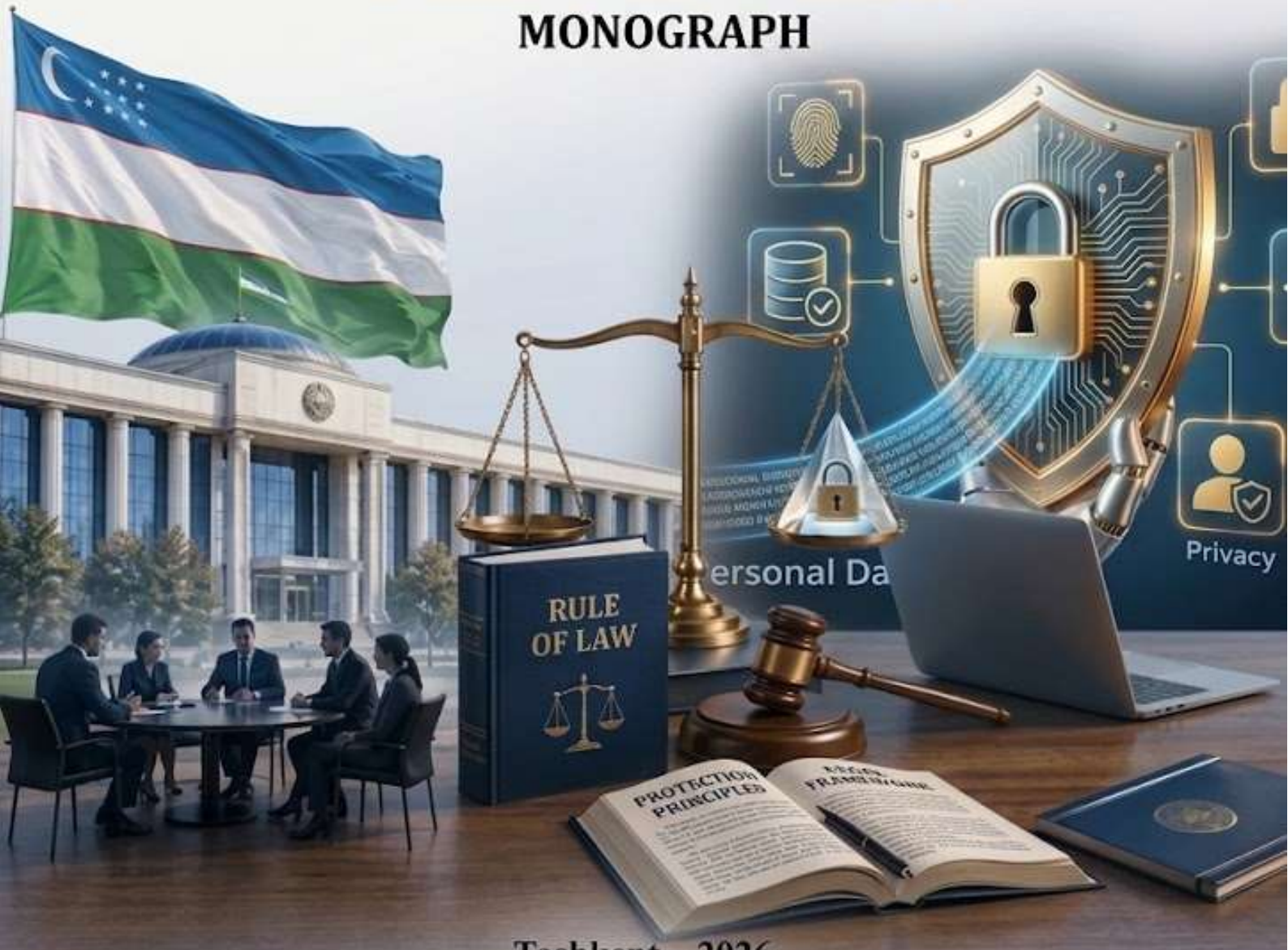
Institute of Legislation and Legal Policy under
the President of the Republic of Uzbekistan

A. ANORBOEV

PERSONAL DATA LAW: PERSONAL DATA PROTECTION IN THE NEW ERA

MONOGRAPH



Tashkent – 2026

INSTITUTE OF LEGISLATION AND LEGAL POLICY UNDER THE PRESIDENT OF THE REPUBLIC OF UZBEKISTAN

A. ANORBOEV

PERSONAL DATA LAW: PERSONAL DATA PROTECTION IN THE NEW ERA

MONOGRAPHY

Tashkent – 2026

A. ANORBOEV. Personal data law: personal data protection in the new era. Monograph. – Tashkent: “Dimal” Publishing House, 2026, – 187 p.

Responsible Editor:
Doctor of Science in Law (DSc), Professor A. Rasulov

Reviewers:
Doctor of Science in Law (DSc), Professor B. Ismailov, Doctor of Science in Law (DSc) B. Muminov, Doctor of Science in Law (DSc), Associate Professor S. Nurumbetova

ЎУК | 344414
ORCID | https://orcid.org/0009-0003-5355-8753
Publons | QPB-1888-2026
SSRN: | 12260788
Index Copernicus | 48623
РИНЦ | 3827-4098
DOI | 10.5281/zenodo.21374052
GOOGLE академия | https://scholar.google.com/citations?user=KIJpct8AAAAJ&hl=ru
ZiyoNet | https://profile.ziyonet.uz/uzc
DergiPark | https://dergipark.org.tr/tr/pub/@amiriddin-anorboyev
Academia | https://independent.academia.edu/AnorboyevAmiriddin/Network?tab=suggested
Scopus | https://www.scopus.com/pages/home
Clarivate Analytics | https://apps.clarivate.com/account?app=endnote&tab=personal
КиберЛенинка | https://cyberleninka.ru/me
OpenAIRE | https://www.openaire.eu/f/269/create-new-article
GitHub | https://github.com/explore
Webofscience | QPB-1888-2026

This fundamental monograph comprehensively examines the institutional and regulatory framework of the right to personal data in the new era, characterized by the rapid development of digital transformation and artificial intelligence, machine learning, neural networks, and decentralized systems. The monograph provides a new doctrinal definition of the concept of personal data based on the principle of technological neutrality, and thoroughly elucidates the dynamic life cycle of the institution of “processing,” from the emergence of information to its complete destruction.

The study analyzes the procedures for processing personal data within the Unified Interactive Public Services Portal and Electronic Government systems, as well as the legal status of subjects and operators. It also puts forward models for eliminating collisions in the legal and technical qualification of offenses in the information sphere committed in cyberspace, particularly cases of unlawful acquisition of personal data through phishing, social engineering, and unauthorized access, as well as gaps in criminal-law protection.

At the same time, the author integrates into the field of science an entirely new **“Cyberalogy”** methodology and develops innovative legal guarantees for ensuring information sovereignty, the inviolability of information in algorithmic environments, and protection against cyber threats. This work serves as a practical and strategic source for legislators, representatives of state and law enforcement bodies, judges, researchers in the fields of information law and cybersecurity, doctoral students, and students of higher educational institutions.

This monograph has been published based on the recommendation of the Council of the Institute of Legislation and Legal Policy under the President of the Republic of Uzbekistan.

TABLE OF CONTENTS

INTRODUCTION

The current stage of human development is characterized by the deep penetration of digital technologies, artificial intelligence, cloud computing, and global information networks into all spheres of society and state life. Digital transformation, on the one hand, increases the efficiency of public administration and electronic government systems and dramatically improves the quality of interactive services provided to the population, while, on the other hand, it is also increasing the threats to the information privacy and personal sovereignty of individuals to an unprecedented degree. Every day, the biometric, genetic, financial, and social behavioral indicators of millions of citizens, including their digital footprints, are being processed by information and communication systems, Big Data, and artificial intelligence algorithms. Under these conditions, the protection of personal data has become not merely a matter of technical security, but a priority component of ensuring fundamental human rights and freedoms, the foundations of the constitutional order, and national information security. Article 31 of the Constitution of the Republic of Uzbekistan strictly establishes that every person has the right to inviolability of private life, to personal and family secrets, and to protection of his or her honor and dignity. For the purpose of consistently implementing this constitutional norm in practice, on July 2, 2019, the Law of the Republic of Uzbekistan “On Personal Data” № LRU–547 was adopted, laying the foundation for regulating this sphere in our country as an independent legal institution. However, in recent years, the rapid development of artificial intelligence (AI), machine learning (Machine Learning), neural networks, decentralized ledgers (Blockchain), and information systems has been creating a number of conceptual and doctrinal gaps (lacuna in lege) in the existing national legislative system.

First, in the current legislation, the descriptions of the concepts of personal data and their processing are defined very narrowly (dogmatically), and they are mainly tied to traditional requisites or static information systems. The mechanism for the digital identification of synthetic and biometric data formed in virtual form, in operational memory (RAM), or in the form of an artificial intelligence avatar (Deepfake) is not perfect.

Second, the dynamics of offenses committed in cyberspace demonstrate that, apart from the “unlawful transfer” or “dissemination” of personal data, acts of “unlawful acquisition” through phishing and social engineering, “unauthorized access,” and “unlawful possession” have not been clearly and comprehensively qualified. This, when colliding with the principles of in dubio pro reo (resolution of doubts in favor of the accused) and nullum crimen sine lege (there is no crime without a law) established in Articles 20 and 21 of our Constitution, creates a legal environment enabling cybercriminals to evade liability.

Third, the concept of linking personal data in legislation exclusively to the form of a “material object” or “paper and plastic” contradicts the principles of digital jurisprudence. According to the doctrine of information law, personal data constitute an intangible benefit, and their protection should be based not on the physical form

of the medium, but on the objective connection of the information with a particular individual and its potential to identify that individual.

In view of the above factors and from the perspective of the cyberalogy doctrine, the need for a comprehensive academic and legal-analytical study of the institutional foundations, regulatory and legal regime, and legal protection mechanisms of the right to personal data determines the relevance of this monograph.

The problems of protecting personal data, information law, and ensuring cybersecurity have been studied from various aspects by domestic and foreign legal scholars.

With regard to the formation of the theory of information law and the institution of personal privacy, among domestic and foreign researchers, G. Mirzo classified personal data into general, special, and biometric types and analyzed their practical status, while I. Bachilo and L. Tereshchenko studied personal data as a special information regime with restricted access rights aimed at ensuring constitutional rights. A. Savelyev scientifically substantiated the identification of an individual through indirect identification means and the protection of dynamic data in the Big Data environment. Among foreign scholars, Paul M. Schwartz and Daniel J. Solove put forward the view that the concept of personal data (PII) is not permanent, but rather a continuum based on the "risk of identification," while A. Miller elucidated the doctrinal foundations of an individual's information autonomy in computerized systems and control over electronic records. At the same time, in national jurisprudence, comprehensive and holistic monographic studies of the right to personal data as an integrated institution under the new conditions in which digital transformation and artificial intelligence (AI Act, GDPR) are developing, particularly with the integration of the cyberalogy concept, had not been sufficiently developed.

This study is aimed at filling this gap. The main purpose of the study is to reveal the institutional and regulatory and legal foundations of the right to personal data, analyze the digital and algorithmic regimes of their processing, and develop scientific and practical proposals and recommendations for ensuring the inviolability of personal data and improving liability mechanisms in the era of artificial intelligence and cyber threats. To achieve this objective, it is established to reconsider the concept and doctrinal definition of personal data based on the principle of technological neutrality, comprehensively analyze the legislative system and mechanisms of state regulation, clarify the life cycle of the processing institution from pseudonymization to complete destruction, identify its specific features in the Unified Interactive Public Services Portal and electronic government systems, substantiate the criminal-law qualification of cases of unauthorized access and data leakage in cyberspace, and develop legal guarantees for protection in algorithmic environments.

The object of the study is the set of social and legal relations arising in the process of collecting, systematizing, storing, processing, transferring, protecting personal data, and applying artificial intelligence and digital technologies in this sphere.

The subject of the study is the constitutional and national legislative norms in the sphere of personal data, international standards (GDPR, Convention 108, UNCITRAL Model Laws), judicial and law enforcement practice, as well as scientific and doctrinal views related to the sphere and the principles of cyberalogy. The methodological basis of the study consists of dialectical and systemic analysis, logical-legal (dogmatic), comparative-legal, functional, formal-legal, and cyberalogical approaches. By means of the comparative-legal method, the norms of national legislation were compared with the GDPR and AI Act regulations of the European Union and UNCITRAL standards. Through the cyberalogical and systemic-functional approaches, personal data were studied not merely as an element of an information system, but as a dynamic object of information sovereignty and algorithmic environments. Formal-legal and logical methods were applied in identifying the elements of crimes and collisions in the current Codes on Administrative Responsibility and Criminal Code.

The study is one of the first comprehensive monographic works to illuminate the right to personal data from a contemporary perspective based on the concept of digital transformation and cyberalogy, and its scientific novelty is manifested in the following:

a technologically neutral (technology-neutral) definition of personal data was proposed;

the expanded life cycle of the “processing” (processing) institution (lifecycle processing) was substantiated; a model for eliminating gaps in criminal-law protection against cybercrime was developed;

the correlation between the “personal data database” and the “algorithmic environment” was established, and the information-legal concept of the object of protection was reconsidered.

The results of the study, scientific conclusions and proposals may be widely used in introducing amendments and additions to the Law of the Republic of Uzbekistan “On Personal Data,” the Criminal Code and the Code on Administrative Responsibility, in improving the methodology for the qualification and investigation of crimes by courts, prosecution, and cybersecurity bodies, as well as in the educational process at higher educational institutions.

CHAPTER I. CONCEPT OF PERSONAL DATA AND ITS INSTITUTIONAL FOUNDATIONS

1.1. Concept of Personal Data and Its Content and Essence

Opinions regarding the concept of personal data are diverse. In particular:

According to G. Mirzo, personal data consist of any information about an individual. Personal data are divided into three types: first, general data; second, special data; third, biometric data. General data include information such as an individual's first and last name, records contained in his or her passport and other personal documents, date and place of birth, e-mail address, places of residence, study and employment, family, social and property status, where he or she received education, profession, amount of income, and similar information. Telephone numbers belong to the category of personal data only in cases where they are recorded together with the owner's first and last name. The state registration number of a vehicle, the account number of a communal-residential utility service, and similar information are not considered personal data. This is because the former directly relates to the vehicle, while the latter relates to the residential property. Special data means information related to an individual's racial and national affiliation, political, religious and philosophical views, health status, and intimate, i.e., private life. Biometric data are personal data possessing physiological and biological characteristics that make it possible to identify an individual. For example, information related to an individual's DNA, voice, iris, fingerprints, facial features, height, and weight falls within this category[1].

However, it is not possible to fully agree with these views, because under the legislation of the Republic of Uzbekistan, personal information is not considered personal data. Personal information is an assessment of the degree of confidentiality of information, whereas personal data constitute a legal status attributed to the identifying characteristics of information. For this reason, the Code of the Republic of Uzbekistan on Administrative Responsibility and the Criminal Code distinguish between liability for violation of personal privacy through personal information and liability for violation of legislation on personal data. In this regard, it is understood that information concerning the private life of an individual that constitutes a personal or family secret is related to the inviolability of the individual as personal information.

Pursuant to the Law of the Republic of Uzbekistan "On Personal Data" № LRU–547 dated July 2, 2019, personal data are information recorded electronically, on paper and (or) another material medium, relating to a specific individual or enabling such individual to be identified[2].

According to A. Savelyev, "personal data are not only information that directly identifies an individual, but also any continuously changing information

[1] Ғ. Мирзо. Шахсга доир маълумотлар ҳимояси: халқаро ҳуқуқ, миллий қонунчилик ва амалий тажриба. – Т.: "Куч-адолатда" газетаси, 2023 йил 27 январь 4-сон // http://pravacheloveka.uz/uz/news/m9732.

[2] Law №. LRU–547 of the Republic of Uzbekistan "On Personal Data" dated July 2, 2019 // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

that, when combined with other data (Big Data), makes it possible to identify a specific individual."[3]. Thus, according to A. Savelyev, if there is a possibility of determining an individual's identity through indirect identification, such information is also considered personal data.

According to I. Bachilo, personal data are information relating to a specific individual, reflecting his or her identity, social status, and physiological characteristics, and having restricted access, protected by law for the purpose of ensuring the constitutional rights of the individual[4].

According to Paul M. Schwartz and Daniel J. Solove, personal data (PII) are not a permanent or strictly defined concept, but rather a continuum based on the "risk of identification." Information may not be personal in itself, but if the likelihood of linking it to a specific individual increases through its analysis within information systems, it acquires the legal status of personal data[5].

According to L. Tereshchenko, personal data are a set of information in respect of which the state establishes a special regime of confidentiality and legal protection for the purpose of ensuring a citizen's right to privacy, and the unlawful use of which may cause harm to the individual[6].

According to A. Miller, personal data are electronic records stored in computerized systems concerning an individual's behavior, financial status, or past, the uncontrolled collection and transfer of which undermines an individual's information autonomy (information autonomy)[7].

If we draw a conclusion from the above views, personal data are any information that makes it possible to identify a specific individual. The attribution of such information to a specific individual is determined through the possibility of identifying that individual. If there is no possibility of identification, such information cannot be considered personal data.

For example, if, through an individual's specific interests, third parties recognize and become able to identify the individual on the basis of information posted by a blogger on his or her blog while concealing his or her identity, this is also considered personal data. What we mean is that, in order for information to acquire the status of personal data, it is not necessary to know the individual's surname, first name, and patronymic; if there is a possibility of identifying the individual even without these details, then such information is also considered personal data.

Personal data may also remain preserved in authorial works and samples of intellectual property. For example, if everyone knows that a particular item can be

---

[3] А. Савельев Проблемы применения законодательства о персональных данных в эпоху «Больших данных» (Big Data) // Право. Журнал Высшей школы экономики. 2015. №1. URL: https://cyberleninka.ru/article/n/problemy-primeneniya-zakonodatelstva-o-personalnyh-dannyh-v-epohu-bolshih-dannyh-big-data (дата обращения: 06.08.2026).

[4] Бачило, И. Л. Б32 Информационное право : учебник для магистров / И. Л. Бачило. — 3-е изд., перераб. и доп. — М. : Издательство Юрайт, 2015. — 564 с.

[5] Paul M. Schwartz ва Daniel J. Solove. The PII Problem: Privacy and a New Concept of Personally Identifiable Information. New York University Law Review, Vol. 86, p. 1814, 2011.

[6] Л. Терещенко. Правовой режим информации. Диссертация. – Москва, 2011. - 55 с.

[7] Arthur R. Miller, The Assault on Privacy, 15 Law Quadrangle (formerly Law Quad Notes) - (1970). Available at: https://repository.law.umich.edu/lqnotes/vol15/iss2/6.

produced by only one individual and, regardless of to whom the product manufactured by that individual is presented, there is a possibility of obtaining information about a specific individual through pseudonyms, nicknames, or other identifying characteristics contained in that product, this is also recognized as personal data.

Thus, in our legislation on personal data, the view that the term personal data should be understood as information recorded electronically, on paper and (or) another material medium, relating to a specific individual or enabling such individual to be identified, is appropriate, and it should not be interpreted only in a narrow sense.

An analysis of modern and foreign legal doctrines, in particular the GDPR standards and the concept of data privacy adopted by states, demonstrates that the content and essence of personal data are not limited solely to traditional details (full name, passport information).

Therefore, when formulating a fundamental definition of the concept of personal data, it is necessary to develop its doctrinal content independent of technological or temporal means.

Personal data – any protected information that, regardless of its material or virtual (cyber, including digital) form, as well as the processing technology, makes it possible to directly or indirectly identify a specific individual and determine his or her information sovereignty.

In this regard, the criterion for attributing information to an individual is manifested not in the fact that the individual is directly named therein, but in the existence of the possibility of recognizing and distinguishing (singularizing) that individual from others through various indirect indicators (intellectual property pseudonyms, behavioral profiles, or digital footprints).

