Approved

by the Order No. 96/26 dated February 6, 2026.

Personal Data Processing and Protection Policy Unitel LLC

Tashkent, 2026

Contents

1. General Provisions
2. Terms and Definitions
3. Personal Data Processing Principles
4. Legal Grounds for Processing Personal Data
5. Terms, Purposes, and Features of Personal Data Processing
6. Rights of Personal Data Subjects
7. Personal Data Protection
8. Personal Data Protection Principle
9. Transfer of Personal Data to Third Parties
10. Cross-Border Data Transfer
11. Storage and Destruction of Personal Data
12. Authorized Division
13. Duties and Responsibilities of the Company's Employees
14. Final Provisions

1. GENERAL PROVISIONS

1.1. This Personal Data Processing and Protection Policy (hereinafter referred to as the 'Policy') defines the procedure for processing and protecting personal data at Unitel LLC (hereinafter referred to as the 'Company').

1.2. The Policy has been drawn up according to the Laws of the Republic of Uzbekistan (hereinafter referred to as the 'RUz') on personal data.

1.3. The Company owns and operates personal data databases and ensures that they are processed according to legal requirements and protected against unauthorized access and other illegal actions with personal data.

2. TERMS AND DEFINITIONS

2.1. **Personal data** means information recorded on electronic, paper, and (or) other tangible media that relates to a certain individual or makes it possible to identify him/her.

2.2. **Personal data processing** means one or a set of actions with personal data:
- collection;
- systematization;
- storage;
- change;
- addition;
- use;
- provision;
- distribution;
- transfer;
- depersonalization;
- destruction.

2.3. **Personal Data Subject (Subject)** means an individual to whom personal data relates.

2.4. **Official Website** means the Company's Internet resource designed to post official information, interact with Personal Data Subjects, and publish mandatory information according to the Laws and the Company's internal regulations available at https://beeline.uz.

2.5. **Services** means a set of services and digital solutions provided by the Company and/or Business Partner, including communication services, Digital Services, as well as other forms of interaction with Subscribers, Users of digital services, Business Partners, and other persons within the scope of the Company's core business.

2.6. **Digital Service** means a set of technological solutions provided by the Company and/or Business Partner using information and communication technologies (including mobile applications, web platforms, and other systems) designed to serve users.

2.7. **Subscriber** means an individual with whom a contract for the communication services has been concluded, or a person who actually uses the Company's communication services subject to a contract (including when registered in the name of a third party).

2.8. **Digital Services User** means an individual who uses the Digital Services of the Company and/or Business Partners according to relevant user agreements/offers, regardless of whether there is a contract for communication services.

2.9. **Contractor (Individual)** means an individual with whom the Company interacts under a civil law contract (including, but not limited to: contracts for work, services, copyright agreements), as well as an individual entrepreneur operating without forming a legal entity.

2.10. **Business Partner** means a legal entity or individual (including individual entrepreneurs) who participates jointly with the Company in implementing services, products, marketing, and bonus programs, as well as other projects on a contractual basis.

2.11. **Authorized Representative** means an individual acting for or on behalf of a Business Partner (legal entity or individual entrepreneur), including prospective Business Partners according to the Laws, Articles of Association, power of attorney, or other legal basis, as well as individual whose personal data is processed by the Company due to their status as a member of a legal entity (including founders, managers, signatories), regardless of whether a contract has been concluded.

2.12. **Third Party** means any person who is not a subject, owner, and/or controller, but who is related to thereto by personal data processing circumstances or relationships.

2.13. **Cross-Border Transfer of Personal Data** means the transfer of personal data outside the Republic of Uzbekistan.

2.14. **Anonymized Personal Data** means personal data that has been processed in such a way that it is no longer possible to identify the specific data subject to whom it belongs.

2.15. **Aggregated Data** means generalized statistical information formed from anonymized personal data that does not provide identification of a specific subject and has aggregate characteristics (e.g., average values, quantity, percentage, distribution).

2.16. **Automated Personal Data Processing** means processing of personal data using information technology, software, algorithms, and automated systems, when actions with personal data involve no or predominantly no human.

2.17. **Authorized Unit** means a structural unit of the Company ensuring the processing and protection of personal data according to the Laws of the Republic of Uzbekistan.

2.18. **Personal Data Protection** means a set of legal, organizational, and technical measures aimed at ensuring the confidentiality, integrity, and availability of personal data, as well as preventing its loss, unauthorized access, alteration, destruction, distribution, and other unlawful actions.

