

JSC Insurance Company Unison



**PERSONAL DATA
PROTECTION POLICY**



Personal Data Protection Policy

JSC Insurance Company Unison

Identification Code	404393152
Legal Address	19 D. Gamrekeli St., Tbilisi
Email	unison@unison.ge
Telephone	+995 32 2 991 991
Last Updated	7 August 2026

Purpose of the Document

This Policy explains how the Company collects, uses, stores, shares and protects personal data, the legal bases on which processing is carried out, and how a data subject may exercise the rights granted by law.

This Policy has been prepared in accordance with the current Law of Georgia on Personal Data Protection.

TABLE OF CONTENTS

1. General Provisions and Company Status
2. Persons Covered by the Policy
3. Sources of Personal Data
4. Categories of Data
5. Purposes of Data Processing
6. Legal Bases for Data Processing
7. Special Categories of Data
8. Data Transfer and Recipients
9. International Data Transfers
10. Direct Marketing
11. Video and Audio Monitoring
12. Data Security
13. Data Retention Periods
14. Rights of the Data Subject
15. Data Protection Officer
16. Supervisory Authority and Right to Appeal
17. Updates to the Policy

1. GENERAL PROVISIONS AND COMPANY STATUS

This Policy describes the main rules governing the processing of personal data by JSC Insurance Company Unison (hereinafter referred to as "Unison", the "Company" or "we") and applies in cases where the Company determines the purposes and means of processing personal data.

In such cases, Unison acts as the "data controller". If, within a specific relationship, the Company processes data on behalf of and under the instructions of another person, its status may be that of a "data processor", and the relevant rights and obligations shall be determined by law and the applicable agreement.

Important Note

Reading this Policy does not, in itself, constitute consent to all types of data processing. Where the law requires the data subject's consent for processing, the Company obtains such consent separately, for a specific purpose, on an informed basis and in the form prescribed by law. In other cases, data are processed on another legal basis provided for by law.

Matters not covered by this Policy shall be governed by the applicable legislation of Georgia. In the event of any discrepancy between this Policy and a mandatory legal provision, the rule established by applicable legislation shall prevail.

2. PERSONS COVERED BY THE POLICY

This Policy may apply to the following natural persons:

- potential, current and former customers/insured persons of the Company;
- policyholders, beneficiaries and other persons connected with an insured event;
- customer representatives, contact persons and authorized persons;
- Company employees, job candidates, interns and former employees;
- users of the website, mobile/electronic services, hotline and other communication channels;
- other persons whose data must be processed for insurance activities, compliance with legal obligations, administration of claims/losses, or protection of the Company's legitimate interests.

3. SOURCES OF PERSONAL DATA

The Company may obtain personal data from:

- directly from the data subject — when submitting an application, proposal, contract, loss/claim notification, during a telephone conversation, written/electronic communication or a visit to the office;
- from the policyholder, insured person, beneficiary, representative or another authorized person;
- from medical/service providers, experts, assistance companies, reinsurers, brokers and other partners — where an appropriate legal basis exists;
- from state authorities, public registers, court/enforcement systems and other lawfully accessible sources;
- from technical and communication data generated when using the website, application and other electronic channels;
- from other third parties where obtaining the data is necessary for a specific lawful purpose and an appropriate legal basis exists.

4. CATEGORIES OF DATA

Depending on the type and purpose of the relationship, the Company processes only data that are necessary and proportionate for achieving the relevant purpose. Possible categories include:

CATEGORY	EXAMPLES
Identification Data	name, surname, date of birth, personal identification number, identity/travel document details, citizenship, signature, photograph;
Contact Data	address, telephone number, email address and other contact channels;
Insurance And Contractual Data	policy/contract details, insured object, information required for risk assessment, loss/claim materials, service history;
Property / Vehicle Data	characteristics of property, vehicles and other insured objects, including VIN/registration number and ownership-related data;
Financial Data	bank account details, payments, debts, indemnities, data on financial standing where necessary for the relevant product or lawful purpose;
Employment-Related Data	education, professional experience, position, remuneration, work schedule and other HR data;
Special Categories Of Data	health status and medical history; as well as other data defined by law as special categories, where their processing is necessary and an appropriate legal basis exists;
Audio-Visual Data	recordings of hotline/service calls, video monitoring recordings and, where necessary, photographic materials;
Electronic / Interactive Data	technical information related to use of the website or application, information entered by the user and the history of communications with the Company;
Public Data	information obtained from sources lawfully available to the public.