From the perspective of processing personal data, it consists of the following participants:

---

personal data subject (subject) – an individual to whom the personal data relate;

personal data database operator (operator) – a state body, individual and (or) legal entity carrying out the processing of personal data;

personal data database owner (owner) – a state body, individual and (or) legal entity having the right to own, use, and dispose of the personal data database;

third party – any person who is not a subject, owner, and (or) operator, but is connected with them through circumstances or relations concerning the processing of personal data.

The concept of processing personal data is defined very narrowly in our national legislation, according to which, **processing of personal data** means the performance of an action or a set of actions involving the collection, systematization,

storage, modification, supplementation, use, provision, dissemination, transfer, depersonalization, and destruction of personal data[8].

However, it should be emphasized that the **"processing" (processing – обработка) institution** occupies a central position in determining the legal regime of personal data. An analysis of national legislation and international practice (the EU GDPR Regulation and Convention 108) demonstrates that data processing is not merely a set of individual actions, but rather a dynamic legal process encompassing the entire life cycle of information, from its emergence to its complete termination. From this perspective, **processing of personal data** is a set of unified operational and analytical actions performed on data, regardless of whether they are carried out in an automated or traditional (destructive) form, as well as regardless of the technological methods applied in terms of time and space:

information generation and collection (collection, acquisition, initial processing, and identification of sources);

systematization and decomposition into structural components (systematization, classification, formation of databases);

dynamic modernization and supplementation (modification, editing, addition, updating);

static and virtual storage (storage, archiving, retention in cloud and physical memory);

analysis and functional use (use thereof, algorithmic processing, profiling, application in decision-making);

transformation and communication (provision, dissemination, transfer, implementation of cross-border flows);

anonymization and differentiation (depersonalization, anonymization, severing of links);

final termination (destruction, irreversible deletion, or loss).

In almost all national and foreign legal systems, the institution of "processing" of personal data is recognized as a dynamic life cycle (lifecycle processing) encompassing all processes from the emergence (genesis) of information to its pseudonymization, terminology, and complete destruction (deletion). However, the dogmatic and enumerative (aggregated) description of this concept in legislation creates a risk of artificially narrowing its actual legal content. Although the actions of "transfer," "provision," or "dissemination" of personal data are expressly established in our current national legislation as stages of processing, the doctrinal and normative form of active or passive actions such as "retrieval" and "acceptance" of such information remains open. This creates serious legal collisions and a "legal gap" (lacuna in lege) in the qualification of unlawful acts committed in cyberspace. To understand this situation more precisely, let us consider several examples:

Example 1: A cybercriminal obtains, through social engineering or fake phishing web pages, the bank card details, PIN code, and biometric logins of the personal data subject without the owner's knowledge or consent. Criminal law

[8] Law № LRU–547 of the Republic of Uzbekistan "On Personal Data" dated July 2, 2019 // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

punishes the unauthorized nature of this action. Therefore, instead of "unlawful acquisition," it is necessary to introduce the concepts of "unauthorized access" and "data breach" within information security systems as separate institutions in the legislation.

Example 2: A cybercriminal sends malicious software to a local server, encrypts a personal data database, and engages in cyber-extortion in exchange for returning the data to its owner or refraining from disclosing it. In this case, the cybercriminal may not have transferred or disseminated the data to a third party; he or she has merely "unlawfully accessed and taken possession of" the data. If "obtaining and possessing" are not qualified as processing, the chain of criminal liability is broken.

Example 3: An extortionist or hacker "purchases" or "downloads" a leaked (data breach) database containing the personal data of millions of citizens from a Darknet forum. He or she has not yet disseminated this data to anyone, but merely stores it in his or her own system. If the act of "obtaining" data itself is not clearly defined in the disposition, bringing such an act within the scope of a criminal offense becomes more complicated.

When a legal gap similar to these three cases comes into conflict with constitutional principles, the inevitability of fair punishment is placed at risk. Our Constitution establishes the principle of *in dubio pro reo* (resolution of doubts in favor of the accused); pursuant to Articles 20 and 21 of the Constitution of the Republic of Uzbekistan, all contradictions and ambiguities in legislation arising in relations between an individual and state bodies shall be interpreted in favor of the individual. At the same time, no person may be imposed, without his or her consent, an obligation not established by legislation[9]. *Nullum crimen sine lege*, that is, there is no crime without a law, and taking into account that the application of analogy is prohibited in criminal and administrative law, the offender may remain unpunished. If the Criminal Code or the relevant regulatory legal act does not directly specify the "unlawful obtaining" or "possession" of personal data as a culpable act (a form of processing), the court will be compelled to find that there are no elements of an offense in the offender's actions and, relying on the constitutional principle of *in dubio pro reo*, acquit him or her. To explain this situation more precisely, Article 165 of the Criminal Code provides that extortion is understood to include demanding that another person transfer property or property rights, provide property benefits, or perform acts of a proprietary nature by threatening to destroy, modify, seize, or block the victim's information resource, or to disclose information that should be kept secret from the victim, or to disseminate fabrications that disgrace the victim, or placing the victim in circumstances that compel him or her to transfer his or her property or rights to property[10], If this information resource is personal data, then in this situation, in addition to extortion, if the offender's actions constitute the unlawful or forcible obtaining of personal data, taking into account the time at which

[9] Constitution of the Republic of Uzbekistan // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

[10] Criminal Code of the Republic of Uzbekistan // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

extortion is deemed completed, the acts committed in the form of extortion would, in this case, constitute two separate offenses. This means that if the offender unlawfully obtained an information resource and that resource contains personal data, the offender's actions must be qualified under two separate articles. Accordingly, in order to eliminate this systemic problem and stabilize the mechanism of criminal-law protection, it is necessary to supplement the concept of "processing of personal data" with a universal concept such as "unlawfully obtaining, possessing, and creating the possibility of using [personal data] by any means." This interpretation will not only close the existing gap in national legislation, but will also create a strong legal immunity against the unlawful circulation of personal data as a result of any cybercrime that may emerge in the future.

Personal data may be introduced into circulation and processed in databases in various forms and on various platforms – information and communication systems, data banks, websites, messengers, cloud storage, as well as any digital and analog means that enable the storage and processing of personal data. Our national legislation provides a legal definition of the concept of a "personal data database," establishing it as a "database in the form of an information system containing personal data." However, this normative description is very narrow (dogmatic) and does not fully meet the requirements of the current era of digital transformation and cybernetics. From a technical and legal perspective, when a data source is autonomously processed in real-time not merely by a traditional "information system," but by Artificial Intelligence (AI), Machine Learning, and Neural Networks integrated into software, it remains unclear and constitutes a legal gap (lacuna) whether the new information resources emerging as a result of such processing fall within this database. For example:

Example 1: An artificial intelligence model collects facial images and voice samples of individuals from millions of open sources (social networks, video-hosting platforms) and processes them within its algorithms. As a result, artificial intelligence does not form a distinct database of the individual, but creates his or her digital avatar (Deepfake) or synthetic biometric model. If the concept of a "database" in legislation is regarded only as a traditional information system in the form of a table, such synthetic data encrypted within artificial intelligence and transformed into neural connections would fall outside the status of a "personal data database." This, in turn, would enable a cybercriminal to evade liability.

Let us consider **Example 2**: bots operating in messengers such as Telegram or WhatsApp and connected to large language models (LLM) receive personal documents, audio messages, and medical information sent by users and process them within a cloud-based neural network. The source is not stored directly in an "information system," but in the messenger API interface and an artificial intelligence algorithm located on foreign servers. Due to the narrow definition in legislation, localizing these artificial intelligence environments or recognizing the data contained therein as an "unlawful database" becomes difficult.

Another example is Face-ID cameras installed in public places and connected to artificial intelligence, which identify (reconnaissance) individuals from video

streams in real time and analyze their movement patterns. Artificial intelligence may analyze this data in operational memory (RAM) without storing it in a traditional database, and may immediately delete it or convert it into a vector. If one adheres strictly to the concept of a "database in the form of an information system," such "processing" and "database formation" actions performed by artificial intelligence in operational memory would remain outside the legal regime.

To eliminate this problem, it is necessary in legal science to harmonize the concepts of an "Information System" and a "Software-Algorithmic Environment." A traditional information system is a passive and static data repository (passport information, addresses). An artificial intelligence database, by contrast, is an active, self-learning, and dynamic algorithmic system.

The European Union's GDPR Regulation[11] and the European Union's "Artificial Intelligence Act" (AI Act) [12] understand a database not as a single server or system, but as "any structured set of data accessible according to specific criteria and the algorithmic systems that process them."

Accordingly, it should be stated that, in order to prevent the emergence of legal gaps due to technological changes, it is necessary to revise the concept of a "personal data database" in legislation based on the principle of technological and platform neutrality (technological neutrality). That is, a personal data database is a structured information resource and virtual collection thereof, whether centralized or decentralized, formed in traditional information systems, software, artificial intelligence models, and algorithmic environments, which enables an individual to be identified regardless of its form and method of processing. Such a doctrinal approach will serve to fully ensure the cybersecurity and criminal-law protection of personal data in the era of artificial intelligence and neural networks. In other words, it is incorrect to understand a personal data database as being linked exclusively to an information system, and in this respect, this concept should also be reconsidered in our legislation. At the same time, even if personal data are not stored in a static database, if they are processed through algorithmic or neural network systems in real time for the purpose of analyzing (profiling) an individual's behavior, biometrics, or appearance, this process shall be recognized as a separate form of processing personal data, and the consent of the data owner shall be required. Such an approach will neither hinder innovation nor leave individual rights unprotected against threats posed by artificial intelligence.

The personal data processed in databases consist of special, biometric, genetic, and publicly accessible data in accordance with Articles 25, 26, and 29 of the Law of the Republic of Uzbekistan "On Personal Data." They include the following:

special data – a set of highly sensitive (sensitive) information revealing a person's racial or national affiliation, political views, religious or philosophical beliefs, membership in trade unions, as well as the state of his or her physical or mental health and intimate (private) life, in respect of which legislation establishes

[11] https://eur-lex.europa.eu/eli/reg/2016/679/oj.
[12] https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai.

the highest level of confidentiality and legal protection, and the disclosure of which may result in the violation of the fundamental rights of the individual;

biometric data – measured indicators describing the anatomical, physiological, and biological characteristics of an individual (facial structure, dactyloscopic fingerprints, retina, voice timbre, and others), enabling the individual's identity to be identified accurately, reliably, and unchangeably, and serving as a central basis for forming the subject's digital image;

genetic data – information resources relating to the inherited or acquired characteristics of an individual, providing unique information about his or her physiology or health and, as a rule, obtained as a result of clinical and algorithmic analysis of biological samples (DNA, RNA), expressing the biological sovereignty of the individual;

publicly accessible data – information made openly available for free access by an unlimited circle of persons with the subject's own will and voluntary consent, or information to which a confidentiality (inviolability) regime is not applied in accordance with legislation, circulating in public sources (open registers, reference materials, mass media), and integrated into society.

According to the legislation, **material objects** means material objects on which information constituting personal data is recorded, including tangible objects, documents containing personal data, and **material objects made of paper or plastic** means text, graphic, and other information printed on paper, plastic cards, and others[13].

Accordingly, national legislation presupposes that personal data are linked exclusively to material objects, including material objects consisting of paper or plastic; however, in our view, limiting the protection of personal data solely to material objects and paper form is conceptually incorrect from the perspective of the doctrine of information law and digital jurisprudence. From the perspective of the theory of information law and the protection of digital assets, the erroneous nature of this approach and the resulting lack of protection of digital assets can be substantiated by the following principal scientific and legal arguments:

1. In the doctrine of information law, personal data constitute an intangible (immaterial) good and an independent object of legal relations. A material object (paper, plastic, server) is merely a temporary carrier (medium) of information. Personal data contained in digital assets (for example, tokenized assets, smart contracts, Web3, and decentralized identifiers – DID) do not have a classical physical source, but exist in the form of abstract code, cryptographic hashes, and distributed virtual memory (IPFS, blockchain nodes). Linking information to a material object artificially narrows its legal nature.

2. Metadata, crypto-wallet addresses, digital footprints, and algorithmic profiles contained in digital assets make it possible to directly or indirectly identify the subject. If the protection mechanism is directed only at the forms of "material object" and "paper," digital assets processed in decentralized ledgers, cloud systems,

[13] Regulation "On the Requirements for Material Carriers Containing Biometric and Genetic Data and Technologies for Storing Such Data Outside Personal Data Databases", approved by Resolution № 570 of the Cabinet of Ministers dated October 5, 2022 // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

and artificial intelligence models will remain outside the legal regime (extra legem), leaving unresolved the issue of liability for their unlawful appropriation or de-anonymization.

3. In accordance with the UNCITRAL Model Law on Electronic Commerce and international GDPR standards, the digital or electronic form of information and its traditional paper or physical form have absolutely equal legal force. Article 3 of the Law of the Republic of Uzbekistan "On Personal Data" also expressly recognizes the recording of information "in electronic form." Therefore, emphasizing only material objects merely clarifies the conditions of physical security, but cannot restrict the institutional definition of personal data.

4. In modern cyberspace, threats to personal data arise not through the theft or damage of a physical source, but at the logical and software level (unauthorized access, API data leakage, information embedding into AI models, and vulnerabilities in smart contracts). Giving priority to the "physical carrier" as the object of protection leaves the logical and software layer of cybersecurity without legal guarantees.

For this reason, in accordance with the cyberalogy concept, the legal protection of personal data should be based not on the form in which they are recorded, stored, or transmitted, but, first and foremost, on their belonging to a particular individual and the possibility of directly or indirectly identifying that individual. From the perspective of scientific and legal as well as legislative drafting technique, it is advisable to recognize not the material or digital carrier of personal data, but rather the substantive essence of the data, their objective connection with a particular individual, and the characteristics that create the possibility of their identification or re-identification (re-identification) as the object of legal protection.

Such an approach ensures the technology-neutral principle of personal data protection, enabling the application of uniform legal protection standards to data regardless of whether they exist in a paper, plastic, electronic, digital, virtual, cloud-based, or distributed information environment. As a result, the object of legal protection becomes linked not to the external form of expression of the data, but to their relevance to an individual, identification potential, and the legal nature of the processing carried out in relation to them.

1.2. System of Legislation on Personal Data

The system of legislation on personal data refers to the types of legislative acts that legally regulate this type of data. A normative legal act is an official document adopted in accordance with legislation and aimed at establishing, amending, or repealing legal norms as generally binding state directives. Normative legal acts are legislative acts that constitute the legislation of the Republic of Uzbekistan. The Constitution and laws of the Republic of Uzbekistan, as well as resolutions of the chambers of the Oliy Majlis of the Republic of Uzbekistan, are legislative acts. Decrees and resolutions of the President of the Republic of Uzbekistan, resolutions of the Cabinet of Ministers of the Republic of Uzbekistan, orders and resolutions of ministries and agencies, and resolutions of local government authorities are subordinate legislation[14].

Accordingly, the types of legislation on personal data consist of the following:
The Constitution of the Republic of Uzbekistan;
Laws of the Republic of Uzbekistan;
Resolutions of the chambers of the Oliy Majlis of the Republic of Uzbekistan;
Decrees and resolutions of the President of the Republic of Uzbekistan;
Resolutions of the Cabinet of Ministers of the Republic of Uzbekistan;
Orders and resolutions of ministries and agencies;
Resolutions of local government authorities.
The system of legislation on personal data in Uzbekistan is as follows:

№	Name of the Legislative Document	Regulated Social Relations
Law of the Republic of Uzbekistan		
1.	Constitution of the Republic of Uzbekistan	**Article 31.** Everyone has the right to privacy, to the confidentiality of personal and family secrets, and to the protection of their honour and dignity.
2.	Code of the Republic of Uzbekistan on Administrative Liability	**Article 46^2. Violation of Legislation on Personal Data** Unlawful collection, systematization, storage, modification, supplementation, use, provision, dissemination, transfer, depersonalization and destruction of personal data, as well as failure to comply with the requirements for the collection, systematization and storage of personal data on technical means physically located within the territory of the Republic of Uzbekistan and in personal data databases registered in accordance with the established

[14] Law № LRU–682 of the Republic of Uzbekistan "On Regulatory Legal Documents" dated April 20, 2021 // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

		procedure in the State Register of Personal Data Bases when processing personal data of citizens of the Republic of Uzbekistan using information technologies, including the World Wide Web, – shall entail the imposition of a fine on citizens in the amount of seven times the basic estimated value, and on officials in the amount of fifty times the basic estimated value. Unlawful processing of personal data using artificial intelligence technologies, and dissemination thereof through mass media, telecommunications networks or the World Wide Web, – shall entail the confiscation of the instruments used to commit the administrative offense and the imposition of a fine in the amount of fifty to one hundred times the basic estimated value.
3.	Criminal Code of the Republic of Uzbekistan	**Article 141[2]. Violation of Legislation on Personal Data** Unlawful collection, systematization, storage, modification, supplementation, use, provision, dissemination, transfer, depersonalization and destruction of personal data, as well as failure to comply with the requirements for the collection, systematization and storage of personal data on technical means physically located within the territory of the Republic of Uzbekistan and in personal data databases registered in accordance with the established procedure in the State Register of Personal Data Bases when processing personal data of citizens of the Republic of Uzbekistan using information technologies, including the World Wide Web, if such acts were committed after the imposition of an administrative penalty for the same acts, – shall be punishable by a fine in the amount of one hundred to one hundred and fifty times the basic estimated value, or deprivation of a certain right for up to three years, or correctional labour for up to two years. The same acts: a) committed by a group of persons upon prior conspiracy;

		b) repeatedly or by a dangerous recidivist; c) for mercenary or other base motives; d) committed using official position; e) resulting in grave consequences, – shall be punishable by a fine in the amount of one hundred and fifty to two hundred times the basic estimated value, or correctional labour for a period of two to three years, or restriction of liberty for a period of one to three years, or imprisonment for up to three years.
4.	Tax Code of the Republic of Uzbekistan	**Article 132. Taxpayer Registration Information** The registration information concerning individuals includes the following personal data: 1. surname, first name, and patronymic; 2. citizenship; 3. personal identification number of the individual; 4. series and number of the passport or identification ID card, date and place of issue; **5.** place of residence (address).
5.	Election Code of the Republic of Uzbekistan	Dissemination of false information, violation of the confidentiality of personal data, as well as dissemination of information that undermines the honour and dignity of candidates is prohibited.
6.	Labour Code of the Republic of Uzbekistan	**§ 6. Protection of the Employee's Personal Data** **Article 175. Employee's Personal Data** Information about facts, events and circumstances in the life of an employee, as well as his or her family members, provided to the employer in connection with employment relations, constitutes the employee's personal data. The following information about the employee constitutes personal data: surname, first name, patronymic, date and place of birth; personal identification number of the individual (if available); education (when and which educational organizations were completed, diploma numbers, field of training or specialty according to the diploma, qualification);

		work performed since the commencement of employment (including military service); address of permanent or temporary place of residence registration; passport information (series, number, by whom and when issued) and identification ID-card information; personal telephone number, e-mail address; military status, military registration information (for citizens in the reserve and persons subject to conscription for military service); taxpayer identification number; number of the individual accumulative pension account; results of mandatory medical examinations; grounds for termination of the employment contract with the employee; marital status, surnames, first names, patronymics and dates of birth of close relatives; other information about facts, events and circumstances in the life of the employee and/or his or her family members that have become known to the employer. Information concerning the employee's personal data belongs to the category of confidential information. **Article 176. General Requirements and Guarantees for the Protection of Employee's Personal Data during Their Processing** When processing personal data (when carrying out a single action or a set of actions involving the collection, systematization, storage, modification, supplementation, use, provision, dissemination, transfer, depersonalization and destruction of personal data), the employer and its representatives shall: comply with the provisions of the legislation on personal data when determining the scope and content of the employee's personal data to be processed; obtain all personal data of the employee directly from the employee. If the employee's personal data can only be obtained from third parties, the employee must be notified thereof in

		advance in writing and his or her written consent must be obtained, except for cases where personal data (results of medical examinations, conclusions based on the results of qualification and other assessments within the framework of professional development, and others) are obtained from those third parties to whom the employee was sent by this employer in accordance with the legislation; notify the employee of the purposes, intended sources and methods of obtaining personal data, as well as the nature of the personal data to be obtained and the consequences of the employee's refusal to give written consent to obtain them; ensure, at the employer's own expense, protection of the employee's personal data against unlawful use or loss; familiarize employees and their representatives, against signature, with the documents available at the employer that establish the procedure for processing employees' personal data, as well as their rights and obligations in this area; develop, jointly with representatives of employees, measures to protect employees' personal data. Unless otherwise provided by this Code or another law, the employer and its representatives shall not have the right to obtain or process personal data concerning an employee's membership in public associations or activities in a trade union. The use of an employee's personal data by the employer's representatives shall be carried out only in accordance with the employee's employment duties. The employer's representatives who process employees' personal data shall not disclose personal data entrusted to them or which became known to them in connection with the performance of their employment duties. **Article 177. Invalidity of the Terms of an Employment Contract and Provisions of Internal Documents Concerning the**