2.19. **Confidentiality of Personal Data** means the state of personal data, when they are secured from illegal processing.

2.20. **Integrity of Personal Data** means the state of personal data, when they are preserved in its original and/or established form, protected from unauthorized or accidental alteration, deletion, or distortion, and can be restored in case of failure, loss, or damage.

2.21. **Technical Information** means a set of data automatically collected and processed when the Subject of Personal Data uses the Company's Services, including, but not limited to: device and module identifiers (IMEI, IMSI, MAC address, serial number, model, equipment type); SIM card and cell tower connection information (CT ID, registration, coverage area); IP address, network parameters, connection type, connection speed, roaming mode; information about the operating system and software (version, identifiers, usage parameters); geodata (country, city, coordinates, entry point); log files and logs (errors, events, API calls, sessions); cookies and similar technologies; information about technical support requests (date, content, result); other automatically generated technical data necessary for the provision, support,

operation, analysis, and security of the Services.

2.22. **Behavioral Profile** means a set of information formed when using the Company's Services by the Subject of Personal Data characterizing their actions, preferences, and level of activity, including actions on websites and in mobile applications (clicks, transitions, session duration, frequency of use); automatically generated behavioral models and specifications ((e.g., interests, preferences, inclinations, level of engagement); consumption, history of Services' use, interaction scenarios; analytical conclusions based on Big Data and machine learning algorithms; other information about individual characteristics of the Subject's behavior when using the Services.

2.23. **Financial Information** means a set of Personal Data about the financial activity of the Data Subject when using the Company's Services or interacting therewith, including, but not limited to: information about the balance, tariffs, accruals, write-offs, and debts; payment history, including the date, amount, method, and purpose of transactions; information about the payment instruments used by the Subject (including card type, payment system, masked number, tokenized data); information about transactions made in the Company's Digital Services (including purchases, subscriptions, bonuses, and discounts); bank and settlement details provided for payments or refunds; other information directly or indirectly disclosing the Subject's transactions stored or processed in the Company's information systems.

2.24. **Artificial Intelligence (AI)** means a set of technological solutions allowing to mimic human cognitive functions (including self-learning and problem-solving) and to obtain results comparable to the results of human intellectual activity when performing specific tasks.

3. PERSONAL DATA PROCESSING PRINCIPLES

3.1. The Company processes personal data strictly according to the principles established by the Laws of the Republic of Uzbekistan. These principles are mandatory for all employees and third parties involved in the Personal Data Processing and are the basis for assessing the legality of the processing.

3.2. Breaching of any of the principles of Personal Data Processing shall be considered as breaching of the Laws of the Republic of Uzbekistan and entails liability in a prescribed manner.

3.3. The core principles of Personal Data Processing:

3.3.1 respect for the constitutional rights and freedoms of the individual and citizen;
3.3.2. legal validity of the purposes and methods of Personal Data Processing;
3.3.3. accuracy and reliability of Personal Data;
3.3.4. confidentiality and security of Personal Data;
3.3.5. equality of rights of subjects, owners, and operators of Personal Data;
3.3.6. safety of individuals, society, and the state;
3.3.7. transparency of Personal Data Processing;
3.3.8. minimization of the Personal Data processed;
3.3.9. observance of time for Personal Data storage.

4. LEGAL GROUNDS FOR PROCESSING PERSONAL DATA

4.1. The Company shall process personal data if there is one of the following legal grounds provided for by the Laws of the Republic of Uzbekistan:

4.1.1. explicit and voluntary consent of the subject, which is provided for specific data processing purposes;

4.1.2. processing is necessary to execute a contract to which the Data Subject is party or in order to take steps at the request of the Data Subject prior to entering into such a contract;

4.1.3. if processing is necessary for the Company to fulfill its obligations under the Laws;

4.1.4. if processing is necessary to protect the legitimate interests of the Data Subject or another person;

4.1.5. if there is a need to process to exercise the rights and legitimate interests of the Company or Third Parties, or to achieve socially significant goals, provided that the rights and legitimate interests of Personal Data Subjects are not breached;

4.1.6. for statistical or other research purposes, subject to mandatory Anonymization of Personal Data;

4.1.7. if this data was obtained from public sources and its processing does not breach the rights and freedoms of the Personal Data Subjects.

