal data processing that arose for the Operator both before and after the approval of this Policy.

1.4. In compliance with Part 2, Article 18.1 of the Personal Data Law, this Policy is published in free access on the Operator's website on the Internet.

2. Terms and Definitions

Personal Data (PD) – Any information relating to a directly or indirectly identified or identifiable individual (data subject).

Personal Data Permitted for Dissemination by the Data Subject – Personal data to which access by an unlimited number of persons has been granted by the data subject through consent to the processing of personal data permitted for dissemination.

Personal Data Operator (Operator) – A state body, municipal body, legal entity, or individual that independently or jointly with others organizes and/or processes personal data, as well as determines the purposes of processing, the composition of personal data to be processed, and the actions (operations) performed with personal data.

Processing of Personal Data – Any action (operation) or set of actions (operations) performed with personal data, with or without automation tools. Processing includes:

- Collection
- Recording
- Systematization
- Accumulation
- Storage
- Updating (modification)
- Retrieval
- Use
- Transfer (provision, access)
- Dissemination
- Depersonalization
- Blocking
- Deletion
- Destruction

Automated Processing of Personal Data – Processing using computer technology.

Provision of Personal Data – Actions aimed at disclosing personal data to a specific person or group of persons.

Blocking of Personal Data – Temporary suspension of processing (except where processing is necessary to clarify personal data).

Destruction of Personal Data – Actions making it impossible to restore PD in the information system or resulting in the destruction of physical storage media.

Depersonalization of Personal Data – Actions making it impossible to determine the belonging of PD to a specific data subject without additional information.

Personal Data Information System (PDIS) – A set of personal data contained in databases and processed using information technologies and technical means.

Cross-Border Transfer of Personal Data – Transfer of PD to a foreign state's authority, foreign individual, or legal entity.

3. Procedure and Conditions for Processing and Storing Personal Data

3.1. The Operator processes PD in accordance with Russian legislation.

3.2. Processing is carried out with the data subject's consent or without it in cases permitted by law.

3.3. Consent for processing PD permitted for dissemination is obtained separately from other consents.

3.4. Such consent may be provided:

- Directly
- Through the authorized body's information system for protecting data subjects' rights.

3.5. The Operator processes PD both automatically and non-automatically.

3.6. Only employees whose duties include PD processing are allowed access.

3.7. Processing methods include:

- Collecting PD orally or in writing with consent
- Entering PD into logs, registers, and information systems
- Other lawful processing methods

3.8. Disclosure to third parties is prohibited without consent, unless required by law.

3.9. PD may be transferred to investigative bodies, the Federal Tax Service, Pension Fund, Social Insurance Fund, and other authorized entities as required by law.

3.10. The Operator implements legal, organizational, and technical measures to protect PD from unauthorized access, destruction, alteration, or dissemination, including:

- Identifying security threats
- Adopting internal regulations
- Appointing responsible personnel
- Ensuring secure storage conditions
- Training employees

3.11. PD is stored only as long as necessary for processing purposes, unless otherwise required by law.

3.12. Collection of PD via the Internet is conducted using databases located in Russia, unless exceptions apply.

3.13. Purposes of PD Processing:

- Compliance with Russian laws
- Conducting business per SKET-Group LLC's charter
- HR record-keeping
- Employee support (employment, education, safety)
- Recruitment

- Pension insurance registration
 - Reporting to authorities
 - Civil law relations
 - Accounting
 - Access control
- 3.14. Employee PD is processed only to ensure legal compliance.
- 3.15. Categories of Data Subjects:
- Current/former employees
 - Job applicants
 - Contractors
- 3.16. Processed PD Includes:
- Employment-related data
 - Recruitment data
 - Contractual relationship data
- 3.17. Storage of PD:
- On paper (in locked cabinets/rooms) or electronically
 - Automated PD is stored in separate folders
 - Open electronic storage is prohibited
 - PD is destroyed when no longer needed
- 3.18. Destruction of PD:
- Paper documents: Shredding, burning, etc.
 - Electronic data: Erasure/formatting
 - Destruction is documented
 -

4. Personal Data Protection

- 4.1. The Operator has established a PD protection system (PDPS) comprising legal, organizational, and technical safeguards.
- 4.2. Legal safeguards include regulatory documents governing PDPS.
- 4.3. Organizational safeguards cover access control and personnel management.
- 4.4. Technical safeguards involve software/hardware solutions.
- 4.5. Key Protection Measures:
- Appointing a PD officer
 - Threat assessment and mitigation
 - Access control with individual passwords
 - Certified antivirus software
 - Employee training
 - Internal audits
 -

5. Rights of Data Subjects and Operator's Obligations

- 5.1. Data Subject Rights:
- Access to their PD
 - Confirmation of processing
 - Information on processing purposes/methods
 - Details on the Operator and third-party access
 - Right to request corrections/blocking/destruction
- 5.2. Operator's Obligations:
- Provide processing information upon collection
 - Notify if PD was obtained indirectly
 - Publish this Policy openly

- Implement PD protection measures
- Respond to data subjects' requests

6. Updating, Correcting, Deleting, and Destroying PD; Responding to Access Requests

6.1. The Operator provides processing details upon request, subject to verification. Requests must include:

- ID details
- Proof of relationship with the Operator
- Signature

6.2. Inaccurate PD is blocked during verification and corrected within 7 days if confirmed.

6.3. Unlawful processing is blocked upon request.

6.4. PD is destroyed when:

- Processing purposes are achieved
- Consent is withdrawn (unless legal exceptions apply)