		Employee's Refusal to Have His or Her Personal Data Protected The terms of an employment contract, other agreements between the employee and the employer, and provisions of internal documents that provide for the employee's refusal to have his or her personal data protected or worsen the employee's position in the field of protection of his or her personal data in comparison with the legislation shall be invalid. **Article 178. Storage, Use and Provision of Employees' Personal Data** The procedure for storing, using and providing employees' personal data shall be established by the employer in compliance with the requirements of this Code and other laws. When providing the employee's personal data, the employer shall comply with the following requirements: not disclose the employee's personal data to a third party without the employee's written consent, except in cases where disclosure is necessary for the purpose of preventing a threat to the life and health of the employee, as well as in other cases provided for by this Code and other laws; not disclose the employee's personal data for commercial purposes without the employee's written consent; warn persons receiving the employee's personal data that such data may be used only for the purposes for which they were disclosed and require confirmation from such persons that this rule has been complied with. Persons receiving the employee's personal data shall comply with the confidentiality regime. This rule shall not apply to the exchange of employees' personal data in accordance with the procedure established by this Code and other laws; provide the employee's personal data within a single organization, with an individual entrepreneur, in accordance with an internal document with which the employee must be familiarized against signature;

		allow access to the use of employees' personal data only to specially authorized persons, provided that such persons shall have the right to obtain only the personal data of the employee that are necessary for the performance of specific employment duties; not request information about the employee's state of health, except for information related to the issue of the employee's ability to perform the employment duties; provide the employee's personal data to employees' representatives in accordance with the procedure established by this Code and other laws and limit this information only to the personal data necessary for the performance of their duties by the specified representatives. **Article 179. Employee's Rights to Ensure the Protection of His or Her Personal Data Stored by the Employer** For the purpose of ensuring the protection of personal data stored by the employer, the employee shall have the following rights: to receive complete information about his or her personal data and the processing of such data; to freely and without charge access his or her personal data, including the right to obtain copies of any record containing the employee's personal data, except in cases provided for by law; to designate a representative for the protection of his or her personal data; to access medical documents reflecting his or her state of health; to demand the removal or correction of inaccurate personal data or the supplementation of incomplete data, as well as data processed in violation of the requirements of this Code or other laws; to demand that the employer notify all persons to whom the employee's inaccurate or incomplete personal data had previously been disclosed of all exclusions, corrections or additions made to such data; to appeal against all unlawful decisions, actions (inaction) of the employer in the processing

		and protection of his or her personal data, including by appealing to the court. If the employer refuses to remove, correct or supplement the employee's personal data, the employee shall have the right to notify the employer in writing of his or her disagreement with the relevant grounds. **Article 180. Legal Consequences of Violation by the Employer of the Procedure for Processing and Protecting the Employee's Personal Data** If a violation by the employer of the procedure for processing and protecting the employee's personal data results in the employee being unlawfully deprived of the opportunity to work or leads to a reduction in the amount of remuneration for the employee's work, the obligation to compensate the employee for the lost wages shall be imposed on the employer through whose fault the violation was committed. If the employer disseminates information that tarnishes the employee's reputation and does not correspond to reality, the employer shall be obliged to refute such information.
7.	Law № 560-II of the Republic of Uzbekistan "On Informatization" dated December 11, 2003	**Article 12[1]. Dissemination of Information Freely Accessible to Everyone on the World Wide Web** The owner of a website and/or a website page or other information resource, including a blogger, shall not allow their website and/or website page or other information resource on the World Wide Web, where information freely accessible to everyone is posted, to be used for the unlawful processing of personal data using artificial intelligence technologies or for the dissemination thereof through mass media, telecommunications networks or the World Wide Web.
8.	Law № LRU–395 of the Republic of Uzbekistan "On Electronic Government" dated December 9, 2015	**Article 12. Principle of Ensuring Information Security and Cybersecurity of Information Systems and Information Resources of Electronic Government** State bodies providing electronic public services shall take the necessary organizational and

		technical measures to ensure the protection of personal data, as well as information constituting state secrets or other secrets protected by law, and to prevent unauthorized access thereto. Personal data stored in the information systems and information resources of state bodies providing electronic public services shall be used for their processing, transfer and receipt with the consent of the applicant to whom such data relate, except in cases established by legislation. **Article 20. Requirements for Electronic Public Services** Interactive public services shall ensure the secure use by applicants of services involving the processing of personal data.
9.	Law № LRU–474 of the Republic of Uzbekistan "On Public Control" dated April 12, 2018.	**Article 7:** It is established that the right of subjects of public control to obtain information may be restricted if such information constitutes personal data, state secrets, or other information constituting a secret protected by law.
10.	Law № LRU–547 of the Republic of Uzbekistan "On Personal Data" dated July 2, 2019.	regulates relations in the field of personal data.
11.	Law № LRU–578 of the Republic of Uzbekistan "On Payments and Payment Systems" dated November 1, 2019.	**Article 22. Procedure for Licensing the Activities of Payment System Operators** The bank's application for a license shall be accompanied by a document on the security policy, including a detailed risk assessment, as well as a description of measures to be taken to ensure information security and cybersecurity and to protect users of payment services, including measures to reduce risks, including the risks of fraud and unlawful use of confidential and personal data. **Article 24. Procedure for Licensing the Activities of Payment Organizations** The application for a license shall be accompanied by a description of measures to be taken to reduce the risks of unlawful use of personal data.

		Article 28. Supervision over the Operation of Payment Systems In exercising supervision over the operation of payment systems, the Central Bank shall request from payment system operators and payment organizations information related to the operation of payment systems, including information containing personal data. **Article 53. Requirements and Procedure for the Protection of Information in the Payment System** Payment system operators and payment service providers may use, process and store only the personal data necessary for the provision of payment services, and they shall not have the right to request from users of payment services any information other than the information necessary for the provision of services.
12.	Law № LRU–580 of the Republic of Uzbekistan "On Amendments and Additions to the Law of the Republic of Uzbekistan 'On Banks and Banking Activities'" dated November 5, 2019.	**Article 48. Consolidated Supervision** The Central Bank shall have the right to conclude written agreements on coordination and cooperation with banking supervisory authorities of other countries (if any) for the purpose of organizing effective cooperation, exchanging information and establishing effective supervision on a consolidated basis, while complying with the laws of those countries protecting secrets, personal data and the procedure for access to confidential information.
13.	Law № LRU–611 of the Republic of Uzbekistan "On Population Census" dated March 16, 2020.	**Article 8. Principle of Universality and Simultaneity** The collection of personal data from all respondents on the single established date of the population census shall be carried out simultaneously throughout the territory of the Republic of Uzbekistan or in its specific territories. **Article 9. Principle of Individuality of the Census** When collecting personal data, a census form shall be completed individually for each respondent. **Article 10. Principle of Confidentiality of Personal Data**

		Personal data collected during the population census shall be confidential and shall not be disclosed or disseminated without the consent of the respondent. **Article 15. Specially Authorized State Body in the Field of Population Census** The specially authorized state body shall determine the procedure for selecting and training census-taking employees, as well as the procedure for processing personal data, and shall carry out their processing. **Article 19. Rights and Obligations of Respondents** Respondents shall have the right to: know for what purpose their personal data are being collected, and who and how will use such data; familiarize themselves with the census forms completed for them and verify the completeness and reliability of the personal data entered in the census forms; provide reliable personal data in accordance with the form of the census questionnaire. **Article 20. Rights and Obligations of Census-Taking Employees** Census-taking employees shall have the right to obtain personal data from respondents in accordance with the census form. Before beginning the collection of personal data, census-taking employees shall show the respondent their identification document, ensure the confidentiality of personal data, and not disclose their content. **Article 21. Population Census Program** The list of questions through which personal data are collected constitutes the Population Census Program. The Population Census Program shall include the following questions: surname, first name, patronymic; date and place of birth; age; sex; nationality;

		citizenship; place of residence (place of stay); knowledge of languages; education; marital status; number of children; household composition; housing conditions; employment; sources of means of subsistence; migration (internal and external). Additional questions may be included in the Population Census Program in accordance with a resolution of the Cabinet of Ministers of the Republic of Uzbekistan. It shall not be permitted to include questions the answers to which may contain information relating to state secrets or other secrets protected by law, or which violate the rights, freedoms and legitimate interests of citizens. The forms of census questionnaires shall be developed and approved on the basis of the Population Census Program. **Article 22. Pilot Population Census** A pilot population census is the testing, in one or several administrative-territorial units, of the draft Population Census Program and the forms of census documents, the collection and processing of personal data, as well as the main measures for preparing for and conducting the population census. The procedure for conducting a pilot population census shall be determined by the Cabinet of Ministers of the Republic of Uzbekistan. **Article 23. Procedure for Collecting Personal Data** The collection of personal data shall be carried out by visiting residential premises and other premises where respondents live (stay), or by interviewing respondents and completing census forms in premises provided for these purposes by local executive authorities.

		The collection of personal data may also be carried out through the use of information and communication technologies, taking into account the requirements for ensuring information security. Respondents shall be interviewed in the state language. Respondents who do not know the state language may be interviewed in their native language or in a freely chosen language of communication. Census forms shall be completed by census-taking employees on the basis of the respondents' statements. During the period of conducting the population census, personal data concerning respondents who are absent from their place of residence (stay), or who have minor persons, shall be provided by adult members of their household. Personal data concerning persons for whom guardianship or trusteeship has been established shall be provided by their guardians or trustees. If a respondent refuses to answer the questions in the census form, the census form shall be completed on the basis of information available from citizens' self-government bodies or local executive authorities. The collection of personal data on questions not provided for in the Population Census Program shall be prohibited. **Article 24. Collection of Personal Data in Relation to Certain Categories of the Population** The collection of personal data concerning respondents who, on the date of the population census, are military personnel undergoing fixed-term military service upon conscription, as well as military personnel engaged in military service under contract and their family members living in closed areas, shall be carried out by the commander of the military unit or a person authorized by him or her. On the date of the population census: children living in boarding schools, educational institutions, and "Children's Towns"; social institutions; religious institutions;

		hospitals and other healthcare organizations; women's rehabilitation and adaptation centers; places of detention, pre-trial detention facilities, correctional institutions and special institutions; the collection of personal data concerning respondents living (staying) in the institutions and organizations specified in this part shall be carried out by the administrations of such institutions and organizations. Citizens of the Republic of Uzbekistan who are employees of diplomatic missions and consular institutions of the Republic of Uzbekistan, as well as representative offices of the Republic of Uzbekistan to international organizations, and their accompanying family members, including citizens sent by the Ministry of Foreign Affairs of the Republic of Uzbekistan to quota positions in international intergovernmental organizations, shall be registered by the Ministry of Foreign Affairs of the Republic of Uzbekistan. Foreign citizens who are employees of permanent missions of foreign states, international and intergovernmental organizations, and representative offices of governmental organizations of foreign states accredited by the Ministry of Foreign Affairs of the Republic of Uzbekistan, and their family members, as well as other persons enjoying diplomatic privileges and immunities in accordance with international treaties of the Republic of Uzbekistan, shall not be registered. **Article 25. Final Data of the Population Census** The aggregated statistical information generated as a result of the collection and processing of personal data constitutes the final data of the population census.
14.	Law № LRU–642 of the Republic of Uzbekistan "On Employment of the	**Article 116. Protection of Personal Data** The protection of personal data used in the interdepartmental software complex "Unified National Labour System" shall be carried out in

	Population" dated October 20, 2020.	accordance with the Law of the Republic of Uzbekistan "On Personal Data".
15.	Law № LRU–649 of the Republic of Uzbekistan "On State Genomic Registration" dated November 24, 2020.	genomic information – personal data containing encoded information about specific sections of the deoxyribonucleic acid (hereinafter referred to as DNA) of a person or an unidentified corpse; This Law regulates relations in the field of state genomic registration.
16.	Law № LRU–703 of the Republic of Uzbekistan "On Courts" dated July 28, 2021.	**Article 61. Rights of a Judge** A judge shall have the following rights: to obtain, free of charge, information necessary for the administration of justice from the information systems of state bodies and other organizations and to use information systems containing personal data, including remotely; to obtain, free of charge and without the written consent of citizens, personal data necessary for the administration of justice from the information systems of state bodies, as well as other organizations.
17.	Law № LRU–706 of the Republic of Uzbekistan "On Transport" dated August 9, 2021.	**Article 35. Inspection at Transport Infrastructure Facilities** The procedure for forming and maintaining automated centralized personal data databases concerning passengers, as well as the procedure for providing the data contained therein, shall be determined by the Cabinet of Ministers of the Republic of Uzbekistan. Transport organizations or carriers of foreign states carrying out international transportation to the Republic of Uzbekistan shall ensure the transfer of data contained in transportation documents (tickets) into automated centralized personal data databases concerning passengers.
18.	Law № LRU–707 of the Republic of Uzbekistan "On Official Statistics" dated August 11, 2021.	Other producers of official statistics shall process, disseminate and store the collected data in accordance with the provisions of this Law and the Law of the Republic of Uzbekistan "On Personal Data".
19.	Law № LRU–788 of the Republic of	**Article 31. Personal File of a Civil Servant**

	Uzbekistan “On Civil Service” dated August 8, 2022.	The personal file of a civil servant consists of his or her personal data and information concerning his or her performance of civil service.
20.	Law № LRU–792 of the Republic of Uzbekistan “On E-Commerce” dated September 29, 2022.	**Article 12. Rights and Obligations of E-Commerce Operators** E-commerce operators shall ensure measures to protect electronic documents, electronic messages and personal data against unauthorized access.
21.	Law № LRU–868 of the Republic of Uzbekistan “On the State Border of the Republic of Uzbekistan” dated September 13, 2023.	**Article 56. Rights and Obligations of Legal Entities Carrying Out International Passenger Transportation** Legal entities carrying out international passenger transportation shall have the right to: obtain information on the procedure for crossing the State Border; in accordance with the legislation on personal data, collect, process, store and use passengers’ personal data without their written consent.
22.	Law № LRU–931 of the Republic of Uzbekistan “On Conflict of Interests” dated June 5, 2024.	**Article 22. Ensuring the Confidentiality of Documents Related to Conflict of Interests** Disclosure of personal data of persons entrusted to employees involved in the identification and regulation of conflicts of interest or which became known to them in connection with the performance of their professional, official or employment duties shall not be permitted. During the regulation of a conflict of interests in the activities of an employee of a state body or other organization, the protection of personal data shall be carried out in accordance with the legislation on personal data.
23.	Law № LRU–938 of the Republic of Uzbekistan “On Probation” dated August 7, 2024.	**Article 47. Socio-Psychological Profile of a Person under Probation Supervision** Within ten working days from the date a person is placed under probation registration, an individual socio-psychological profile of the person under probation supervision shall be compiled by an employee of the district (city) probation unit and a specialist psychologist based on the results of assessing his or her specific individual characteristics, psychological traits and behavior.

		The socio-psychological profile of a person under probation supervision shall reflect personal data, including special personal data.
24.	Law № LRU–996 of the Republic of Uzbekistan "On Protecting Children from All Forms of Violence" dated November 14, 2024.	**Article 42. Confidentiality of Information** All personal data that become known to persons who have provided assistance to a victim of violence shall be protected by the legislation on personal data. Persons to whom the personal data of a victim of violence have been entrusted, or who have become aware of such data in connection with the performance of their professional, official or employment duties, and who have allowed the disclosure of such data shall be held liable as provided by law.
Decrees of the President of the Republic of Uzbekistan		
1.	Decree № DP–113 of the President of the Republic of Uzbekistan "On Additional Measures to Simplify the Provision of Public Services, Reduce Bureaucratic Barriers and Develop the National Public Services Provision System" dated April 20, 2022.	**8.** In order to ensure the confidentiality and reliable protection of personal data, the following procedure for obtaining personal data using the "Electronic Government" system shall be introduced from August 1, 2022: when personal data are requested by state bodies through the "Electronic Government" system, a notification thereof shall be sent to the personal account of the personal data subject in the Unified Interactive Public Services Portal (YIDXP) or to the mobile phone number identified through the Mobile-ID system (except in cases involving state secrets and information whose use is restricted in accordance with legislation); when performing works and providing services by business associations, state organizations and institutions, and non-governmental organizations authorized to use the "Electronic Government" system, personal data shall be provided through the "Electronic Government" system with the consent of the personal data subject. In this case, the data shall be provided to the relevant organization through the "Electronic Government" system after obtaining confirmation from the personal account of the personal data subject in the Unified Interactive Public Services Portal (YIDXP) or from the mobile

<table>
<tr><td></td><td></td><td>phone number identified through the Mobile-ID system.</td></tr>
<tr><td>2.</td><td>Decree № DP–157 of the President of the Republic of Uzbekistan “On Additional Measures to Improve the Public Services Provision System and Radically Reduce Bureaucratic Procedures in the Field” dated September 8, 2025.</td><td>
DECREE № DP–157 OF THE PRESIDENT OF THE REPUBLIC OF UZBEKISTAN DATED SEPTEMBER 8, 2025
ANNEX 2
LIST
of Personal Data Belonging to an Individual and Provided in Real-Time Mode on the Unified Interactive Public Services Portal
<table>
<tr><th>№</th><th>Name of Personal Data</th><th>Authorized Body Responsible for Providing the Data</th></tr>
<tr><td>1.</td><td>Information on whether or not the person is registered with a narcological dispensary</td><td rowspan="3">Ministry of Health
Ministry of Internal Affairs
Ministry of Higher Education, Science and Innovation</td></tr>
<tr><td>2.</td><td>Information on whether or not the person is registered with a psychiatric dispensary</td></tr>
<tr><td>3.</td><td>Information on being registered with a state medical institution</td></tr>
<tr><td>4.</td><td>Information on the absence of a criminal record (or the presence of a criminal record)</td><td rowspan="4">Ministry of Preschool and School Education
Ministry of Justice
Ministry of Poverty Reduction and Employment
Cadastre Agency
National Agency for Social Protection
Youth Affairs Agency
Tax Committee
Committee on Family and Women</td></tr>
<tr><td>5.</td><td>Biometric passport (ID card) information</td></tr>
<tr><td>6.</td><td>Driver’s license information</td></tr>
<tr><td>7.</td><td>Information on the place of</td></tr>
</table>
</td></tr>
</table>

				residence and place of stay	
			8.	Information on citizenship of the Republic of Uzbekistan	
			9.	Information on motor vehicles registered in the person’s name	
			10.	Information on the personal identification number of an individual	
			11.	Information on the biometric passport for travel abroad	
			12.	Information about the student’s place of study (from a higher education institution)	Extra-budgetary Pension Fund under the Ministry of Economy and Finance, National Agency for Social Protection Bureau of Compulsory Enforcement
			13.	Information on the person’s education (secondary specialized, vocational, professional and higher education)	
			14.	Information on the person’s general secondary education (certificate information)	
			15.	Information on licenses, permits and notifications issued in the person’s name	Ministry of Health Ministry of Internal Affairs