5. TERMS, PURPOSES, AND FEATURES OF PERSONAL DATA PROCESSING

5.1. In order to comply with the Laws of the Republic of Uzbekistan on Personal Data, the Appendix hereto defines the categories of Personal Data Subjects, the purposes of Personal Data Processing, as well as the list of Personal Data processed for each category.

5.2. The Company carries out both Automated Personal Data Processing and non-automated processing of personal data to the extent necessary to achieve the objectives provided for in this Policy.

5.2.1. For the purposes of concluding and executing a contract (including the provision of Services and the sale of goods), as well as taking measures at the request of the Subject prior to entering into a contract, including for assessing reliability and solvency, preventing fraud, making decisions on the possibility of selling goods (including on installment terms), providing Services with deferred payment, or establishing Credit Limits, the Company is entitled to carry out Automated Personal Data Processing (including Financial Information, Behavioral Profile, and Technical Information) using scoring algorithms. The results of such processing, based on information available to the Company and (or) data obtained from Third Parties (including credit bureaus), shall be recognized by the Parties as a sufficient and exclusive basis for the Company to make relevant decisions (including refusal to conclude a contract or provide Services or goods) without the need for additional manual review or personnel intervention.

5.2.2. In cases where a decision producing legal consequences for the Subject or otherwise significantly affecting their rights and legitimate interests is made exclusively by Automated Personal Data Processing, the Company, upon receipt of a corresponding written request from the Subject (submitted in a manner allowing for reliable identification of the applicant), is obliged to:

- explain the procedure for making such a decision;

- provide an opportunity to file a reasoned objection against such a decision;

- explain the procedure for the Subject to protect their rights;

- consider the objection and notify the Subject of the results in writing within the time limit established by the Laws.

5.3. The Company shall be entitled to process data about the actions, preferences, and interactions of Personal Data Subjects with the Services (including Behavioral Profile, Technical,

and Financial Data) for the purposes of providing, optimizing, and developing the Services, while complying with the principles of minimization and non-breach of the rights of subjects.

Processing involves automated means and does not involve individualized Processing of Personal Data by Company employees.

The results of such processing are aggregated or anonymized with no possibility to identify specific subjects.

Such data may be transferred to Partners only aggregated and/or anonymized.

5.4. The consent of the Subject of Personal Data to the Processing of Personal Data may be provided in the following forms:

5.4.1. by accepting an offer (public agreement) that explicitly specifies the purposes of personal data processing; in this case, consent is deemed to have been given after the offer is accepted;

5.4.2. by confirming your consent with the terms and conditions of service provision in the Company's Digital Services;

5.4.3. by entering into agreement;

5.4.4. in the form of a separate document drawn up in written or electronic form;

5.4.5. through conclusive actions including the actual use of the Company's services;

5.4.6. by other means not contrary to the Laws of the Republic of Uzbekistan.

5.5. In cases where Personal Data is processed without the consent of the Data Subject (for example, to perform a contract, based on legal requirements, or to protect the rights and legitimate interests of the Company), the Company shall strictly comply with the Laws of the Republic of Uzbekistan.

5.6. The Company shall provide video surveillance within its areas and facilities to ensure security, protect property, and prevent incidents.

The Company shall not process data obtained through video surveillance to identify specific Subjects of Personal Data.

Herewith, video surveillance recordings may be transferred in cases provided for by the Laws of the Republic of Uzbekistan, including upon request of law enforcement agencies, courts, or other authorized state bodies.

5.7. To ensure access control and monitoring of access to the Company's area and facilities, it is permitted to process biometric personal data of employees, interns, trainees, Contractors (individuals), and Authorized Representatives. Such processing is subject to consent of the Subject for purposes specified herein in compliance with the Laws of the Republic of Uzbekistan on Personal Data.

5.8. The Company is entitled to use artificial intelligence, machine learning, and algorithmic analysis technologies as a tool for Automated Personal Data Processing to the extent necessary to achieve the objectives provided for in this Policy.

5.8.1. When using artificial intelligence technologies, the Company takes necessary measures aimed at ensuring compliance with human and civil rights and freedoms. The application of these technologies is carried out taking into account the minimization of risks of harm; however, the Company shall not be held liable for subjective assessments of the ethicality of the algorithms' operation, provided they function within the framework of the Laws.

6. RIGHTS OF PERSONAL DATA SUBJECTS

6.1. Data Subjects have the rights provided for by the Laws of the Republic of Uzbekistan, including the right to access, correct, restrict, and destroy Personal Data, as well as other rights aimed at protecting their legitimate interests.