5. PURPOSES OF DATA PROCESSING

The Company may process data, including for the following purposes:

- offering insurance products, risk assessment, entering into, administering, renewing and terminating contracts;
- registration, investigation and assessment of insured events/losses, payment of indemnities, management of recourse/subrogation claims and handling of disputes;
- administration of services covered by health insurance and communication with providers;
- customer identification and the prevention/detection of fraud, money laundering and other unlawful activities within the limits established by law;
- management of payments, outstanding debts and financial settlements;
- communication with customers, review of applications/claims/complaints and improvement of service quality;
- protection of the Company's legal claims, interests and rights, including in judicial/administrative proceedings;
- fulfilment of statutory obligations, supervisory and audit requirements, reporting obligations and submission of requested information;
- ensuring information security, business continuity, physical security and protection of property;
- statistical, analytical and management reporting, using depersonalized/aggregated data where appropriate;
- direct marketing — only in compliance with the conditions established by law.

6. LEGAL BASES FOR DATA PROCESSING

The Company processes data only where a legal basis provided for by the Law of Georgia on Personal Data Protection exists. Depending on the specific processing activity, such basis may include:

- the data subject's consent;
- entering into or performing a contract/transaction;
- a case expressly provided for by law or performance of a statutory obligation imposed on the Company;
- protection of the vital interests of the data subject or another person;
- protection of an important public interest or performance of a task falling within a field of public interest as defined by law;
- protection of an important legitimate interest of the Company or a third party, provided that no overriding interest in protecting the rights of the data subject exists;
- review of an application submitted by the data subject or provision of services to the data subject;
- other grounds provided for by law.

For each processing activity, the Company ensures that the legal basis for processing is substantiated and that the principles of data minimization, purpose limitation and proportionality are observed.

7. SPECIAL CATEGORIES OF DATA

Due to the specific nature of insurance activities, particularly in health insurance, claims administration or the review of legal claims, the Company may process health-related data and other special categories of personal data.

Such data are processed only where the specific legal basis required by law exists and appropriate safeguards are in place to protect the rights and interests of the data subject. Written consent may constitute one such basis, but it is not the only possible basis.

8. RECEIPT / TRANSFER OF DATA

Where a specific purpose and legal basis exist, personal data may be transferred to the extent necessary for that purpose. Possible recipients of the data include:

- medical and other service providers, experts, assistance/claims administration companies;
- reinsurers, insurance/reinsurance brokers and other relevant participants in the insurance sector;
- banks, payment service providers, credit information bureaus and other financial service providers;
- IT, communications, hosting, archiving, courier and other service providers that process data on the Company's instructions and are subject to appropriate confidentiality/security obligations;
- auditors, legal advisers and other professional advisers;
- courts, enforcement authorities, law-enforcement, regulatory/supervisory and other authorized state bodies — in cases provided for by law;
- other persons where data transfer is necessary for performance of a contract, protection of a legal claim or on another lawful basis.

Where a third party processes data on behalf of Unison, the Company ensures that its relationship with the data processor is governed by the terms required by law and that appropriate data security safeguards are in place.

9. INTERNATIONAL DATA TRANSFERS

If, within a particular insurance, reinsurance, assistance, technological or other service, it becomes necessary to transfer data to another state or an international organization, the Company carries out such transfer only in compliance with the conditions established by Georgian legislation and with appropriate data protection safeguards, including, where required, on the basis of the relevant authorization of the State Audit Office of Georgia.

10. DIRECT MARKETING

Personal data are processed for direct marketing purposes only on the basis of the data subject's consent. For the processing of data other than the name, surname, address, telephone number and email address for direct marketing purposes, the Company obtains written consent where required by law.

The data subject may opt out of direct marketing at any time, free of charge and without providing any reason. The request may be made through the same channel used for marketing communications or by another available means, including by email to unison@unison.ge

The Company shall stop processing data for direct marketing purposes within a reasonable period after receiving the request, but no later than 7 business days. The fact and time of giving and withdrawing consent shall be recorded for the period prescribed by law.

11. VIDEO AND AUDIO MONITORING

The Company may conduct video monitoring for the safety of persons and property, prevention/detection of crime, protection of confidential information or another legitimate purpose permitted by law, only where and to the extent such monitoring is an adequate and proportionate means of achieving that purpose.