		16.	Information on individual entrepreneurship		
		17.	Information on work experience and place of employment	Ministry of Higher Education, Science and Innovation	
		18.	Information on the area of the residential premises	Ministry of Preschool and School Education Ministry of Justice	
		19.	Information on immovable property registered in the person's name		
		20.	Information on inclusion in the Social Register	Ministry of Poverty Reduction and Employment Cadastre Agency	
		21.	Information on the citizen's inclusion in the "Iron Notebook"		
		22.	Information on the citizen's inclusion in the "Youth Notebook"	National Agency for Social Protection	
		23.	Information on whether or not there is tax debt for taxes and fees	Youth Affairs Agency Tax Committee Committee on Family and Women	
		24.	Information on salary		
		25.	Information on self-employment		
		26.	Information on the citizen's inclusion in the "Women's Notebook"	Extra-budgetary Pension Fund under the Ministry of Economy and Finance, National Agency for Social Protection	
		27.	Information on the amount of	Bureau of Compulsory Enforcement	

<table>
<tr><td></td><td></td><td>
<table>
<tr><td></td><td>pensions (allowances) paid</td><td></td></tr>
<tr><td>28.</td><td>Information on inclusion in the list of pension and allowance recipients</td><td></td></tr>
<tr><td>29.</td><td>Information on whether or not there is outstanding debt under an enforcement document</td><td rowspan="2">Ministry of Health</td></tr>
<tr><td>30.</td><td>Information on the imposition of a temporary restriction on departure from the Republic of Uzbekistan</td></tr>
</table>
Note: The relevant authorized bodies listed in this list and the Ministry of Digital Technologies shall be responsible for the accuracy of the information included in this list and its continuous updating in real-time mode.
</td></tr>
<tr><td colspan="3">Resolutions of the President of the Republic of Uzbekistan</td></tr>
<tr><td>1.</td><td>“Regulation on the Special Regulatory Regime in the Sphere of Crypto-Asset Circulation (the “Regulatory Sandbox” Special Regime)”, annexed to the Regulation “On the National Agency of Prospective Projects of the Republic of Uzbekistan”, approved by Resolution № RP–3150 of the President of the Republic of</td><td>Paragraph 6:
It is provided that the National Agency of Prospective Projects of the Republic of Uzbekistan shall, on the basis of agreements concluded with the relevant authorized state body, determine the procedure and conditions for the processing by participants of the special regime of depersonalized personal data, as well as the requirements imposed on them.</td></tr>
</table>

	Uzbekistan dated 27 July 2017.	
2.	Resolution № RP–14 of the President of the Republic of Uzbekistan dated 19 January 2026 "On Measures to Raise the Activities of the Internal Affairs Bodies in the Field of Migration and Personalization to a Qualitatively New Level through Digitalization".	**1.** The following shall be identified as priority areas of the State policy in the field of migration and personalization: **(a)** the gradual transformation of the migration and personalization divisions of the internal affairs bodies into "service divisions" that provide the population with more convenient and high-quality services based on the principles of efficiency and transparency; **(b)** raising the organization of the activities of the republican, regional, district (city) divisions in the field of migration and personalization to a qualitatively new level and increasing their efficiency; **(c)** digitalization of public services provided in the field of migration and personalization; **(d)** ensuring the accuracy and reliability of personal data; **(e)** ensuring information security and cybersecurity in existing information systems through the widespread introduction of modern information and communication technologies into the sector.
Resolutions of the Cabinet of Ministers		
1.	**Rules for Retail Trade in the Republic of Uzbekistan**, approved by Resolution № 75 of the Cabinet of Ministers dated 13 February 2003.	**Paragraph 187[25].** When applying a discount to the price of goods, if the provision of such discount requires the consumer to provide or register personal data, the seller shall comply with the legislation on personal data and shall inform consumers of the purposes and conditions of processing their data.
2.	**Rules for Conducting Electronic Commerce**, approved by Resolution № 185 of the Cabinet of Ministers dated 2 June 2016.	**Paragraph 17:** It is stipulated that an information intermediary, i.e. a legal entity providing services related to the circulation of electronic documents and electronic messages in electronic commerce, shall ensure measures to protect electronic documents, electronic messages, and personal data against unauthorized access.
3.	Regulation "On the Procedure for Exercising State	establishes the procedure for exercising state control over compliance by owners and/or operators with the requirements of legislative acts

	Control over Compliance with the Special Conditions for the Processing of Personal Data of Citizens of the Republic of Uzbekistan", approved by Resolution № 707 of the Cabinet of Ministers dated 5 September 2018	concerning the collection, systematization, and storage of personal data of citizens of the Republic of Uzbekistan on technical means physically located within the territory of the Republic of Uzbekistan and in personal data databases registered in the State Register of Personal Data Databases in the prescribed manner, when processing personal data of citizens of the Republic of Uzbekistan using information technologies, including processing on the Internet.
4.	Regulation "On Authorized Representatives of Candidates", approved by Resolution № 936 of the Central Election Commission of the Republic of Uzbekistan dated 11 September 2019	**Paragraph 11.** During the period of pre-election campaigning, it is prohibited to disseminate false information to a proxy, to violate the confidentiality of personal data, as well as to disseminate information that discredits the honor and dignity of candidates.
5.	The Regulation "On the Procedure for Providing an Electronic Fiscal Receipt through an Electronic Payment Organization and/or Electronic Commerce Platforms (Marketplace) When Making Paid Transactions with the Population," approved by Resolution № 943 of the Cabinet of Ministers of the Republic of Uzbekistan dated November 23, 2019.	**12^{6}.** E-commerce platforms shall ensure the confidentiality of personal data and information constituting a tax secret in their databases. **12^{7}.** E-commerce platforms shall not disclose or disseminate personal data and information constituting a tax secret obtained from the information systems of the tax authorities to third parties.
6.	Resolution № 71 of the Cabinet of Ministers of the Republic of Uzbekistan dated	It establishes the procedure for providing the public service (hereinafter referred to as the "public service") for registering personal data databases in the State Register of Personal Data Databases,

	February 8, 2020, "On Approval of the Administrative Regulations for the Provision of Public Services for Maintaining the State Register of Personal Data Databases."	removing them from the Register, and making amendments and additions to the Register.
7.	The Regulation "On the Unified National System for the Delivery of Correspondence Sent by State Bodies and Organizations, Confirmation of Its Delivery, Storage and Recording of Information," approved by Resolution No. 637 of the Cabinet of Ministers of the Republic of Uzbekistan dated October 9, 2020.	**17.** The operator of the Unified National System shall ensure the information security of information systems and information resources used for the provision of postal communication services through the system, as well as the protection of personal data in the system and information contained in postal items.
8.	The Regulation "On the Procedure for Conducting Proceedings in Cases Related to Administrative Offenses through the Unified Electronic Case Management System for Administrative Offenses," approved by Resolution № 431 of the Cabinet of Ministers of the Republic of Uzbekistan dated July 8, 2021.	**57.** The authorized body's employee (official) shall be responsible for the accurate entry, via a tablet or computer, of the personal data of the offender, victim, witness, and attesting witness (surname, first name, patronymic, and date of birth) into the administrative protocol or the decision on the imposition of an administrative penalty. If the offender, victim, witness, or attesting witness is not a citizen of the Republic of Uzbekistan, or if it is not possible to establish their identity using identification systems, and they have a foreign passport or other identity document that has not been entered into the database, the responsible employee of the authorized body shall manually enter the personal data into the electronic system on the basis of these documents and shall be personally responsible for the accuracy of such entry.

		If it is established that the personal data or other information of the offender, victim, witness, or attesting witness has been entered incorrectly into the system, the authorized body where the responsible employee who entered such information serves (works) shall, within three days, appoint an internal investigation against that responsible employee. **66.** If information relating to the person being checked is found in the record-keeping document, the date of the check and the text "The information is checked using the electronic key of an employee of the Ministry of Internal Affairs" shall be written on the reverse side of the request, and an electronic stamp and electronic digital signature shall be affixed. **75.** The responsible employee of the authorized bodies shall be responsible for ensuring that personal data in the "E-ma'muriy ish" system is not disclosed to third parties and that such data is not used for malicious purposes.
9.	Resolution № 479 of the Cabinet of Ministers of the Republic of Uzbekistan dated August 30, 2022, "On Measures to Introduce the Mobile-ID System for the Identification of Individuals in the Republic of Uzbekistan."	**29.** The Mobile-ID system shall be used for the following purposes: confirming the identity (authenticating) of users when accessing the portals and information systems of state bodies and organizations through the OneID system; confirming the authenticity (verifying) of a user using the Mobile-ID system; confirming applications submitted by users for the use of electronic public services; receiving notifications when state bodies and organizations obtain the user's personal data through the "Electronic Government" system; granting permission for state bodies and organizations, economic associations, and non-governmental organizations to obtain the user's personal data through the "Electronic Government" system; in other cases provided for by legislation. **30.** In the cases specified in paragraph 29 of this Regulation, authentication of users using the Mobile-ID system, confirmation of applications, and granting permission to obtain personal data

		through the “Electronic Government” system shall be carried out by entering a one-time unique code from an SMS message sent to the mobile telephone number with which the user has undergone identification in the Mobile-ID system.
10.	Resolution № 516 of the Cabinet of Ministers of the Republic of Uzbekistan dated September 20, 2022, “On Measures to Further Improve the Interagency Electronic Cooperation System and Information Data Exchange.”	It establishes the procedure for electronic cooperation and information exchange among state bodies and organizations through the Interagency Integration Platform of the “Electronic Government” system, as well as the procedure for connecting them to this platform.
11.	Resolution № 570 of the Cabinet of Ministers of the Republic of Uzbekistan dated October 5, 2022, “On Approval of Certain Regulatory Legal Documents in the Field of Personal Data Processing.”	Determining the level of protection of personal data when processing personal data, and ensuring the security of such data during processing; Determining the levels of protection of personal data based on threats to the security of such data during processing; Requirements for ensuring the level of protection of personal data, the procedure for storing, using, and accounting for biometric and genetic data on material media, as well as requirements for technologies for storing biometric and genetic data outside personal data databases are provided for.
12.	The Regulation “On the Procedure for Providing Publicly Available Information from the State Register of Rights to Immovable Property through the National Geographic Information System,” approved by Resolution No. 610 of the Cabinet of Ministers of the Republic of Uzbekistan	The procedure for providing publicly available information from the State Register of Rights to Immovable Property through the National Geographic Information System of the Cadastre Agency under the Ministry of Economy and Finance of the Republic of Uzbekistan to state administration bodies and economic associations, individuals, and other legal entities has been established.

	dated October 18, 2022.	
13.	The Regulation "On the Procedure for Installing and Operating Special Automated Software and Technical Means for Photo and Video Recording in Front of Schools Located Along Roads, at Pedestrian Crossings on Roads with at Least Four Lanes, at Road Traffic Accident Hotspots, and at Railway Crossings," approved by Resolution № 148 of the Cabinet of Ministers of the Republic of Uzbekistan dated March 25, 2024.	**28.** During the operation of the special automated photo and video recording system, the legislation on personal data must be strictly complied with.
14.	The Regulation "On the Procedure for Remote Digital Identification of Clients in the Securities Market," approved by Resolution № 238 of the Cabinet of Ministers of the Republic of Uzbekistan dated April 26, 2024.	**5.** The investment intermediary shall process the client's personal data only for the purposes provided for in this Regulation.
15.	The Licensing Requirements and Conditions for Carrying Out Activities Involving the Organization of Games and Lotteries Based on Risk and Bookmaker Activities on the Worldwide Information Network Known as the Internet, approved by Resolution № 814 of	Compliance with the requirements of the legislation of the Republic of Uzbekistan in the areas of organizing games and lotteries on the Internet and carrying out bookmaker activities, combating the legalization of proceeds derived from criminal activities, combating the financing of terrorism and the financing of the proliferation of weapons of mass destruction, storing and using personal data, and advertising shall constitute the licensing requirements and conditions for carrying out activities involving the organization of games and lotteries based on risk, as well as bookmaker

	the Cabinet of Ministers of the Republic of Uzbekistan dated December 6, 2024.	activities, on the worldwide information network known as the Internet:
16.	Resolution №318 of the Cabinet of Ministers of the Republic of Uzbekistan dated May 15, 2025, "On Measures to Create Additional Convenience for the Population in the Use of Vehicles."	**6.** In order to ensure the security of personal data when recording cases involving violations of traffic rules through special technical means, as well as to prevent abuses in this area, it shall be established that: the data storage and processing devices and software of the special automated photo and video recording system for violations of traffic rules installed by business entities shall be gradually transferred, by the end of 2025, to the management of the state institution "Center for the Development of Safe City Systems" of the Ministry of Internal Affairs; the state institution "Center for the Development of Safe City Systems" shall be responsible for ensuring that the special automated photo and video recording system for violations of traffic rules installed by business entities is operated in accordance with the established procedure and in compliance with the technical requirements.
17.	The Regulation "On the Procedure for Organizing the Activities of the Trusted Third Party Service," approved by Resolution № 551 of the Cabinet of Ministers of the Republic of Uzbekistan dated September 2, 2025.	**7.** The main tasks of the Trusted Third Party Service shall be as follows: verifying the authenticity of the electronic digital signature in an electronic document, verifying that it belongs to the person who signed it, and confirming the legal validity of electronic documents by issuing an electronic receipt; acting as an information intermediary in the process of interagency electronic cooperation to ensure, at a specific point in time, guarantees for maintaining the integrity and reliability of electronic documents; confirming that electronic documents whose authenticity has been verified by the Trusted Third Party Services of foreign states or legal entities performing the functions of such services, pursuant to a mutual agreement, have legal force in the Republic of Uzbekistan.

		9. In the process of processing personal data, the Trusted Third Party Service shall be obliged to take measures to ensure the security established by the legislation of the Republic of Uzbekistan on personal data. **12.** The Trusted Third Party Service shall carry out its activities in the following areas: **a) Bilateral Trusted Third Party Service.** In this case, the Trusted Third Party Service, in cooperation with the Trusted Third Party Services of foreign states or legal entities performing the functions of such services, shall verify and confirm the authenticity of electronic digital signatures and that they belong to the persons who signed them, generate an electronic receipt, and transmit information to the relevant systems during the exchange of documents between users in the Republic of Uzbekistan, as well as between users in the Republic of Uzbekistan and users in a foreign state; **b) Unilateral Trusted Third Party Service.** In this case, the Trusted Third Party Service shall, upon the request of a user in the territory of the Republic of Uzbekistan and/or in a foreign state, verify and confirm the authenticity of the electronic digital signature in the document provided and that it belongs to the person who signed it, generate an electronic receipt, and transmit information to the relevant systems; **c) Mutual verification of electronic digital signatures of registration centers.** In this case, the Trusted Third Party Service shall verify and confirm the authenticity of users' electronic digital signatures and that they belong to the persons who signed them, in order for users to access, through electronic information exchange, systems where it is necessary to use the electronic digital signature keys of another registration center by means of an electronic digital signature key obtained from a particular registration center. The Trusted Third Party Service may carry out its activities in areas of the use of electronic

		digital signatures that are not prohibited by legislation.
18.	Resolution № 700 of the Cabinet of Ministers of the Republic of Uzbekistan dated November 6, 2025, “On Further Improvement of Certain Procedures in the Customs Sphere.”	**The Regulation “On the Procedure for Applying Forms of Customs Control,” approved by Resolution № 700 of the Cabinet of Ministers of the Republic of Uzbekistan dated November 6, 2025** **154.** During the implementation of forms of customs control, an official of the customs authority shall, when using technical means, take measures to ensure personal safety, prevent harm to human life and health, the environment, goods and means of transport, and protect personal data. **The Regulation “On the Procedure for Customs Control and Clearance of International Postal and Courier Items,” approved by Resolution № 700 of the Cabinet of Ministers of the Republic of Uzbekistan dated November 6, 2025** **56.** When carrying out customs control and clearance, an employee of the customs authority shall be obliged not to disclose information constituting a commercial secret or confidential personal data that becomes known to them as a result of performing their official duties during declaration and clearance, except in cases established by legislation. **60.** Ensuring full compliance with the requirements of the legislation on personal data and ensuring data security during customs control and clearance shall be the obligation of postal communication operators and express carriers.
19.	The Regulation “On the Procedure for Electronic Identification of Citizens in Public Places by Officers of Patrol and Post Service Units of Internal Affairs Bodies,” approved by Resolution № 754 of the Cabinet of Ministers of the	**5.** Through the “E-Patrol” system, a citizen’s personal data (surname, first name, patronymic, residential address, date of birth), as well as information concerning offenses or other information (criminal record, being wanted, or being registered for preventive, probation, or administrative supervision purposes, and others) shall be checked on the spot, thereby ensuring promptness and preventing unnecessary inconvenience. In this regard, the server equipment of the Ministry of Internal Affairs of the Republic of

	Republic of Uzbekistan dated December 1, 2025.	Uzbekistan shall be used to identify citizens by their fingerprints or facial features. **7.** In accordance with the Law of the Republic of Uzbekistan "On Personal Data," disclosure of personal data that becomes known to an employee through the tablet assigned to them shall not be permitted. **29.** The employee shall be responsible for ensuring that personal data in the "E-Patrol" system is not disclosed to third parties and is not used for malicious purposes.
20.	Resolution № 766 of the Cabinet of Ministers of the Republic of Uzbekistan dated December 4, 2025, "On Improving the Procedure for Handling Documents Classified as 'For Official Use.'"	**ANNEX** to the Rules for Handling Documents Classified as "For Official Use" **MODEL LIST** of Information with Restricted Access for Official Use 1. Personal data of an individual.
21.	Resolution № 415 of the Cabinet of Ministers of the Republic of Uzbekistan dated July 29, 2026, "On Approval of the List of Foreign States Ensuring an Equivalent Level of Protection of Personal Data."	A list of foreign states ensuring an equivalent level of protection of personal data has been approved, and the following has been established: personal data and depersonalized data shall be automatically transferred cross-border to the states included in the list through information systems established on the basis of international agreements, without additional permits and without notifying the authorized state body, provided that measures are taken to prevent data leakage; the transfer of personal data in any form to foreign states not included in the list shall be permitted if the operator and the owner of the personal data database comply with the legal, organizational, and technical conditions established by the authorized state body; if a data leakage is detected during the cross-border transfer of personal data, the operator of the personal data database shall notify the authorized state body thereof within 24 hours from the time the incident is detected and shall provide detailed

		information within 72 hours on the causes of the data leakage and the measures taken to eliminate them.
Departmental Regulatory Legal Documents		
1.	The Instruction on the Procedure for Considering Administrative Cases Concerning Violations of Traffic Rules, approved by Order No. 68 of the Minister of Internal Affairs of the Republic of Uzbekistan dated May 31, 2011 (registration № 2240, dated July 5, 2011).	**Paragraph 10.** The employee of the Road Traffic Safety Service shall be responsible for the accurate entry, in electronic form via a tablet or computer, of the personal data of the offender, victim, witness, and attesting witness (surname, first name, patronymic, and date of birth) into the electronic administrative protocol. If the offender, victim, witness, or attesting witness is not a citizen of the Republic of Uzbekistan, or if it is not possible to establish their identity using identification systems, and they have a foreign passport or other identity document that has not been entered into the database, the employee of the Road Traffic Safety Service shall manually enter the personal data into the electronic system on the basis of these documents and shall be personally responsible for the accuracy of such entry.
2.	Order № 53-mh of the Minister of Justice of the Republic of Uzbekistan dated March 2, 2012, "On Approval of the General Legal Classifier of Branches of Legislation of the Republic of Uzbekistan" (registration № 2333, dated March 2, 2012).	**12.00.00.00** **INFORMATION AND INFORMATIZATION** **12.03.00.00** **Information Resources. Use of Information Resources** **12.03.06.00** **Personal Data and Their Protection**
3.	The Regulation on Minimum Requirements for Information Security in the Information Systems of Microfinance Organizations,	**4.** Non-bank credit organizations shall comply with the following minimum requirements to prevent the unlawful use of confidential and personal data and the illegal disclosure of information. **6.** The duties of the employee responsible for information security shall include conducting awareness-raising activities regarding the