6.2. Requests providing execution of the Personal Data Subjects' rights may be submitted as follows:

- by email to the addresses specified on the official resources of the Company;
- by mail to the legal address of the Company;
- personally, when visiting the Company's office.

6.3. Withdrawal of consent to the processing of personal data, a request for the destruction or suspension of the processing of personal data necessary for the Company's Services, entails further failure to provide such Services by the Company.

7. PERSONAL DATA PROTECTION

7.1. The Company shall protect Personal Data when they are processed according to the Laws of the Republic of Uzbekistan.

7.2. Personal Data protection involves the legal, organizational, technical, and other means aimed at preventing their unauthorized access, loss, alteration, disclosure, or destruction.

8. PERSONAL DATA PROTECTION PRINCIPLE

8.1. The Company shall protect Personal Data strictly according to principles hereof. These principles are mandatory for all employees involved in the Personal Data Processing and are the basis for assessing the security.

8.2. Breaching of any of the principles of Personal Data Processing shall be considered as breaching of this Policy and entails liability in a prescribed manner.

8.3. The Company shall protect Personal Data according to the following principles arising from the Laws of the Republic of Uzbekistan and international information security practices:

8.3.1. compliance with the law-based regime that excludes unauthorized disclosure or distribution of Personal Data without the consent of the subject or with no other legal basis;

8.3.2. integrity and security - compliance with requirements and measures to prevent loss, distortion, or unauthorized alteration of Personal Data; Personal Data shall be kept up to date, consistent, and secure;

8.3.3. access restriction - Personal Data can be accessed by a strictly limited group of persons within the scope of their official role-based duties and the minimum necessary amount;

8.3.4. transparency and accountability - Personal Data Protection mechanisms shall be documented, and data processing and protection shall be subject to verification and audit;

8.3.5. assignment of responsibilities - ensuring that duties and responsibilities for Personal Data Protection are established in job descriptions, confidentiality agreements, and other internal regulations governing the activities of employees and other persons authorized to Process Personal Data.

9. TRANSFER OF PERSONAL DATA TO THIRD PARTIES

9.1. It is permitted to transfer Personal Data to Business Partners or Third Parties, including cross-borderly, only for their processing and if there are legal grounds provided for in clauses 4.1. and 10.2 hereof.

9.2. The following safety measures shall be observed:

- entering into agreement with a Business Partner or Third Party providing obligations regarding the Protection of Personal Data;
- assessing the legality of transfers and maintaining a register of such transactions.

9.3. If the relationship with a Business Partner or Third Party involves access to, processing, or transfer of Personal Data, provisions on the protection of Personal Data shall be

recorded. These provisions may be included directly in the contract or executed as separate non-disclosure agreement (NDA) or other supplementary agreement to the contract.

10. CROSS-BORDER DATA TRANSFER

10.1. Personal Data can be transferred cross-borderly only if the recipient country adequately protects the rights of Personal Data Subjects.

10.2 Personal Data can be transferred cross-borderly to a country that does not provide adequate protection of the rights of Personal Data Subjects in the following cases:

- the consent of the Data Subject to the Cross-Border Transfer of Personal Data;
- the need to protect the constitutional order of the Republic of Uzbekistan, public order, the rights and freedoms of citizens, and the health and morality of the population;
- as provided for by international treaties of the Republic of Uzbekistan.

11. STORAGE AND DESTRUCTION OF PERSONAL DATA

11.1. Personal Data is stored in a form that provides identification of the Data Subject for no longer than is necessary for the processing and the established storage periods.

11.2. Unless otherwise provided by the Laws of the Republic of Uzbekistan, Personal Data shall be stored for the period necessary to achieve the purposes of processing, but not longer than the general limitation period established by the Laws of the Republic of Uzbekistan after termination of contractual or other legal relations with the Subject of Personal Data.

11.3. Upon expiration of the storage period, Personal Data shall be destroyed or anonymized, unless otherwise provided by Laws.

12. AUTHORIZED DIVISION

12.1. The Company establishes an Authorized Division whose tasks include organizing the Processing and Protection of Personal Data.

12.2. The activities, tasks, rights, and obligations of the Authorized Division shall be provided by the Laws of the Republic of Uzbekistan, the regulations on the Authorized Division, and other internal regulations of the Company.