Audio recording of hotline calls and other relevant telephone communications may be carried out for service quality control, substantiation of disputes/factual circumstances, security or another lawful purpose. The data subject shall be informed of audio monitoring in accordance with the procedure established by law.

Access to video and audio recordings is limited to duly authorized persons, within the scope of their business need and granted access rights. Access and related actions are logged where required by applicable legislation and the Company's internal rules.

12. DATA SECURITY

The Company applies organizational and technical measures appropriate to the nature and volume of the data, the purposes of processing and the relevant risks, in order to protect personal data against unlawful or unauthorized processing, accidental loss, destruction, alteration, disclosure or damage.

- defining access rights according to roles and business need;
- logging actions performed on data in electronic systems where appropriate;
- confidentiality obligations for employees and data processors;
- information security, backup, access control and other appropriate mechanisms;
- periodic assessment and, where necessary, updating of security measures.

13. DATA RETENTION PERIODS

Personal data are retained only for the period necessary for the purpose for which they were processed, or for the period required by legislation/a legal requirement. When determining retention periods, the Company takes into account applicable insurance, civil, tax, accounting, anti-money laundering, consumer protection and other relevant legal requirements, as well as limitation periods for potential disputes or claims.

- video recordings are generally retained for the period determined by the technical system and the Company's internal rules, but no longer than 1 month, unless a longer retention period becomes necessary due to a specific incident, dispute or another lawful purpose;
- telephone recordings are retained for no longer than 5 years, unless a specific legal basis/purpose requires a shorter or different retention period;
- once the retention purpose has expired, the data are deleted, destroyed or depersonalized unless another legal basis exists for their continued retention.

14. RIGHTS OF THE DATA SUBJECT

Subject to the conditions and exceptions established by law, the data subject has the right to:

RIGHT	DESCRIPTION
Right To Information	to learn whether data concerning them are being processed, what data are processed, for what purpose and on what basis, how long they are retained, the source from which they were obtained and to whom they have been/may be disclosed;
Access To Data And Copies	to access personal data concerning them and receive copies within the scope provided for by law;
Rectification / Updating / Completion	to request rectification, updating or completion of incorrect, inaccurate or incomplete data;
Cessation Of Processing, Deletion Or Destruction	to request cessation of data processing, deletion or destruction where no exception or retention basis provided for by law applies;
Restriction / Blocking	to request temporary restriction of data processing in cases provided for by law;
Data Portability	in cases provided for by law and where technically feasible, to receive data provided by them in a structured format or request their transfer to another data controller;
Rights Relating To Automated Decision-Making	in cases provided for by law, not to be subject to a decision of material significance based solely on automated processing and to request appropriate safeguards;
Opt-Out From Direct Marketing	to withdraw consent at any time, easily and free of charge, where processing is based on consent;
Withdrawal Of Consent	to request at any time that processing of data for direct marketing purposes be stopped;
Right To Appeal	to apply to the State Audit Office of Georgia and/or a court if they believe their data are being processed in violation of applicable legislation.

The time limit for responding to/fulfilling a request is determined by law. For example, the standard time limit for providing information about data processing, access to data and copies is no later than 10 business days from receipt of the request (in exceptional cases this period may be extended in accordance with the procedure established by law), while information concerning a decision on data blocking shall be provided immediately, but no later than 3 business days.

A request to exercise your rights may be sent by email to unison@unison.ge or personal@unison.ge, or submitted at the Company's office. Where necessary, the Company may request information reasonably required to verify the identity of the person making the request.

15. DATA PROTECTION OFFICER

As an insurance organization, the Company ensures the performance of the Data Protection Officer function within the scope required by law. For questions, requests or complaints relating to personal data protection, you may contact:

Data Protection Officer	LLC Data Protection Officer
Email	Info@Dpo.Ge
Company Contact Email	personal@unison.ge

16. SUPERVISORY AUTHORITY AND RIGHT TO APPEAL

The supervisory authority responsible for personal data protection in Georgia is the State Audit Office of Georgia. If you believe that the processing of your personal data violates applicable legislation, you have the right to apply, in accordance with the procedure established by law, to the State Audit Office of Georgia and/or a court.

State Audit Office of Georgia: www.sao.ge

Law of Georgia on Personal Data Protection: Legislative Herald of Georgia

17. UPDATES TO THE POLICY

The Company may periodically update this Policy to reflect changes in legislation, data processing activities, technologies or organizational arrangements. The current version is published on the Company's website and indicates the date of the latest update.