	Pawnshops, and Mortgage Refinancing Organizations, approved by Resolution № 15/6 of the Board of the Central Bank of the Republic of Uzbekistan dated June 27, 2020 (registration № 3260, dated June 30, 2020).	obligation and responsibility of employees to keep confidential the confidential and personal data that become known to them in the course of their work, as well as eliminating the risks of unlawful use of confidential and personal data.
4.	The Regulation on the Procedure for Licensing the Activities of Service Providers in the Field of Crypto-Asset Turnover, approved by Order № 32 of the Director of the National Agency of Prospective Projects of the Republic of Uzbekistan dated July 14, 2022 (registration № 3380, dated August 15, 2022).	**9.** The following shall constitute the licensing requirements and conditions for carrying out the activities of service providers: **a)** availability of an electronic platform and/or a set of technical and software tools located on servers within the territory of the Republic of Uzbekistan; **b)** storage for five years of information on all transactions related to crypto-assets, identification information of platform participants, materials relating to the relationships between service providers and platform participants (including between platform participants), as well as business correspondence; **c)** compliance with the requirements of the legislation of the Republic of Uzbekistan in the areas of crypto-asset turnover, combating the legalization of proceeds derived from criminal activities, combating the financing of terrorism and the financing of the proliferation of weapons of mass destruction, as well as the storage and use of personal data;
5.	The Regulation on the Procedure for Licensing the Activities of Payment System Operators and Payment Organizations, approved by Resolution № 8/3 of the Board of the Central Bank of the Republic of Uzbekistan dated April 18, 2023	**23.** A license applicant that is not a bank shall submit to the Central Bank an application for obtaining a license to carry out the activities of a payment system operator and a payment organization in electronic or written form in accordance with Annex 1 to this Regulation, and shall attach to the application a document on the security policy, including a detailed risk assessment, as well as a description of the measures to be taken to ensure information security and cybersecurity and to reduce risks related to the protection of users of payment services, including

	(registration No. 3431, dated May 5, 2023).	the risks of fraud and unlawful use of confidential and personal data.
6.	The Regulation "On the Procedure for Supervising and Conducting Oversight of the Activities of Payment System Operators and Payment Organizations," approved by Resolution № 8/4 of the Board of the Central Bank of the Republic of Uzbekistan dated April 18, 2023 (May 15, 2023, registration № 3434).	**3.** In supervising the activities of payment system operators and payment organizations, the Central Bank shall request information related to the operation of payment systems from payment system operators and payment organizations, including information containing personal data. **36.** If a payment system operator and/or payment organization fails to comply with an instruction to remedy a violation and violates the requirements for maintaining the confidentiality of personal data, the Central Bank shall apply one of the sanctions specified in paragraph 35 of this Regulation to the payment system operator and/or payment organization.
7.	Order № 19-mh of the Minister of Justice of the Republic of Uzbekistan dated November 15, 2023 (dated November 15, 2023, registration № 3477), "On Approval of the Model Procedure for Organizing the Activities of the Structural Unit or Authorized Person of the Owner and/or Operator of a Personal Data Database Responsible for Ensuring the Processing and Protection of Personal Data."	The procedure for organizing the activities of the structural unit of the owner and/or operator of a personal data database that ensures the processing and protection of personal data (hereinafter referred to as the unit), or of an authorized person, has been established.
8.	Order № 20-mh of the Minister of Justice of the Republic of Uzbekistan dated November 15, 2023 (dated November 15,	The procedure for processing and protecting personal data, the principles, purposes, and conditions of processing personal data, as well as the rights and obligations of the owner and/or operator of a personal data database have been established.

	2023, registration № 3478), “On Approval of the Model Procedure for Processing Personal Data.”	
9.	The Regulation “On Ensuring Information Security and Cybersecurity in the Payment Systems of Payment System Operators and Payment Service Providers and Taking Measures to Prevent Offenses Committed Through Digital Technologies,” approved by Resolution № 13/1 of the Board of the Central Bank of the Republic of Uzbekistan dated April 24, 2024 (dated May 21, 2024, registration № 3513).	**Chapter 3. Confidentiality of Payment Information and Protection of Personal Data Contained Therein** **12.** Payment system operators and payment service providers shall take the following measures to protect the confidentiality and integrity of information, including personal data of payment service users, and to ensure an adequate level of security: develop a procedure for protecting the integrity and inviolability of confidential and personal data processed within the payment system, as well as a procedure for accessing such data; develop rules and requirements for ensuring security and confidentiality when handling protected information regulated by internal documents; minimize, to the extent possible, the number of employees handling confidential and personal data, conclude undertakings (agreements) with employees to prevent the disclosure of confidential and personal data, and determine employees’ rights of access to such data based on their job responsibilities; form and approve the composition of a commission for maintaining a list of confidential information; determine and approve the list and scope of confidential information; form and approve a list of employees authorized to work with confidential information; develop and approve the technical passport of the informatization facility; develop and approve the procedure for handling confidential information; register data carriers containing confidential information, destroy them, and maintain logs for

<table>
<tr><td></td><td></td><td>the removal from and return to the premises of confidential information carriers;
establish the procedure for using electronic digital signature keys and storing encrypted data in order to ensure the integrity and security of data;
ensure identification, authentication, and authorization when accessing resources containing confidential and personal data;
prevent the unauthorized granting of rights to access and work with confidential and personal data;
record in electronic logs the actions performed during the processes of accessing, processing, storing, and providing users of information systems with access to protected data;
prevent the removal of external storage devices and technical means from the premises, as well as their theft;
monitor the implementation of measures to ensure the secure transfer, storage, deletion, and processing of data, as well as to prevent their unauthorized leakage.</td></tr>
<tr><td>10.</td><td>Order № 14 of the Director of the National Agency of Prospective Projects of the Republic of Uzbekistan dated June 25, 2025 (dated July 7, 2025, registration № 3643), “On Approval of the Regulation on the Procedure for Imposing Fines on Organizers of Risk-Based Games, Lotteries, and Bookmaker Activities on the Worldwide Information Network Known as the Internet, as well as on Foreign Legal Entities Illegally Providing Services to Residents of the</td><td>FINES
imposed for violations by an organizer of games, lotteries, and bookmaker activities on the Internet of the legislation on lotteries and other risk-based games, including the legislation on combating the legalization of proceeds derived from criminal activities, the financing of terrorism, and the financing of the proliferation of weapons of mass destruction, in an amount not exceeding 1 percent of the minimum amount of the charter fund (charter capital) of the organizer of games, lotteries, and bookmaker activities on the Internet
<table>
<tr><th>№</th><th>Type of Violation</th><th>Applicable Fine Amount (as a percentage of the minimum amount of the charter fund (charter capital)</th></tr>
</table>
</td></tr>
</table>

	Republic of Uzbekistan in the Field of Organizing and Conducting Lotteries and Risk-Based Games.”			
				established for organizers organizing games in accordance with the type of activity)
		Section 1. Violation of Licensing Requirements		
		2.	Transfer of a license to another legal entity, including granting the right to carry out the activity, transferring the rights to a license under a contract, and/or waiving such rights in favor of another person.	0.8 percent
		Section 3. Violation of Technical Requirements		
		20.	Failure to comply with the requirements for the storage and use of personal data	0.8 percent, 1 percent if committed repeatedly within one year

ANNEX 2

to the Regulation on the Procedure for Imposing Fines on Organizers of Risk-Based Games, Lotteries, and Bookmaker Activities on the Worldwide Information Network Known as the Internet, as well as on Foreign Legal Entities Illegally Providing Services to Residents of the Republic of Uzbekistan in the Field of Organizing and Conducting Lotteries and Risk-Based Games

FINES
IMPOSED ON FOREIGN LEGAL ENTITIES ILLEGALLY PROVIDING SERVICES TO RESIDENTS OF THE REPUBLIC OF UZBEKISTAN IN THE FIELD OF ORGANIZING AND CONDUCTING LOTTERIES AND RISK-BASED GAMES

<table>
<tr><td></td><td></td><td>
<table>
<tr><th>№</th><th>Type of Violation</th><th>Applicable Fine Amount (fines applied in multiples of the basic calculated amount)</th></tr>
<tr><td>3.</td><td>Failure to comply with the requirements for the storage and use of personal data</td><td>15 000</td></tr>
</table>
</td></tr>
<tr><td>11.</td><td>The Regulation “On Minimum Requirements for Ensuring Information Security and Cybersecurity in the Information Systems of Electronic Factoring Platforms,” approved by Resolution № 16/2 of the Board of the Central Bank of the Republic of Uzbekistan dated July 16, 2025 (dated August 13, 2025, registration No. 3665).</td><td>2. Organizations shall, for the purpose of ensuring information security and cybersecurity in the information systems and resources supporting the platform (hereinafter referred to as information systems) provided by the organizations:
a) develop and approve an information security policy. In doing so:
requirements for ensuring information security and cybersecurity in information systems and resources shall be established;
employees of the organization shall be familiarized with the established requirements, and strict compliance by employees with these requirements shall be ensured;
b) appoint an employee responsible for ensuring information security and cybersecurity (hereinafter referred to as the responsible employee);
c) ensure the integrity of confidential information, including information constituting bank secrecy and personal data, and develop a procedure for accessing and using such information. In doing so, the procedure shall provide for:
development of requirements and rules for ensuring security, confidentiality, and integrity when handling confidential information, including information constituting bank secrecy and personal data;
conclusion of undertakings (agreements) with employees to prevent the disclosure of confidential information, including information constituting bank secrecy and personal data, and</td></tr>
</table>

		determination of employees' rights to access and use such information based on their job responsibilities; formation and approval of a list of confidential information; formation and approval of a list of employees authorized to work with confidential information; development and approval of the procedure for handling confidential information; provision of measures to prevent the unauthorized removal of external storage devices and technical means outside the controlled area; d) establish requirements for assessing and managing risks arising in information systems; e) develop a procedure for identifying, preventing, and eliminating malfunctions, disruptions, and information security and cybersecurity incidents that have occurred or may occur in information systems, as well as for storing information about such incidents and maintaining records thereof. **3.** The responsible employee shall, in the course of their activities: monitor compliance by the organization's divisions and employees with the established requirements for ensuring information security and cybersecurity in information systems and resources; organize the information security and cybersecurity assurance system; conduct explanatory work with employees regarding their obligation to keep confidential information, including information constituting bank secrecy and personal data, secret and their liability for violating their obligations, and monitor the preservation of such information; monitor the introduction of changes to information systems; organize the determination of users' rights and access limits when working with information resources; control access to information systems;

		restrict unauthorized access to information systems and information resources; develop internal regulatory documents on ensuring information security and cybersecurity; submit proposals to management on matters of ensuring information security and cybersecurity; ensure the organization of overall control over the storage of information. **9.** The personal data database of organizations shall be registered in the State Register of Personal Data Databases. **10.** Organizations shall take the following measures to ensure continuous protection of confidential information, including information constituting bank secrecy and personal data, at all stages of the formation, transmission, storage, and processing of information: implement an identification, authentication, and authorization system; apply methods for preventing unauthorized access to the system (login, password, multi-factor authentication (MFA), and others); ensure that the database administrator's password is at least 12 characters long, using uppercase and lowercase letters, numbers, and special characters (@, #, $, &, %, and others) as password characters; protect documents and identification data against forgery, unauthorized copying, alteration, deletion, and provision to third parties; ensure the control and accounting of software in information systems, as well as the continuous operation of software versions, hardware-software devices, and software tools; ensure that information systems are kept up to date (on the latest version), with new versions of software being introduced into the information system after testing; carry out all information exchange between application servers and users in the corporate network through the Transport Layer Security (TLS) protocol (version 1.3 or higher); provide information systems with primary and backup communication channels;

		close ports and stop services on servers that are not necessary for operational activities; in the event of unauthorized access to an information system or information security and cybersecurity incidents, take measures to continuously strengthen protection systems based on their analysis; when integrating external information systems with the information system, establish the use of a token provided for authorization when using Web service (WebAPI) methods created for this purpose.
12.	The Regulation "On Minimum Requirements for Information Security and Cybersecurity of Commercial Banks of the Republic of Uzbekistan," approved by Resolution № 19/1 of the Board of the Central Bank of the Republic of Uzbekistan dated August 1, 2025 (dated August 18, 2025, registration № 3669).	**17.** The bank shall ensure the non-disclosure of confidential information established by legislative documents and its internal documents. In doing so, the bank shall: establish and maintain the up-to-date status of the list of confidential information pertaining to the bank or its division, including information constituting bank secrecy and personal data; have each employee sign an undertaking to keep confidential information secret for the purpose of compensating for any damage caused; ensure that employees who are not authorized to access confidential information do not use such information; ensure the secure storage of computers containing confidential information and the documents stored on them; ensure compliance with the requirements specified in the Laws of the Republic of Uzbekistan "On Bank Secrecy" and "On Personal Data"; take measures to prevent unauthorized access to confidential information. **78.** Measures shall be taken at the bank to ensure information security and cybersecurity when using the Internet. Computers of users working with confidential information, including information constituting bank secrecy and personal data, may be connected to the Internet through a proxy server. In doing so, connection to the Internet shall be

		organized only on the basis of a list of information resources related to official work activities.
13.	The Regulation “On Minimum Requirements for Information Security and Cybersecurity of Credit Bureaus,” approved by Resolution № 20/2 of the Board of the Central Bank of the Republic of Uzbekistan dated August 19, 2025 (dated September 23, 2025, registration № 3679).	**27.** Credit bureaus shall establish requirements in contracts concluded with system participants for ensuring information security and cybersecurity, as well as the security of confidential information, including information constituting bank secrecy and personal data. **28.** Credit bureaus shall take the following measures to restrict unauthorized access to and use of informatization facilities: control physical access to informatization facilities and access to buildings and premises where technical equipment is located; control employees’ access to informatization facilities and implement systems to protect against unauthorized dissemination of data; monitor activities in premises where servers and telecommunications equipment are located using video surveillance systems. **29.** Credit bureaus shall ensure information security and cybersecurity of information systems storing all types of data, including information constituting bank secrecy, personal data, and other information protected by law. **30.** Before implementing remote service information systems and making changes to them, credit bureaus shall ensure the following: complete testing of all functions of remote information systems; conduct an examination of remote information systems against technical specifications and for their compliance with the technical specifications and cybersecurity requirements, and submit the expert opinions obtained based on the results thereof to the Central Bank; develop instructions for the use of software and provide them to clients while ensuring that such instructions remain up to date; ensure that changes are made to eliminate identified vulnerabilities; monitor the up-to-date status of software used by clients.

		After introducing a new edition (version) of remote information systems, credit bureaus shall restrict the use of the old edition (version) and transition (update) to the new edition (version). **31.** Credit bureaus shall specify the obligations of the parties concerning information security and cybersecurity in contracts concluded with users of credit information. **32.** Credit bureaus shall take the following measures to ensure the confidentiality and integrity of information, including the protection of personal data, and to ensure security: develop and approve a procedure for ensuring the integrity and inviolability of confidential and personal data processed through information systems and for accessing such data; develop rules and requirements for ensuring security and confidentiality when handling protected information regulated by internal documents; minimize, to the extent possible, the number of employees handling confidential and personal data, conclude undertakings (agreements) with employees to prevent the disclosure of confidential and personal data, and determine employees' rights to access and use such data based on their job responsibilities; form and approve the composition of a commission for maintaining a list of confidential information; determine and approve the list and scope of confidential information; form and approve a list of employees authorized to work with confidential information; develop and approve the technical passport of the informatization facility; register and destroy confidential information carriers, and maintain logs of their removal from and return to the premises; establish the procedure for using electronic digital signature keys and storing encrypted data in order to ensure data integrity and security; ensure identification, authentication, and authorization when accessing information

		resources containing confidential and personal data; prevent the unauthorized granting of rights to work with confidential and personal data; record in electronic logs the actions performed by information system users when accessing, processing, storing, and providing protected data; control the removal of external storage devices and technical means from the premises; ensure measures to prevent the unauthorized leakage of data during their transmission, storage, processing, and deletion. **32.** Credit bureaus shall take the following measures to ensure the confidentiality and integrity of information, including the protection of personal data, and to ensure security: develop and approve a procedure for ensuring the integrity and inviolability of confidential and personal data processed through information systems and for accessing such data; develop rules and requirements for ensuring security and confidentiality when handling protected information regulated by internal documents; minimize, to the extent possible, the number of employees handling confidential and personal data, conclude undertakings (agreements) with employees to prevent the disclosure of confidential and personal data, and determine employees' rights to access and use such data based on their job responsibilities; form and approve the composition of a commission for maintaining a list of confidential information; determine and approve the list and scope of confidential information; form and approve a list of employees authorized to work with confidential information; develop and approve the technical passport of the informatization facility; register and destroy confidential information carriers, and maintain logs of their removal from and return to the premises;

		establish the procedure for using electronic digital signature keys and storing encrypted data in order to ensure data integrity and security; ensure identification, authentication, and authorization when accessing information resources containing confidential and personal data; prevent the unauthorized granting of rights to work with confidential and personal data; record in electronic logs the actions performed by information system users when accessing, processing, storing, and providing protected data; control the removal of external storage devices and technical means from the premises; ensure measures to prevent the unauthorized leakage of data during their transmission, storage, processing, and deletion. **40.** When engaging other organizations to make changes to their information systems, credit bureaus shall conclude an agreement on non-disclosure of confidential and personal data. **43.** A mechanism for detecting anomalous (fraud) situations shall be implemented in the process of obtaining information constituting bank secrecy and personal data from the information system. **45.** Confidential and personal data shall be transmitted by credit bureaus only through authorized information systems.
14.	The Rules for the Provision of Telecommunication Services, approved by Order No. 287-mh of the Minister of Digital Technologies of the Republic of Uzbekistan dated January 6, 2026 (dated January 26, 2026, registration № 3762).	**170.** The formation, maintenance, operation and technical monitoring of the NPMR, including the collection, storage, processing and transfer of information and data contained therein, as well as the provision of access to the NPMR, shall be ensured by the NPMR operator in compliance with the requirements of the Law of the Republic of Uzbekistan “On Personal Data”. **171.** The information necessary for carrying out the process of porting a subscriber number shall be provided by mobile communication operators (providers) to the NPMR operator and vice versa, in compliance with the requirements of the Law of the Republic of Uzbekistan “On Personal Data”.

		286. After termination of the contract concluded with the subscriber, the operator (provider, broadcaster) shall delete the subscriber's personal data from its database in accordance with legislative documents. After providing information about the subscriber to the operator (provider), the dealer shall delete the personal data that became known to it in accordance with legislative documents.
15.	**Ethical Rules for the Development, Implementation, and Use of Artificial Intelligence-Based Solutions**, approved by Order No. 284-mh of the Minister of Digital Technologies of the Republic of Uzbekistan dated February 24, 2026 (registered on March 14, 2026, №3787)	**5.** The use of artificial intelligence technologies and systems shall be carried out in accordance with the Laws of the Republic of Uzbekistan "On Personal Data", "On Informatization", and "On Cybersecurity", as well as other legislative acts. **14.** According to the principle of data protection: when using artificial intelligence technologies and systems, participants in artificial intelligence shall ensure the protection of state secrets and other secrets protected by legislation, personal data, and other data with restricted access; the unlawful processing of personal data by participants in artificial intelligence shall be prohibited. **17.** Developers and implementers of artificial intelligence technologies and systems shall have the following obligations: they shall be obliged to ensure the protection of personal data and data with restricted access. **19.** Users of artificial intelligence systems shall be obliged to ensure the protection of personal data and data with restricted access.

These legislative acts may be further continued; at the same time, national and international documents of a normative or recommendatory nature that do not have the character of normative legal acts as a source of law may also form part of the system of legislation relating to personal data. Accordingly, legislation on personal data consists of the Law of the Republic of Uzbekistan "On Personal Data" № LRU–547 dated July 2, 2019, and other legislative acts. If an international treaty of the Republic of Uzbekistan establishes rules other than those provided for by the legislation of the Republic of Uzbekistan on personal data, the provisions of the international treaty shall apply.