13. DUTIES AND RESPONSIBILITIES OF THE COMPANY'S EMPLOYEES

13.1. Employees shall comply with the Laws of the Republic of Uzbekistan and the internal regulations of the Company on Personal Data.

13.2. Employees shall assist the Authorized Division in monitoring compliance with Laws of the Republic of Uzbekistan and the internal regulations of the Company on Personal Data.

13.3. Upon employment, the employee shall sign an agreement for non-disclosure of confidential information and personal data and read this Policy.

13.4. Company employees shall be personally liable for breaching the Laws of the Republic of Uzbekistan, this Policy, and other internal regulations of the Company for Personal Data.

13.5. Company employees who directly handled Personal Data shall, if transferred to another position, change position within the Company, or dismissed, transfer all physical media with information (including paper documents and other media with Personal Data) in a prescribed manner. Technical equipment provided by the Company (including laptops, desktop

computers, and other devices) shall be returned and, if necessary, for business purposes, may be checked for unlawful actions.

14. FINAL PROVISIONS

14.1. This Policy is an internal regulation of the Company and is binding on all employees and other persons involved in the Processing of Personal Data.

14.2. This Policy is publicly available on the Company's Official Website and Digital Services in a section accessible to all users.

14.3. This Policy comes into force upon its publication in the specified sources, unless otherwise provided by the Policy or as decided by the Company.

14.4. The Company reserves the right to amend the Policy without specific notification to the Subjects of Personal Data. The new edition shall be deemed effective after it is posted on the Company's Official Website and Digital Services, unless otherwise specified in the new edition.

Appendix

CATEGORIES OF PERSONAL DATA SUBJECTS, PURPOSES OF PROCESSING, AND LIST OF PERSONAL DATA PROCESSED

This Appendix establishes the categories of Personal Data Subjects, the purposes of processing, and the list of personal data processed by the Company. It applies to all Personal Data processing activities by the Company, including automated and non-automated processing.

Subjects of Personal Data	Purposes of Personal Data Processing	List of Personal Data
Company's Subscribers	**1. Provision and support of Services -** provision of the Company's Services, including entering into and execution of contracts, registration and authorization in digital systems, communication services, and access to the Services of the Company and Business Partners; support for Services, including maintaining accounts and billing, issuing invoices, recording payments, managing debt, and processing payment transactions. **2. Identification, security, and legal protection:** – identification and authentication of Subscribers, including when using mobile applications, personal accounts, via phone numbers, device identifiers, and other identification means; secure access to information systems and applications, protection against fraud and unauthorized access, detection, prevention, and investigation of suspicious activities; – implementation of the Company's rights and legitimate interests, including protection of interests in pre-trial and judicial proceedings, as well as interaction with government agencies according to the Laws and upon official requests. **3. Working with customer experience and service quality -** improving the quality of Services, including handling requests and complaints, technical support, troubleshooting, satisfaction surveys, analyzing feedback; providing a personalized interface and services in a digital environment. **4. Information communications and notifications -** informing Subscribers about new products, services, tariffs, changes in the	– last name, first name, patronymic; – date and place of birth; – details of the identity document; – National Identity Number (PINFL); – sex; – citizenship; – phone number; – email; – address of registration at the place of residence; – information about the communication services provided (including information about the contract for communication services, information from other documents generated during the period of provision of communication services); – cost details by phone number; – Technical information; – Behavioral profile; – Financial information.

service, promotions, application updates, and other information related to the service.

5. Marketing and commercial interaction:

– trigger and targeted communication services, including SMS mailings, automated IVR calls, commercial offers, and other information generated based on the Subscriber's actions, service history, behavior in Digital Services, events, and preferences;

– marketing activities aimed at increasing subscriber engagement and loyalty, creating personalized offers, participating in promotions, bonus and partner programs, and sending advertising and informational communications.

6. Analytics, forecasting, and interaction with Business Partners:

– projects to analyze user behavior, preferences, and consumer trends, including the collection and analysis of behavioral data, navigation logs, user scenarios, and parameters of interaction with Digital Services, behavior modeling and demand forecasting using Big Data and machine learning technologies, as well as optimization of the Company's Services;

– use of scoring algorithms, including assessment of payment discipline, risk analysis, forecasting the likelihood of response to offers based on data about activity, preferences, and history of interaction with the Services;

– within the scope of purposes specified, it is permitted to transfer Anonymized Personal Data and/or Aggregated Data to provide services to Business Partners, provided that it is impossible to identify the Personal Data Subjects.