Although Article 1 of this Law stipulates that the purpose of this Law is to regulate relations in the field of personal data, in practice, pursuant to Article 3 of

this Law, the Law applies to relations arising in the course of processing and protecting personal data, regardless of the means of processing used, including information technologies.

This Law does not apply to:

the processing of personal data by an individual for personal and household purposes;

the formation, storage, and use of documents of the National Archival Fund and other archival documents containing personal data;

the processing of personal data included in information constituting state secrets, as well as information relating to matters of defense and national security;

relations arising in the course of processing personal data obtained during operational-search, intelligence and counterintelligence activities, combating crime, maintaining law and order, as well as within the framework of combating the legalization of proceeds derived from criminal activity.

Relations related to the processing and protection of personal data in a territory where a special legal regime has been established by a constitutional law of the Republic of Uzbekistan shall be regulated by rules different from those established by this Law.

Therefore, based on the scope of application, legislation on personal data is divided into the following types:

the Law of the Republic of Uzbekistan “On Personal Data” № LRU–547 dated July 2, 2019, and legislative acts and other documents adopted on the basis thereof;

legislation and other documents relating to the processing of personal data by an individual for personal and household purposes;

legislation and other documents relating to the formation, storage, and use of documents of the National Archival Fund and other archival documents containing personal data;

legislation and other documents relating to the processing of personal data included in information constituting state secrets, as well as information relating to matters of defense and national security;

legislation and other documents relating to relations arising in the course of processing personal data obtained during operational-search, intelligence and counterintelligence activities, combating crime, maintaining law and order, as well as within the framework of combating the legalization of proceeds derived from criminal activity;

documents established by separate legislation;

international documents.

All of these documents together constitute the body of legislation on personal data.

1.3-§. State regulation of the sphere of personal data

State regulation of the personal data sphere means that the state, through its regulatory function, ensures that the sphere of personal data is regulated by the relevant legislation, and that the legal status and powers of the competent authorities in this area are understood.

The Law of the Republic of Uzbekistan "On Personal Data" № LRU–547 dated July 2, 2019, stipulates that state regulation of the personal data sphere is carried out by the Cabinet of Ministers of the Republic of Uzbekistan and the authorized state body in the field of personal data.

At the same time, state supervision over compliance with the special conditions for the processing of personal data of citizens of the Republic of Uzbekistan using information technologies, including on the Internet global information network, is carried out by the State Inspectorate for Control in the Sphere of Informatization and Telecommunications of the Republic of Uzbekistan[15].

The Cabinet of Ministers of the Republic of Uzbekistan:

ensures the implementation of a unified state policy in the field of personal data;

approves state programs in the field of personal data;

determines the procedure for maintaining the State Register of Personal Data Databases;

approves the procedure for registering personal data databases in the State Register of Personal Data Databases;

coordinates the activities of state and economic administration bodies and local state authorities in the field of personal data.

The Cabinet of Ministers of the Republic of Uzbekistan, based on the information submitted by the authorized state body in the field of personal data:

determines the level of protection of personal data depending on threats to the security of such data during their processing;

establishes requirements relating to ensuring the protection of personal data, the fulfillment of which during the processing of personal data ensures the established level of their protection;

establishes requirements for material objects containing biometric and genetic data, as well as for technologies for storing such data separately from personal data.

At the same time, the list of foreign states ensuring an equivalent level of protection of personal data is determined by the Cabinet of Ministers of the Republic of Uzbekistan.

The Personalization Center is the authorized state body in the field of personal data (hereinafter referred to as the authorized state body).

The authorized state body:

implements state policy in the field of personal data;

[15] Regulation "On the Procedure for Exercising State Control over Compliance with the Special Conditions for the Processing of Personal Data of Citizens of the Republic of Uzbekistan", approved by Resolution № 707 of the Cabinet of Ministers dated September 5, 2018 // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

participates in the development and implementation of state programs and other programs in the field of personal data;

approves the Model Procedure for the Processing of Personal Data;

approves the Model Procedure for organizing the activities of a structural subdivision or an authorized person of the owner and/or operator that ensures the processing and protection of personal data;

maintains the State Register of Personal Data Databases;

issues a certificate confirming the registration of a personal data database in the State Register of Personal Data Databases;

within the scope of its powers, exercises state control over compliance with the requirements of legislation on personal data;

submits proposals to the Cabinet of Ministers of the Republic of Uzbekistan on improving the regulatory legal framework in the field of personal data;

submits to the authorized state bodies in the field of ensuring state security the established information applicable to their respective areas of activity;

determines the necessary level of protection of personal data;

analyzes the volume and content of the personal data to be processed, the type of activity, and the reality of threats to the security of personal data;

issues binding instructions to legal entities and individuals on eliminating violations of the legislation on personal data;

cooperates with authorized bodies of foreign states and international organizations in the field of personal data.

In addition, the Regulation "On the Procedure for Exercising State Control over Compliance with the Special Conditions for the Processing of Personal Data of Citizens of the Republic of Uzbekistan", approved by Resolution No. 707 of the Cabinet of Ministers dated September 5, 2018, establishes the procedure for exercising state control over compliance by owners and/or operators with the requirements of legislative acts concerning the collection, systematization, and storage of personal data of citizens of the Republic of Uzbekistan when processing such data using information technologies, including on the Internet global information network, on technical means physically located within the territory of the Republic of Uzbekistan and in personal data databases registered in accordance with the established procedure in the State Register of Personal Data Databases. According to this Regulation, state control over compliance with the special conditions for the processing of personal data of citizens of the Republic of Uzbekistan is exercised through maintaining the Register of Violators of the Rights of Personal Data Subjects (hereinafter referred to as the Register). State control over compliance with the special conditions for the processing of personal data of citizens of the Republic of Uzbekistan using information technologies, including on the Internet global information network, is carried out by the State Inspectorate for Control in the Sphere of Informatization and Telecommunications of the Republic of Uzbekistan (hereinafter referred to as the "Uzkomnazorat" State Inspectorate).

The "Uzkomnazorat" State Inspectorate:

conducts studies, inspections, monitoring, and analysis of compliance by owners and/or operators with the special conditions for the processing of personal data of citizens of the Republic of Uzbekistan;

in the event of violations of the special conditions for the processing of personal data of citizens of the Republic of Uzbekistan using information technologies, including on the Internet global information network, issues instructions that are mandatory for execution by state bodies, individuals, and/or legal entities to eliminate such violations;

draws up protocols on administrative offenses against owners and/or operators processing citizens' personal data using information technologies, including on the Internet global information network, concerning violations of the special conditions for the processing of personal data of citizens of the Republic of Uzbekistan, and submits them to the court for consideration;

provides information to the Cabinet of Ministers of the Republic of Uzbekistan on the activities of owners and/or operators involving the processing of personal data using information technologies, including on the Internet global information network;

maintains the Register and cooperates with authorized bodies of foreign states and international organizations in the field of personal data.

The inclusion in and removal from the Register of owners and/or operators that have violated the special conditions for the processing of personal data of citizens of the Republic of Uzbekistan shall be carried out in accordance with the scheme attached as Annex 1 to the monograph.

The Center for Mass Communications Issues (hereinafter referred to as the Center), within the scope of the tasks assigned to it, monitors the activities of owners and/or operators processing personal data on the Internet global information network in order to identify cases of violations of the special conditions for the processing of personal data of citizens of the Republic of Uzbekistan using information technologies, including on the Internet global information network. When the Center identifies cases of violations by owners and/or operators processing personal data on the Internet global information network of the special conditions for the processing of personal data of citizens of the Republic of Uzbekistan, it submits information thereon to the authorized state body in the field of personal data within 24 hours for the issuance of an opinion.

Within 24 hours after receiving the information submitted by the Center, the authorized state body in the field of personal data submits an opinion to the "Uzkomnazorat" State Inspectorate regarding violations by owners and/or operators processing personal data using information technologies, including on the Internet global information network, of the special conditions for the processing of personal data of citizens of the Republic of Uzbekistan. The opinion of the authorized state body in the field of personal data shall indicate the date on which the opinion was adopted, the subject of the examination (the list of resources of owners and/or operators that have violated the special conditions for the processing of personal data of citizens of the Republic of Uzbekistan), the results of the monitoring conducted (with an indication of the provisions of the legislative acts that were violated), and

proposals regarding inclusion in the Register and taking measures against owners and/or operators of personal data databases. Within one day from the date of receipt of the submitted opinion, the "Uzkomnazorat" State Inspectorate shall issue an appropriate instruction to the owner or operator of the personal data database to eliminate the identified deficiencies, specifying a definite period. The owner or operator of the personal data database shall take measures to eliminate the deficiencies specified in the instruction and timely submit information to the "Uzkomnazorat" State Inspectorate.

If the violations of the law specified in the instruction are not eliminated within the period established in the instruction of the "Uzkomnazorat" State Inspectorate, information about the owner and/or operator shall be entered into the Register. An owner and/or operator that has violated the special conditions for the processing of personal data of citizens of the Republic of Uzbekistan using information technologies, including on the Internet global information network, shall have the right to challenge in court the opinion of the authorized state body in the field of personal data that served as the basis for entering the owner and/or operator into the Register.

The restriction of activities in the national segment of the Internet global information network of owners and/or operators that have violated the special conditions for the processing of personal data of citizens of the Republic of Uzbekistan using information technologies, including on the Internet global information network, shall be carried out by the Ministry of Digital Technologies of the Republic of Uzbekistan (hereinafter referred to as the Ministry). The restriction of access shall apply to the information resources of the Internet global information network of the owner and/or operator of the personal data database whose identification information has been entered into the Register. Within 12 hours after entry into the Register, the "Uzkomnazorat" State Inspectorate shall submit to the Ministry a submission on restricting the access of the owner or operator of the personal data database to the information resources of the Internet global information network. Within 12 hours after entry into the Register, the Ministry shall restrict the access of the owner or operator of the personal data database to the resources of the Internet global information network.

The following shall constitute grounds for the "Uzkomnazorat" State Inspectorate to remove the owner and/or operator of a personal data database from the Register:

1. The opinion of the authorized state body in the field of personal data, based on information from the Center, concerning the elimination by the owner and/or operator of deficiencies on the Internet global information network resource;
2. The entry into legal force of a court decision annulling the opinion of the authorized state body in the field of personal data that served as the basis for entering into the Register the owner and/or operator that violated the special conditions for the processing of personal data of citizens of the Republic of Uzbekistan using information technologies, including on the Internet global information network.

The “Uzkomnazorat” State Inspectorate shall examine the written (electronic) application submitted by the owner of the Internet global information network resource concerning the elimination of deficiencies on the Internet global information network resource and, within one day, submit it to the authorized state body in the field of personal data for issuing an opinion.

The authorized state body in the field of personal data, together with the Center, shall examine, within 24 hours, the information concerning the elimination by the owner and/or operator of deficiencies on the Internet global information network resource and provide an opinion to the “Uzkomnazorat” State Inspectorate. Based on the circumstances identified above, the “Uzkomnazorat” State Inspectorate shall, within 24 hours, remove the owner and/or operator of the personal data database (or the identification information of the information resource) from the Register. After the owner and/or operator of the personal data database (or the identification information of the information resource) has been removed from the Register, the Ministry shall, on the basis of the submission of the “Uzkomnazorat” State Inspectorate, remove the access-restricting barriers within 12 hours. The information recorded, processed, and otherwise carried out in the Register, as well as the history of changes thereto, shall be stored in accordance with the established procedure.

The experience of foreign countries and GDPR standards indicate that, in ensuring the inviolability of personal data, powers are usually centralized within a single independent body — the Data Protection Authority (DPA). This body simultaneously performs the functions of supervision, monitoring, and administrative restriction. Institutional coordination is carried out through the state’s ministries of digitalization, communications, or justice, while law-enforcement restrictions are implemented through judicial bodies. The table in accordance with Annex 2 provides complete and up-to-date information on the system of authorized state bodies responsible for processing and supervising personal data, based on the experience of 200 countries around the world.

CHAPTER II. REGULATORY AND LEGAL REGIME OF PERSONAL DATA PROCESSING AND STATUS OF SUBJECTS

2.1-§. Content and essence of personal data processing

The subject and the operator are participants in the processing of personal data. The subject's legal representative, the owner, and third parties may also act as participants in the processing of personal data. Under the applicable legislation, while the legal representatives of citizens may be their parents, adoptive parents, or guardians, individuals and legal entities, state bodies and organizations, civil society institutions, and business entities are considered third parties. The processing of personal data means carrying out one action or a set of actions involving the collection, systematization, storage, modification, supplementation, use, provision, dissemination, transfer, depersonalization, and destruction of personal data.

By the processing of personal data, we should understand the creation, use, modification, destruction of personal data, or the performance of any action related thereto.

A personal data database is formed by collecting personal data that is necessary and sufficient for the performance of tasks carried out by the owner and/or operator of the personal data database, as well as by a third party. The procedure and principles for collecting and systematizing personal data shall be independently determined by the owner and/or operator. Personal data shall be stored in a form that allows the identification of the subject to the extent required by the purposes previously stated at the time of collection of the personal data. The storage period of personal data shall be determined by the date on which the purpose of their collection and processing is achieved. The modification and supplementation of personal data shall be carried out by the owner and/or operator on the basis of an application by the subject, no later than within three days from the time such application is submitted. The modification and supplementation of personal data that do not correspond to reality shall be carried out immediately upon identification of such inconsistency. Actions involving personal data aimed at achieving the objectives of the activities of the owner, operator, and third party constitute the use of personal data.

The use of personal data by the owner, operator, and third party shall be carried out only for the purposes previously stated for the collection of such personal data, provided that the necessary level of protection of such data is ensured. The use of personal data by employees of the owner and/or operator, as well as of a third party, whose activities are related to the processing of personal data, shall be carried out only in accordance with their professional, official, or employment duties. Employees of the owner and/or operator, as well as of a third party, whose activities are related to the processing of personal data, shall not disclose personal data entrusted to them or that have become known to them due to the performance of their professional, official, or employment duties. Actions aimed at disclosing

personal data to a specific person constitute the provision of personal data. The provision of personal data to state administration bodies shall be carried out free of charge. If the subject refuses to provide their personal data, they shall have the right not to state the reasons for their refusal. Actions aimed at disclosing personal data to an indefinite range of persons, including making personal data publicly available through the mass media, posting them on the Internet global information network, or otherwise providing access to personal data, constitute the dissemination of personal data.

Where the dissemination of personal data goes beyond the previously stated purposes of collecting such data, such dissemination shall be carried out with the consent of the subject. The transfer of personal data by the owner and/or operator outside the territory of the Republic of Uzbekistan constitutes cross-border transfer of personal data. Cross-border transfer of personal data shall be carried out to the territories of foreign states that ensure an equivalent level of protection of the rights of personal data subjects.

Cross-border transfer of personal data to the territories of foreign states that do not ensure an equivalent level of protection of personal data may be carried out in the following cases:

1. when the subject has given consent to the cross-border transfer of their personal data;
2. when it is necessary to protect the constitutional order of the Republic of Uzbekistan, maintain public order, protect the rights and freedoms of citizens, and protect the health and morality of the population;
3. in cases provided for by international treaties of the Republic of Uzbekistan.

Cross-border transfer of personal data may be prohibited or restricted for the purposes of protecting the foundations of the constitutional order of the Republic of Uzbekistan, the morality, health, rights, and legitimate interests of citizens of the Republic of Uzbekistan, and ensuring the defense and state security of the country.

Actions that, as a result of their implementation, make it impossible to determine the attribution of personal data to a specific subject constitute depersonalization of personal data. When processing personal data for the purposes of conducting historical, statistical, sociological, and scientific research, the owner and operator, as well as a third party, shall depersonalize such data. Actions that, as a result of their implementation, make it impossible to restore personal data constitute destruction of personal data.

Personal data shall be destroyed by the owner and/or operator, as well as by a third party, in the following cases:

when the purpose of processing personal data has been achieved;

when the subject withdraws the consent given for the processing of personal data;

when the period for processing personal data established by the consent given by the subject has expired;

when a court decision has entered into legal force.

In order to ensure that all of the above actions are carried out correctly and systematically, a subdivision shall be established or an authorized person shall be appointed by the owner and/or operator, taking into account the scope of tasks, the number of databases, and the degree of their automation, for the purpose of ensuring the processing and protection of personal data. The subdivision or authorized person shall perform only the lawful instructions of the owner and/or operator and shall be directly accountable to the head of the owner and/or operator. The subdivision or authorized person shall carry out its activities in accordance with the Law of the Republic of Uzbekistan "On Personal Data," other legislative acts in the field of personal data, and internal rules approved by the owner and/or operator. When the head and employees of the subdivision or the authorized person are transferred to another position (when the subdivision is liquidated) or when their employment contracts are terminated, their right to access the database shall be revoked by the owner and/or operator no later than their last working day. The following shall constitute the main tasks of the subdivision or authorized person:

1) ensuring the protection, integrity, and preservation of personal data and compliance with their confidentiality during the processing of personal data;

2) preventing unlawful processing of personal data and, when violations of the requirements established by legislation are identified, blocking (restricting) personal data in coordination with the owner and/or operator;

3) organizing and coordinating the information security policy of the owner and/or operator for ensuring the security of the personal data database;

4) organizing seminars and training sessions for employees working with personal data;

5) studying the causes that pose threats to the owner's and/or operator's personal data database security and developing proposals and recommendations for eliminating and preventing existing deficiencies.

The subdivision or authorized person may also perform other tasks in accordance with legislative acts. In this case, the owner and/or operator shall ensure that any tasks performed by the subdivision or authorized person do not lead to a conflict of interests.

The subdivision or authorized person shall have the following rights:

1) temporarily suspending the operation of personal data databases, with the permission of the owner and/or operator, until the deficiencies identified in the personal data database are eliminated;

2) applying to the relevant authorized body to obtain appropriate recommendations regarding any problems and/or misunderstandings arising in the process of working with personal data;

3) having unrestricted access to the personal data databases available to the owner and/or operator for the purpose of performing its duties;

4) obtaining information from the owner and/or operator about the purposes of processing personal data.

The subdivision or authorized person may also have other rights in accordance with legislative acts and/or internal rules approved by the owner or operator.

The obligations of the subdivision or authorized person shall include:

1) exercising internal control over compliance by employees of the owner and/or operator with legislative acts on personal data;

2) conducting periodic inspections of the personal data database and the activities of employees working with such database, and improving the status and practices of personal data processing;

3) organizing the destruction of personal data upon expiration of the period for their storage or after the purpose of their collection and processing has been achieved;

4) taking legal, organizational, and technical measures to protect personal data;

5) compiling a list of employees granted the right to work with personal data databases, maintaining and analyzing electronic records reflecting the login of the owner's and/or operator's employee who has accessed personal data databases, the time of access, the name of the resource, and other information;

6) ensuring the possibility of restoring personal data that have been modified or destroyed as a result of unauthorized access to personal data;

7) storing, modifying, supplementing, using, providing, disseminating, transferring, depersonalizing, and destroying data in personal data databases, blocking (restricting) such data, identifying and analyzing attempts at unauthorized access, and taking measures for their prompt elimination;

8) where necessary, organizing activities to ensure the real-time storage of copies (replicas) of electronic (digital) data contained on server devices where personal data are stored in another territory;

9) ensuring the confidentiality of personal data during the period of employment and thereafter.

The subdivision or authorized person may also perform other obligations in accordance with legislative acts and/or internal rules approved by the owner or operator.

The substance and essence of the concepts relating to the processing of personal data are provided in Annex 3, and understanding their meaning contributes to the development of skills for the proper implementation of these processes.

The system thus developed fully encompasses 4 fundamental stages:

1. **Legal and operational framework**: Classical regulatory practices such as collection, storage, provision, transfer, blocking, depersonalization, and destruction;

2. **Information and cybersecurity level**: Tokenization, homomorphic encryption, pseudonymization, quarantine, DLP control, and localization;

3. **Algorithmic and artificial intelligence architecture**: Profiling, federated learning, synthetic data generation, scoring, and dynamic micro-consent;

4. **Quantum-biological and cognitive level**: DNA-genomic engineering, neurocognitive traces, shields against quantum de-anonymization, and cognitive substrate transfer.

This four-level framework encompasses all theoretical, practical, and prospective technological stages of the personal data life cycle.

These concepts can be divided into the following 7 blocks, namely:

I. Fundamental Regulatory and Legal Concepts

personal data;
subject;
owner;
operator;
third party;
processing;
consent;
lawfulness;
purpose limitation;
data minimization.

II. Basic Operations of Data Processing

collection;
recording;
systematization;
storage;
search;
review;
use;
modification;
supplementation;
provision;
dissemination;
cross-border transfer;
integration;
blocking;
depersonalization;
destruction.

III. Modern Technologies for Ensuring the Confidentiality and Protection of Personal Data

pseudonymization;
tokenization;
data masking;
obfuscation;
homomorphic encryption;
differential privacy;
zero-knowledge proof;
federated learning;
TEE;
synthetic data.

IV. Analytics and Artificial Intelligence-Based Processing

profiling;
scoring;
clustering;
anomaly detection;

automated decision-making;
AI model training;
data enrichment;
synthetic data generation;
predictive analytics.

V. Cybersecurity and Technical Protection

DLP;
logging;
audit trail;
access control;
RBAC;
least privilege;
encryption;
key management;
backup;
recovery;
replication;
quarantine;
data sanitization.

VI. Exercise and Governance of Rights

data portability;
consent management;
consent revocation;
data retention;
legal hold;
right to erasure;
right to rectification;
right of access;
de-indexing;
DPIA;
Privacy by Design;
Privacy by Default.

VII. Prospective and Futuristic Technologies

digital twin;
neurodata;
BCI;
ambient sensing;
genomic processing;
quantum-resistant cryptography;
post-mortem digital identity;
neural digital twins and others.

These can be referred to in one term as a **comprehensive scientific-legal-technological taxonomy of personal data processing**.

As an independent scientific terminological taxonomy at the intersection of personal data protection, cyber law, artificial intelligence, and digital transformation,

these concepts constitute a part of cyber terminology and may also be referred to as the **“Legal-Technological Taxonomy of Personal Data Processing.”** The main methodological formula in this regard is as follows:

“legal category → processing operation → technological mechanism → risk → protection measure → subject right → legal consequence”.

2.2-§. Procedure for Processing Personal Data

The processing of personal data shall be carried out in accordance with the fundamental principles of the Law of the Republic of Uzbekistan “On Personal Data.” These principles are as follows:

1) respect for the constitutional rights and freedoms of individuals and citizens;
2) lawfulness of the purposes and methods of processing personal data;
3) accuracy and reliability of personal data;
4) confidentiality and protection of personal data;
5) equality of the rights of subjects, owners, and operators;
6) security of the individual, society, and the state.

The processing of personal data shall be carried out in the following cases:

when the subject has given consent to the processing of such data;

when it is necessary to process such data for the performance of a contract to which the subject is a party, or to take measures at the request of the subject prior to entering into such a contract;

when it is necessary to process such data for the fulfillment of obligations of the owner and/or operator established by legislation;

when it is necessary to process such data to protect the legitimate interests of the subject or another person;

when it is necessary to process such data for the exercise of the rights and legitimate interests of the owner and/or operator or a third party, or for the achievement of socially significant purposes, provided that the rights and legitimate interests of the subjects of personal data are not violated;

when personal data are processed for statistical or other research purposes, subject to their mandatory depersonalization;

if such data have been obtained from publicly available sources.

Where the processing of personal data is necessary for the purpose of protecting the rights and legitimate interests of the subject, such processing may be carried out without the subject’s consent until it becomes possible to obtain such consent.

The purposes of processing personal data shall be determined by regulatory legal acts, regulations, constituent documents, or other documents regulating the activities of the owner and/or operator and shall comply with the Law of the Republic of Uzbekistan “On Personal Data.”

The purposes of processing personal data shall correspond to the purposes previously stated at the time of their collection, as well as to the rights and obligations of the owner and/or operator.

If the purpose of processing personal data changes, the owner and/or operator shall obtain the subject’s consent to the processing of their data in accordance with the changed purpose.

Personal data shall be accurate and reliable and, where necessary, shall be modified and supplemented.

The scope of personal data that may be entered into a personal data database shall be determined by the subject in accordance with the Law of the Republic of Uzbekistan "On Personal Data." The scope and nature of the personal data being processed shall correspond to the purposes and methods of their processing.

Personal data shall be processed in a form that permits the identification of the subject or in a depersonalized form.

The period for processing personal data shall not exceed the period during which the subject's consent to the processing of their personal data remains valid.

When processing personal data by the owner and/or operator or a third party, the following requirements shall be complied with:

1) processing personal data for specific and predetermined purposes;

2) preventing the combination of personal data databases whose purposes are incompatible with each other during the processing of personal data;

3) ensuring the accuracy, reliability, integrity, and completeness of personal data;

4) if the storage period of personal data is not established by legislation or by a contract concluded with the subject, storing personal data for a period not exceeding the period required to achieve the purposes of their processing;

5) unless otherwise provided by legislative acts, ensuring the destruction or depersonalization of the personal data being processed after the purposes of their processing have been achieved or when the need to achieve such purposes no longer exists.

It is known that personal data may exist in two forms, namely:

1) publicly available personal data;

2) non-publicly available personal data.

Personal data that may be freely accessed with the consent of the subject or to which confidentiality requirements do not apply are publicly available personal data. These include personal data placed in publicly available sources, including electronic information resources, mass media, and other sources.

Non-publicly available personal data are personal data for which the subject has not given consent to free access and the use of which is restricted by legislative acts. They may include biographical, biometric, genetic, special, and other data relating to the subject.

The processing of personal data shall be carried out by the owner and/or operator, as well as by a third party, with the consent of the subject or their legal representative; however, consent shall not be required in the following cases, including:

1) when it is necessary to process such data for the performance of a contract to which the subject is a party, or to take measures at the request of the subject prior to entering into such a contract;

2) when it is necessary to process such data for the fulfillment of obligations of the owner and/or operator established by legislation;

3) when it is necessary to process such data to protect the legitimate interests of the subject or another person;

4) when it is necessary to process such data for the exercise of the rights and legitimate interests of the owner and/or operator or a third party, or for the achievement of socially significant purposes, provided that the rights and legitimate interests of the subjects of personal data are not violated;

5) when personal data are processed for statistical or other research purposes, subject to their mandatory depersonalization;

6) if such data have been obtained from publicly available sources.

The subject's consent to the processing of special personal data shall be obtained in written form or in the form of an electronic document.

If the purposes of processing personal data are clearly specified in an offer (public contract), acceptance (confirmation) of the offer (public contract) shall be considered the subject's consent to the processing of personal data.

The subject's consent to the requirements and conditions established for using the services of the owner and/or operator shall be considered the subject's consent to the processing of the subject's personal data by the owner and/or operator.

The subject or their legal representative shall have the right to withdraw their consent to the processing of personal data at any time.

In this case, the subject's personal data shall be destroyed by the owner and/or operator no later than the next working day following the day on which the application (notification) to terminate the processing of personal data is received.

The following information shall be specified in the subject's consent to the processing of personal data:

1) the name and TIN of the operator (the surname, first name, and patronymic and personal identification number of an individual);

2) the surname, first name, and patronymic of the subject and the details of the identity document;

3) the purposes of processing personal data;

4) the list of the subject's personal data for which consent to processing is being given;

5) the period or duration for which consent to the processing of personal data is valid;

6) consent to the provision of personal data to third parties and/or the cross-border transfer of such data;

7) consent to the dissemination of personal data in publicly available sources;

8) other information.

The consent of the subject or their legal representative shall not be required for the collection of publicly available personal data.

Data collected using video recording devices installed for the purpose of privacy protection or as a precautionary measure shall not be considered the collection of personal data if their processing for specific purposes is not envisaged.

In this case, the dissemination of data collected using such video recording devices shall not be permitted.

The procedures and principles for systematizing personal data shall be independently determined by the owner and/or operator.

Personal data shall be stored in a form that makes it possible to identify the data subject to the extent required by the purposes previously stated at the time of collecting the personal data.

Personal data shall be amended and supplemented by the owner and/or operator on the basis of an application (request) from the data subject or his or her legal representative, as well as in other cases provided for by legislative acts.

Amendments and additions to personal data shall be made by the owner and/or operator no later than three days from the time the application (request) is submitted by the data subject, and the data subject shall be notified thereof.

Amendments and additions to inaccurate personal data shall be made immediately upon identification of such discrepancy.

Personal data shall be used by the owner and/or operator, as well as by a third party, solely for the purposes previously stated for their collection.

The use of personal data by employees of the owner and/or operator, as well as of a third party, whose activities are related to the processing of personal data, shall be carried out solely in accordance with their professional, official, or employment duties.

Where personal data are disseminated beyond the previously stated purposes of their collection, such dissemination shall be carried out with the consent of the data subject.

When personal data are requested by state bodies, a notification thereof shall be sent to the personal data subject (except for cases involving state secrets and information whose use is restricted in accordance with legislation).

Personal data shall be provided to economic associations, state organizations and institutions, and non-governmental organizations with the consent of the data subject.

Notification of the data subject and obtaining his or her consent shall not be required in the following cases:

1) when state bodies exercise their powers;

2) when personal data are provided for processing for historical, statistical, sociological, or scientific purposes;

3) when personal data are collected from publicly available sources.

Cross-border transfer of personal data shall be carried out to the territories of foreign states that ensure equal protection of the rights of personal data subjects.

Cross-border transfer to the territories of foreign states that do not ensure equal protection of personal data may be carried out in the following cases:

1) when the data subject has given consent to the cross-border transfer of his or her personal data;

2) when it is necessary to protect the constitutional order of the Republic of Uzbekistan, maintain public order, and protect the rights and freedoms of citizens, as well as the health and morality of the population;

3) in cases provided for by international treaties of the Republic of Uzbekistan.

When personal data are processed for the purposes of conducting historical, statistical, sociological, or scientific research, the owner and operator, as well as a third party, shall depersonalize such data.

Obtaining the consent of the data subject for the depersonalization of personal data shall not be required.

Depersonalization of personal data shall exclude the possibility of restoring the personal data.

Personal data shall be destroyed by the owner and/or operator, as well as by a third party, within three days in the following cases:

1) upon achievement of the purpose of processing personal data;

2) upon withdrawal of the data subject's consent given for the processing of personal data;

3) upon expiry of the period for processing personal data established by the consent given by the data subject;

4) upon entry into legal force of a court decision.

Where the processing of personal data concerning a data subject is carried out in violation of legislation, such data shall be destroyed from the source in which they are stored within one working day upon the request of the data subject or his or her legal representative, pursuant to a court decision, or at the request of another competent state body.

In accordance with Article 27-1 of the Law of the Republic of Uzbekistan "On Personal Data", personal data databases that are required to be stored within the territory of the Republic of Uzbekistan shall be registered in the State Register of Personal Data Databases. Registration of a personal data database shall be carried out by notification under the application principle. An application for registration of a personal data database in the State Register of Personal Data Databases shall be submitted to the competent state authority.

Personal data databases containing:

1) personal data relating to participants (members) of a public association or religious organization and processed accordingly by the public association or religious organization, provided that such data are not disseminated or disclosed to third parties;

2) personal data made publicly available by the data subject;

3) only the surname, first name, and patronymic of the data subjects;

4) personal data necessary for a one-time entry of the data subject into the territory where the owner and/or operator is located or for other similar purposes;

5) personal data entered into information systems having the status of automated state information systems;

6) personal data processed without the use of automation tools;

7) personal data processed in accordance with labor legislation,

shall not be subject to registration.

The owner and/or operator shall notify the competent state authority of each change in the information required for registration of the respective personal data database no later than ten calendar days from the date such change occurs.

The Administrative Regulation for the provision of the public service for maintaining the State Register of Personal Data Databases, approved by Resolution No. 71 of the Cabinet of Ministers dated February 8, 2020, establishes the procedure for providing the public service (hereinafter referred to as the public service) for registering personal data databases in the State Register of Personal Data Databases, removing them from the register, and making amendments and additions to the register. However, the requirements of this Regulation shall not apply to:

processing of personal data by an individual for personal and household purposes and without connection to his or her professional or commercial activities;

formation, storage, and use of documents of the National Archival Fund and other archival documents containing personal data;

processing of personal data classified as information constituting state secrets;

processing of personal data obtained in the course of operational-search, intelligence, and counterintelligence activities, combating crime, maintaining law and order, as well as within the framework of combating the legalization of proceeds derived from criminal activity.

The State Register of Personal Data Databases shall be established for the purpose of registering personal data databases and systematizing their records, as well as monitoring compliance with the requirements of legislative acts in the process of processing personal data.

Personal data databases shall be registered by the owner and/or operator in the State Register.

The applicant personally applies to the Public Services Center to use the public service or registers on the Unified Interactive Public Services Portal of the Republic of Uzbekistan (hereinafter referred to as the UIPS Portal) to use public services in electronic form. Applications may be submitted through the UIPS Portal 24 hours a day, every day, regardless of weekends and public holidays. In this case, if applications are submitted after working hours or on weekends and public holidays, the next working day shall be considered the day on which the applications are received by and accepted by the competent authority. If the applicant applies in person, an employee of the Public Services Center shall fill out the questionnaire on behalf of the applicant, whereas if the applicant applies through the UIPS Portal, the applicant shall independently fill out the questionnaire electronically in the following form in accordance with this Regulation:

QUESTIONNAIRE
ON THE PROVISION OF PUBLIC SERVICES FOR MAINTAINING THE STATE REGISTER OF PERSONAL DATA DATABASES

I. Information about the Applicant – Individual	
Surname:	
First name:	

Patronymic:	
Personal Identification Number of an Individual (PINFL):	
Telephone number:	
Email address (if available):	
Residential address:	
II. Information about the Applicant – Legal Entity	
Official name (full):	
Location:	
Telephone number:	
Email address (if available):	
TIN:	
III. Information about the Database of the Owner and/or Operator	

Name of the personal data database:

Date of commencement of processing of personal data:

Term or condition for completion of processing of personal data:

Country where the personal data database is located:

Address where the personal data database is located:

Purpose of processing personal data:

Is the personal data database managed remotely?

Does the personal data database belong to this owner and/or operator?

Is there a possibility of cross-border transfer of personal data during the processing of personal data?

Full name and position of the person responsible for the processing of personal data:

Rights with respect to the personal data database:

List of personal data processed in the personal data database:

□ Full name	□ Year of birth	□ Month of birth
□ Day of birth	□ Place of birth	□ Citizenship
□ Personal Identification Number of an Individual (PINFL)	□ Photograph	□ Educational institutions
□ Residential address	□ Marital status	□ Employment activity
□ Monthly expenses	□ Telephone number	□ Religious views
□ Racial origin	□ Social origin	□ Trade union membership
□ Political party membership	□ Nationality	□ Financial status
□ Physical condition	□ Property status	□ Criminal record status
□ Relation to military service	□ Mental state	

Biometric data:
Genetic data:

When applying through a representative to use public services, a power of attorney confirming the representative's authority shall be attached to the questionnaire. After the necessary information has been entered into the questionnaire, the applicant shall verify the accuracy of the information and confirm it using modern means of identification of signatures (electronic digital signature, fingerprinting, Mobile-ID, and others). If the applicant applies through the UIPS Portal, it shall not be required to confirm the questionnaire with an electronic digital signature. The public service shall be provided free of charge.

The authorized body shall register the personal data database in the State Register or refuse to register it within five business days from the date following the date on which the questionnaire is received.

In this case, on the same day on which the authorized body registers the personal data database in the State Register, it shall issue a certificate of registration in the State Register in the following form, containing a QR code (matrix barcode), certify it with its electronic digital signature, and send it to the Public Service Center (if the applicant applied in person) or to the applicant (if the applicant applied electronically) through the Unified Interactive Public Services Portal:

"

my.gov.uz

O'zbekiston Respublikasi Ichki ishlar vazirligi huzuridagi Migratsiya va personallashtirish departamenti

Hujjat yaratilgan sana: Hujjat berilgan:
Ariza raqami:

Shaxsga doir ma'lumotlar bazasining davlat reestriga kiritilganligi to'g'risida GUVOHNOMA

Shaxsga doir ma'lumotlar bazasi nomi:
Davlat ro'yxatidan o'tkazilgan sana (kun, oy, yil):
Shaxsga doir ma'lumotlar bazasining ishlov berish maqsadi:
Soliq to'lovchining identifikasiatsiya raqami (STIR):
Mulkdor yoki operatorning pochta manzili:
Shaxsga doir ma'lumotlar bazasida biometrik ma'lumotlar:
Shaxsga doir ma'lumotlar bazasida genetik ma'lumotlar:
Shaxsga doir ma'lumotlar bazasida maxsus ma'lumotlar:

Vakolatli davlat organi rahbari F.I.O: QR-kod

Mazkur hujjat Vazirlar Mahkamasining 2017-yil 15-sentabrdagi 728-son qarori bilan tasdiqlangan O'zbekiston Respublikasi Yagona interaktiv davlat xizmatlari portali to'g'risidagi nizomga muvofiq shakllantirilgan elektron hujjatning nusxasi hisoblanadi. Elektron hujjatning nusxasida ko'rsatilgan ma'lumotlar to'g'riligini tekshirish uchun repo.gov.uz *veb-saytiga o'ting va elektron hujjatning noyob raqamini kiriting yoki mobil telefon yordamida QR-kodni skaner qiling.*

Diqqat! Vazirlar Mahkamasining 2017-yil 15-sentabrdagi 728-son qaroriga muvofiq elektron hujjatlardagi ma'lumotlar qonuniy hisoblanadi. Davlat organlariga Yagona portalda shakllantirilgan elektron hujjatlarning nusxalarini qabul qilishni rad etishlari qat'iyan taqiqlangan.

"

The inaccuracy or incomplete submission of the information specified in the questionnaire shall constitute grounds for refusal to provide the public service.

Refusal to provide the public service on other grounds, including grounds of expediency, shall not be permitted.

The Public Service Center shall send the result of the service to the applicant's electronic address within ten minutes and shall notify the applicant thereof through the information and communication system. At the applicant's request, the Public Service Center may provide the result of the service in electronic or paper form. Based on the decision adopted on the registration in the State Register, the responsible employee of the authorized body shall register the personal data database in the State Register with a unique registration number.

The date of issuance of the certificate of registration in the State Register shall be deemed the date of registration in the State Register.

If it becomes necessary to make amendments and additions to the registration data in the State Register, the applicant shall reapply in accordance with the procedure established above by this Regulation no later than seven business days.

In this case, the authorized body shall review the questionnaire within five business days and send a notification concerning the amendments made to the Public Service Center or, if the application was submitted through the Unified Interactive Public Services Portal, to the applicant. The amendments and additions shall be entered into the State Register without changing the registration number.

The personal data database shall be removed from the State Register, and the public service shall be provided upon application in accordance with the procedure established above, in the following cases:

upon the application of the owner and/or operator for removal from the State Register;

upon termination of the activities of the owner and/or operator;

on the basis of a court decision to terminate the processing of personal data by the owner and/or operator.

After removal from the State Register, its registration number shall not be used thereafter, and the previously issued certificate of registration of the personal data database in the State Register shall be deemed invalid. The information contained in the State Register shall be publicly accessible for familiarization by legal entities and individuals.

Information concerning the registration of the owner and/or operator in the State Register shall be obtained automatically by entering the registration number of the relevant database into the information system for maintaining the State Register.

The Public Service Center and the authorized body shall ensure the confidentiality of information obtained as a result of carrying out their activities.

The actions or inaction of the authorized body concerning registration in the State Register may be appealed by the owner and/or operator, in accordance with the procedure established by law, to a superior state body or to a court.