7. Transfer of data to Business Partners and Third Parties when performing contractual obligations, providing Services, features, integrating, and interacting with Digital Services and products of Business Partners.

8. Sale of goods – sale of goods to Subscribers, including the conclusion and execution of sale and purchase agreements, processing of installment plans, settlement management, and payment accounting; conducting scoring to assess the Subscriber's compliance with the criteria for granting installment plans.

Users of Digital Services	**1. Provision and support of Digital Services -** provision of Digital Services of the Company and Business Partners, including registration and support of user accounts, creation of personal accounts in mobile applications and on websites, linking accounts to phone numbers or other identifiers, restoring access, managing profile settings and Personal Data. **2. Security and stable operation -** ensuring the security and uninterrupted operation of digital services, including protection against unauthorized access, data leaks, and fraud, checking the correctness of authorization, maintaining technical logs, and monitoring the performance of mobile applications and websites. **3. User behavior analysis and technical analytics -** collection and processing of data on user actions (clicks, navigation, views, and other interaction scenarios) to analyze behavior, define preferences, interface difficulties, and assess the effectiveness of mobile application and website features. **4. Personalization and improvement of user experience -** adaptation of the interface and displayed content to individual user preferences, use of recommendations, hints, and scenarios, configuration of notifications, themes, display of modules, and other elements of Digital Services. **5. Participation in marketing and customer programs -** implementation of loyalty programs, bonus and promotional offers, informing about new products, changes in terms of service, conducting surveys, quizzes, sweepstakes, and other events involving users, as well as analyzing responses to advertising campaigns and segmenting the audience to promote the Services. **6. Interaction with Business Partners -** transfer of data to Business Partners when fulfilling contractual obligations, providing joint Digital Services, and ensuring the integration of digital platforms and features. **7. Protection of the Company's rights and legitimate interests -** exercising the Company's rights and legitimate interests, including protecting its interests in pre-trial and court proceedings, as well as complying with legal requirements.	– last name, first name, patronymic; – date and place of birth; – phone number; – email; – details of the identity document; – sex; – citizenship; – address of registration at the place of residence; – information about the Service provided (including information about the contract for services, information from other documents generated during the period of provision of services); – photo image (if the User adds a digital service independently in the Digital Service being used); – Technical information; – Behavioral profile; – Financial information.

Contractors (individuals) and Authorized Representatives	**1. Entering into and execution of contracts:** - conclusion, support, and termination of contracts (including civil law, copyright, contract, and other agreements); - keeping records of calculations, accruals, and payments related to services and works. **2. Verification of compliance with legal and internal requirements:** - identification and verification (KYC), including collecting, checking, and confirming information and documents; - assessment of trustworthiness, professional suitability, status, and business reputation; - compliance and security verification, including sanctions restrictions, conflicts of interest, anti-money laundering (AML) measures, and other restrictions. **3. Organization of access to Company resources:** - providing access to the Company's information systems, offices, and other facilities to fulfill contractual obligations; - compliance with internal access control procedures, information security, and other access procedures. **4. Contractual communication and document management:** - processing notifications, requests, claims, acts, reports, and other contract-related documents; - interaction on quality, deadlines, and conditions of services or works. **5. Protection of the rights and legitimate interests of the Company:** - representing the Company's interests in pre-trial and court proceedings; - preparation of evidence, correspondence, information, and other materials for dispute resolution or compliance with legal requirements.	- last name, first name, patronymic; - date and place of birth; - details of the identity document; - National Identity Number (PINFL); - Tax ID; - sex; - citizenship; - address of registration at the place of residence; - phone number; - email; - position, name of organization, information about the powers; - information about the concluded agreement (number, date, type of agreement); – bank details.
Company employees and their relatives	**1. Compliance with legal requirements:** – compliance with labor, tax, and other Laws of the Republic of Uzbekistan; - keeping personnel records and employee files;	- last name, first name, patronymic; - date and place of birth; - details of the identity document;

	- calculation and payment of wages, taxes, and mandatory deductions; - preparation and submission of mandatory reports to authorized government agencies. **2. Social and recruitment package:** - processing and support of medical insurance; – registration of a subscription to gyms; – registration of corporate mobile communications; – issuing and servicing bank cards for payments with an employee; - other benefits and compensation provided for by the Laws and the Company's internal regulations. **3. - HR management and staff development;** - personnel reserve management; - organization of transfers within the Company; - planning and supporting career growth and professional development; - organization of training and professional development; – organization of business trips and official trips. **4. Analytics and statistical data processing:** - collection, recording, analysis, and preparation of statistical and management HR reports; - forecasting personnel needs and resources. **5. Organization and maintenance of internal and external communication:** - supporting interaction within the Company (including cross-functional and interregional); - communication with employees of legal entities whose members (shareholders) are VEON Ltd., VEON UZBEKISTAN HOLDING B.V., VEON CENTRAL ASIA B.V. and their affiliates; - interaction with the Company's Partners when fulfilling contracts and other obligations. **6. Exercising the rights and protecting the interests of the Company:**	- sex; - National Identity Number (PINFL); - Tax ID; - address of registration at the place of residence; - actual address; - phone number; - email; - education, work performed since the beginning of employment; - military status, military registration information; - payment card details; - individual retirement account number; - marital status; - full names and dates of birth of close relatives, and details of identity documents; - grounds for termination of the employment agreement; - photo; - results of the mandatory medical examination; - information from a CV, questionnaire, or other documents submitted on one's own initiative; - Biometric data: may be processed for controlling access to the Company's areas and facilities.

	- operation of business processes and workplace management; - duties and quality of work control; - time-keeping and performance evaluation; - protection of the Company's property and other legitimate interests; - participation in pre-trial and court disputes, consideration of appeals and claims. **7. Security:** - physical and information security, occupational safety; - protection of workers' lives and health; - protection of strictly private, confidential information, and closed information; - control of access to the Company's premises, resources, and systems. **8. Control measures** - audits, inspections, reviews, and internal investigations; – compliance with internal controls, anti-corruption procedures, and corporate ethics.	
Candidates for vacant positions	**1. Selection and evaluation of candidates:** - review of talent, experience, competencies, and other parameters with the Company's established requirements; – verification of information provided by the candidate, including reference and other information; - organizing and conducting interviews, assessment, and other stages of HR selection. **2. Succession pipeline.** **3. Exercising the rights and protecting the interests of the Company:** - resolution of potential disputes, including pre-trial and court settlement in case of appeal of the recruitment results; - compliance with the Company's internal regulations ensuring transparency and soundness of decision-making based on the results of recruitment.	- last name, first name, patronymic; - date and place of birth; - details of the identity document; - sex; - National Identity Number (PINFL); - citizenship; - phone number; - email; - address of registration at the place of residence; - information about education, job description, qualifications; - photo; - information from a CV, questionnaire, or other documents submitted by a candidate on one's own initiative;
Company's interns and visiting students	**1. Organization and support of internships/ on-the-job training -** registration, implementation, and documentation of internships or on-the-job (industry) training at the Company according to the Laws and regulations of the Company.	- last name, first name, patronymic; - date and place of birth; - details of the identity document; - sex;

	2. Access mode: – registration of access authorization cards and management of access to the Company's areas and facilities; – compliance with access mode and physical security measures. **3. Technical and operational access:** - providing access to information systems, resources, and technical infrastructure necessary to perform assignments during internship/on-the-job training; – observance of information security measures; - drafting contracts and other agreements, including for connecting business communications and other corporate services. **4. Exercising the rights and protecting the interests of the Company** - compliance with the Laws of the Republic of Uzbekistan; – protection of rights in pre-trial and judicial proceedings.	- National Identity Number (PINFL); - citizenship; - phone number; - email; - address of registration at the place of residence; - payment card details; - photo; - information from a CV, questionnaire, or other documents submitted on one's own initiative. - Biometric data: may be processed for controlling access to the Company's areas and facilities.
Visitors to the Company's offices and facilities	**1. Access control and access mode observance:** – identification and registration of visitors; – registration of temporary access authorization cards and control of access to the Company's area and facilities; – record the entry and exit time. **2. Physical and information security:** - protecting the life and health of employees, visitors, and other persons within the Company's area; - prevention and detection of unauthorized access, offenses, and other incidents; – protection of property and information resources. **3. Incident response and internal investigations:** – monitoring of security events (including using video surveillance); – internal checks in case of access breaches or violations. **4. Exercising the rights and legitimate interests of the Company,** including protecting rights in pre-trial and court proceedings.	- last name, first name, patronymic; - details of the identity document; - date and time of entry/exit; - purpose of the visit.