All of the above processes shall be carried out in accordance with the following scheme:

SCHEME

MAINTENANCE OF THE STATE REGISTER OF PERSONAL DATA DATABASES

Stages	Subjects	Activities	Time limits for completion
Stage 1	Applicants	Apply for the state service by personally visiting the Public Services Center or through the Unified Interactive Public Services Portal of the Republic of Uzbekistan (hereinafter referred to as the – Unified Portal).	At their own discretion
Stage 2	1. Public Services Center 2. Unified Interactive Public Services Portal	1. The Center employee fills out the application form and sends it to the authorized body. 2. The completed application form is automatically sent to the authorized body.	1. Within 10 minutes after the application form is completed 2. In real-time mode
Stage 3	Department of Migration and Personalization	1. Registers personal data databases in the State Register of Personal Data Databases. 2. Refuses to register personal data databases in the State Register of Personal Data Databases.	Within 5 working days
Stage 4	1. Public Services Center 2. Unified Interactive Public Services Portal	1. Sends the result of the service to the applicant's email address and notifies the applicant thereof through the information and communication system. 2. Sends the result of the service to the applicant automatically.	1. Within 10 minutes 2. In real-time mode

The data subject gives consent to the processing of personal data in any form that makes it possible to confirm the fact of its receipt.

Consent of the subject in writing, including in the form of an electronic document, is required for the processing of special personal data.

If the subject is legally incapable or has limited legal capacity, the subject's legal representative gives consent for the processing of the subject's personal data in writing, including in the form of an electronic document.

For the processing of personal data of minor subjects, their parents (guardians, custodians), and in their absence, the guardianship and custodianship authorities, give consent in writing, including in the form of an electronic document.

In the event of the death of the subject, consent for the processing of their personal data, if the subject did not give such consent during their lifetime, is given by their heirs in writing, including in the form of an electronic document.

The processing of personal data of a subject who has been declared deceased by a court or who has been declared missing shall be carried out with the written consent of their heirs, including in the form of an electronic document.

The subject withdraws the consent given for the processing of personal data in the same form in which such consent was given or in writing, including in the form of an electronic document.

The subject shall have the right to receive information pertaining to the processing of their personal data, containing the following:

1) confirmation of the fact that their personal data have been processed;

2) the grounds and purposes for processing personal data;

3) the methods used in processing personal data;

4) the name of the owner and (or) operator and their (its) location (postal address), information about persons who have access to personal data or to whom personal data may be disclosed on the basis of a contract concluded with the owner and (or) operator or on the basis of law;

5) the composition of the personal data pertaining to the respective subject and being processed, and the source from which they were obtained, unless this Law provides for another procedure for providing such information;

6) the periods for processing personal data, including the periods for their storage;

7) the procedure for exercising by the subject the rights provided for in Article 30 of the Law of the Republic of Uzbekistan "On Personal Data";

8) information on the completed or intended cross-border transfer of personal data.

If providing the subject with their personal data would violate the rights and legitimate interests of other persons, the subject's right to receive information pertaining to the processing of their personal data may be restricted.

The procedure for providing third parties with information pertaining to the processing of the subject's personal data shall be determined in accordance with the terms of the subject's consent to the processing of personal data.

The owner and (or) operator shall be exempt from the obligation to provide the subject with information pertaining to the processing of their personal data if:

the subject has previously been informed of the processing of their personal data;

the personal data have been made publicly available by the subject or have been obtained from a publicly available source;

the provision of such information would result in the violation of the rights and legitimate interests of individuals and legal entities.

A notification of refusal to provide information pertaining to the processing of personal data shall be sent in writing to the subject who submitted the request within ten days.

The subject may appeal the decision to refuse to provide information pertaining to the processing of personal data to the authorized state body or to a court.

When the subject's personal data are entered into a personal data database, the subject shall be notified in writing of the purposes of processing personal data and of their rights established by Article 30 of the Law of the Republic of Uzbekistan "On Personal Data".

If personal data are provided to a third party, the owner and (or) operator shall notify the subject thereof in writing within three days.

Written notification of the subject shall not be carried out in the following cases:

when state bodies exercise their powers;

when personal data are provided for processing for historical, statistical, sociological or scientific purposes;

when personal data are collected from publicly available sources.

The subject shall have the right not to be subject to a decision based solely on automated processing of their personal data that concerns their rights and legitimate interests and produces legal consequences, except for the cases provided for in the second part of this Article.

A decision may be made based solely on automated processing of the subject's personal data in the following cases:

when the subject's consent in writing, including in the form of an electronic document, is available;

if the decision is being made for the performance of a contract between the owner and the subject or for the fulfilment of the terms of a previously concluded contract;

in cases provided for by legislation.

The owner and (or) operator shall explain to the subject the procedure for making a decision based solely on automated processing of their personal data and the possible legal consequences of such a decision, provide the opportunity to object to such a decision, and also explain to the subject the procedure for protecting their rights and legitimate interests.

The owner and (or) operator shall consider the objection specified in the third part of this Article and shall notify the subject in writing of the results of consideration of such objection within ten days.

Information concerning racial or social origin, political, religious or ideological beliefs, membership in political parties and trade unions, as well as information concerning physical or mental health, private life and criminal convictions shall constitute special personal data.

The processing of special personal data shall be prohibited, except for the cases provided for in the third part of this Article.

The processing of special personal data shall be permitted in the following cases:

by an authorized state body for the purpose of ensuring the protection of state security from external and internal threats;

if the subject has given consent in writing, including in the form of an electronic document, to the processing of their special personal data;

if the special personal data have been made public by the subject in publicly available sources;

for the purpose of protecting the rights and legitimate interests of the subject or other persons;

when courts and relevant law enforcement bodies carry out their activities within the framework of an initiated criminal case or enforcement proceedings;

when measures aimed at combating the legalization of proceeds from criminal activity and the financing of terrorism are carried out by prosecution authorities;

when state statistics bodies carry out their activities, as well as when personal data are used by other state bodies for statistical purposes, provided that such data are depersonalized;

when medical and social services are provided or medical diagnosis or treatment is prescribed, provided that such data are processed by a medical worker or another person of a healthcare institution who is entrusted with the obligation to ensure the protection of personal data;

when rights are exercised and obligations are fulfilled in the field of labor relations;

when the protection of the legitimate interests of the subject or a third party is ensured if the subject is legally incapable or has limited legal capacity;

when personal data, including personal data of candidates for elected state positions, are made public;

when the activities of a non-governmental non-profit organization, religious organization, political party or trade union are carried out, provided that the processing relates only to the personal data of members or employees of such organizations and associations and such data are not provided to a third party without the consent of the subjects;

when processing the personal data of children deprived of parental care, when such children are placed in families of citizens for upbringing (foster care), as well as when other measures to ensure guardianship and custody are carried out;

when personal data are processed for the purpose of ensuring state security;

when information concerning criminal convictions is processed by state bodies, as well as by other persons within the scope of their powers.

Personal data describing the anatomical and physiological characteristics of the subject shall constitute biometric data.

Personal data relating to inherited or acquired characteristics of the subject and resulting from the analysis of the subject's biological profile or the analysis of another element that makes it possible to obtain alternative information shall constitute genetic data.

Biometric and genetic data used to identify the subject may be processed only if the consent of the respective subject is available, except in cases related to the implementation of international treaties of the Republic of Uzbekistan, the administration of justice, and enforcement proceedings, as well as in other cases provided for by legislation.

The use of biometric and genetic data in electronic form outside information systems and their storage outside such systems may be carried out only on material information carriers that exclude unauthorized access to them.

2.3-§. Rights and obligations of participants in personal data processing

The data subject shall have the right to:

1) know of the existence of their personal data and their composition held by the owner and (or) operator, as well as by a third party;

2) receive, upon request, information from the owner and (or) operator concerning the processing of personal data;

3) receive information from the owner and (or) operator on the conditions for providing access to their personal data;

4) apply to the authorized state body or a court concerning the protection of their rights and legitimate interests with respect to their personal data;

5) give consent to the processing of their personal data and withdraw such consent, except in cases provided for by this Law;

6) give consent to the owner and (or) operator, as well as to a third party, for the dissemination of their personal data in publicly accessible sources of personal data;

7) have the right to require the owner and (or) operator to temporarily suspend the processing of their personal data if the personal data are incomplete, outdated, inaccurate, obtained unlawfully, or are not necessary for the purposes of processing.

The disposal of the personal data of a subject recognized as legally incapable or having limited legal capacity shall be carried out by their legal representative.

It shall be the obligation of the subject to provide their personal data for the purposes of protecting the foundations of the constitutional order of the Republic of Uzbekistan, the spirituality, health, rights and legitimate interests of citizens of the Republic of Uzbekistan, and ensuring the defense of the country and state security.

The owner and (or) operator shall have the right to process personal data.

The owner and (or) operator shall:

1) comply with the legislation on personal data;

2) upon the subject’s request, provide information pertaining to the processing of their personal data;

3) approve the composition of personal data that is necessary and sufficient for the performance of their functions;

4) take measures to destroy personal data upon achievement of the purpose for which the personal data were processed, as well as in other cases established by this Law;

5) in cases provided for by legislation, provide evidence that the subject’s consent to the processing of their personal data has been obtained;

6) amend and (or) supplement personal data if the reliability of the new information is confirmed by documents, or, if it is impossible to make such amendments and (or) supplements, destroy such information;

7) temporarily suspend the processing of personal data or destroy them if there is information that the conditions for processing personal data have been violated;

8) ensure the subject's ability to electronically submit documents for the temporary suspension of the processing of their personal data and (or) their destruction;

9) notify the subject, as well as other participants in the processing of personal data, in writing when personal data are amended, destroyed or access to them is restricted;

10) notify the subject in writing if personal data are provided to a third party;

11) register personal data databases owned by them and (or) being processed;

12) take necessary legal, organizational and technical measures to protect personal data.

The owner and (or) operator shall have the right to entrust the processing of personal data to a third party in the following cases:

1) if the subject's consent in writing, including in the form of an electronic document, is available;

2) if the decision is being made for the performance of a contract between the owner and the subject or for the fulfilment of the terms of a previously concluded contract;

3) in cases provided for by legislation.

The obligations of the owner and (or) operator, as well as of a third party, concerning the protection of personal data shall arise from the moment of collection of personal data and shall remain in effect until the moment they are destroyed or depersonalized.

The owner and (or) operator shall designate a structural unit or an official responsible for work related to the processing and protection of personal data and shall ensure its activities in accordance with the Model Procedure for the Processing of Personal Data.

2.4-§. Procedures for Processing Personal Data on the Unified Interactive Public Services Portal

The Unified Interactive Public Services Portal is an information system operating on the basis of the "Electronic Government" system, whose information, methodological and technical support and administration are carried out by the Unified Integrator for the Creation and Support of State Information Systems – "UZINFOCOM" LLC, and which serves as a single point of access to electronic public services provided by state bodies. Electronic public services available on the UIPSP may also be implemented by placing a relevant link (hyperlink) on the official websites of state bodies, as well as in the mobile applications of mobile communication operators, commercial banks and payment system operators, subject to compliance with information security requirements, and in this process, the exchange of personal data is also carried out through the portal.

The activities of this portal are carried out in accordance with the Regulation "On the Unified Interactive Public Services Portal of the Republic of Uzbekistan", approved by Resolution № 728 of the Cabinet of Ministers dated September 15, 2017. The UIPSP was accepted and launched on October 11, 2016, pursuant to Acceptance Certificate № EZ-18-8/5637[16]. The Portal has been gradually improved and developed in stages over the period of its operation. Access to the Portal is available through the my.gov.uz link via the Unified Identification System (ONE-ID) or its alternative versions, MOBILE-ID (MyID).

A Unified Registry has been established within this system, through which 363 electronic public services are currently provided[17]. More than 16.1 million users are currently registered on the Portal, a total of 891 electronic public services and services are provided, the satisfaction level of users of the Portal is 86.1 percent, and it takes only an average of 3 minutes and 35 seconds to use the services and facilities on the Portal[18]. Foreign citizens have also been provided with the opportunity to use the Portal; currently, more than 900 services have been launched for them, enabling them to submit applications for all services in 24/7 mode within an average of 5 minutes[19]. Furthermore, the Portal also provides opportunities to access a list of state organizations, free Wi-Fi zones, submit reports concerning corruption, and use emergency services [20]. Moreover, the Portal provides an opportunity to make payments for the relevant services and facilities in real time, and the Portal also has a mobile application. The Portal also provides an opportunity to pay taxes and other mandatory payments and fines, as well as to obtain information on outstanding debts[21].

[16] https://reestr.uz/kr/projects/1376?type=passport.
[17] https://my.gov.uz/uz/reyestr?limit=30&service_type=electronic.
[18] https://my.gov.uz/uz/statistics.
[19] https://my.gov.uz/uz/for-foreigners.
[20] https://my.gov.uz/uz.
[21] https://my.gov.uz/uz/page/mission.

The following shall constitute the objectives of the Unified Portal:

1) ensuring the high-quality and uninterrupted operation of information systems that provide applicants with electronic public services by state bodies;

2) ensuring the efficiency, promptness and transparency of the activities of state bodies, strengthening their responsibility and executive discipline by creating additional mechanisms for ensuring information exchange with the population and business entities.

The Unified Portal shall perform the following tasks:

1) ensuring guaranteed and secure access for applicants to electronic public services;

2) sending requests and other documents for obtaining electronic public services and receiving the results of the provision of electronic public services;

3) creating the possibility for state bodies to receive and consider requests concerning the use of electronic public services and send the results thereof to applicants;

4) implementing online payment opportunities using payment systems;

5) monitoring the status and progress of the provision of electronic public services;

6) generating, storing and verifying the authenticity of electronic documents;

7) generating statistical data based on received requests and electronic public services provided.

Electronic public services on the Unified Portal shall be introduced by the Ministry of Digital Technologies of the Republic of Uzbekistan (hereinafter referred to as the Ministry) based on an analysis conducted in accordance with the criteria for assessing the demand for public services.

Electronic public services must be convenient for use and meet the needs and interests of applicants.

The main language of the Unified Portal shall be the state language; versions in the Karakalpak, Russian, English and other languages may also be available.

Electronic public services may be provided in the form of information and interactive public services.

An electronic public service aimed at satisfying the information needs of applicants, provided through the publication and other dissemination of information concerning the activities of a state body, shall be considered an information public service.

An electronic public service provided to an applicant through bilateral electronic interaction between that person and the state body providing electronic public services shall be considered an interactive public service.

An interactive public service may be implemented in the form of an automated public service, the provision of which shall be carried out exclusively using information systems and databases of the “Electronic Government” system, including departmental information resources and databases.

The information provided in the process of providing electronic public services must be up-to-date and reliable and must be protected against unauthorized access, leakage, destruction, distortion and blocking.

The use of information generated on the Unified Portal in the provision of an electronic public service to persons who are not participants in the processes of providing or using the electronic public service shall be prohibited without the consent of the Ministry.

Electronic public services shall be provided on a paid or free-of-charge basis.

The procedure and methods for applicants to make payments for the use of paid electronic public services shall be established by the Regulation.

State bodies may establish a different amount of payment for the provision of electronic public services in cases provided for by the Regulation, including where the periods and procedures for the provision of electronic public services are shortened.

According to the level of authentication of applicants, electronic public services shall be divided into the following:

low – services that do not require the provision of personal data;

medium – services that require the provision of authentic personal data;

high – services for which requests for their provision are sent using an electronic digital signature.

State bodies shall determine, in coordination with the Ministry, the level of authentication of applicants necessary for the provision of electronic public services.

The procedure for providing an electronic public service and the requirements imposed on it shall be established by the Regulation.

The Regulation shall be developed by the state body providing the result of the public service in coordination with the Ministry, and such coordination shall constitute the basis for registration in the Unified Register of Electronic Public Services.

Regulations for the provision of electronic public services shall be approved by the Cabinet of Ministers of the Republic of Uzbekistan or, based on the requirements of the legislation on administrative procedures, by an internal regulatory legal act of the authorized body.

The Regulation shall contain the following:

the name of the public service;

a description of the following procedures for its provision:

a) regarding the procedure for receiving a request from the applicant:

the category of persons to whom the electronic public service is provided;

the method of submitting the request;

the information specified in the request (the list of information in the application, the application form);

the required level of authentication of the applicant when the request is submitted electronically;

the list and samples of documents submitted for the provision of the electronic public service;

b) regarding the procedures for considering and processing the request:

the list and composition of information obtained through interagency electronic interaction within the framework of the provision of the electronic public service, as well as the list of state bodies providing (receiving) such information;

the periods and method for considering (processing) the request, and if an information system is used – its name and registration number in the Register of State Information Resources and Information Systems of State Bodies;

the periods for considering (processing) the request;

the cost of the service and the method of payment (if the service is paid);

c) regarding the procedures for storing the result and sending the response:

the method and type of storage of the result of the provision of the public service;

the form of submission of the result of the provision of the public service;

the grounds for refusal to provide the public service.

When introducing an electronic public service, along with the Regulation, it is also required to have a technical document on the introduction of electronic public services on the Unified Portal (hereinafter referred to as the Technical Document).

The Technical Document shall be developed by the state body and, after coordination with the "Digital Government Projects Management Center" SE and the Unified Integrator, shall be approved by the Ministry.

The Technical Document shall contain the graphical and textual information required for the creation and design of the electronic public service to be introduced on the Unified Portal, including:

the category of persons to whom the electronic public service is provided;

a description of the procedure and stages for the provision of the electronic public service;

technical specifications of the electronic public service;

a graphical representation of the procedure for providing the electronic public service, indicating the period for its provision and the state bodies responsible for it;

the cost of providing the public service and methods of payment (if the service is paid);

the rights and obligations of the parties when receiving the request from the applicant, considering the request, storing the result and sending the response;

the procedure for interagency electronic interaction between the Unified Portal and the relevant information systems of state bodies and mobile communication operators, commercial banks and payment system operators.

The Technical Document may also contain other types of information required for the technical implementation of the electronic public service.

Electronic public services on the Unified Portal shall be provided through:

the applicant's personal account;

the state body's personal account.

Access to the personal account on the Unified Portal shall be carried out through the Unified Identification System in accordance with the procedure established by legislation.

Requests for obtaining electronic public services shall be sent through the applicant's personal account.

The applicant's personal account provides the ability to use the electronic public service, monitor the status of the provision of the electronic public service, store and process personal data, and assess the quality of the provision of the electronic public service.

The applicant's personal account enables users to be informed about the electronic public services to be provided to them on the basis of information contained in the information systems and databases of the "Electronic Government" system, including departmental information resources and databases.

Requests for the provision of electronic public services shall be received and responses thereto shall be sent through the state body's personal account.

In this case, state bodies providing electronic public services shall independently obtain, through interagency electronic interaction, the necessary documents and information available from other authorized bodies for the provision of the service.

The consideration and processing of a request for the provision of an electronic public service and the storage of the result of its provision shall be carried out using interagency and departmental information systems, including information resources and databases.

The state body's personal account is intended for processing received requests by an authorized official of the state body through the ability to prepare, edit, search for and submit the documents and information necessary for the provision of the electronic public service.

The right to use the state body's account shall be granted to an authorized official by the Ministry on the basis of an official request from the head of the respective state body.

The official request of the state body must contain the following information about the authorized officials of the state body providing electronic public services who are registered in the Unified Identification System:

a) surname, first name and patronymic of the authorized official;

b) position held;

c) information provided to the user for identification in the Unified Identification System.

The information systems used by state bodies in the process of providing electronic public services must be integrated with the infrastructure of electronic government and comply with the requirements established by legislation.

The results of the provision of electronic public services in the form of electronic documents generated on the Unified Portal and in the mobile applications of mobile communication operators, commercial banks and payment system operators through the Unified Portal shall be equated by state bodies, when providing public services, with documents issued on paper.

The applicant shall have the right to choose the form in which to receive a response concerning the result of consideration of their request for the provision of public services.

If the applicant has indicated in the request that the response should be sent on paper, the result of the provision of the public service shall, at the request of an individual, be sent to the postal address at which the individual is registered at their place of residence or place of stay, and, in the case of a legal entity, to its location corresponding to its postal address.

The results of the provision of electronic public services shall be stored in the electronic document repository on the basis of information received from state bodies in the form of electronic documents.

The applicant shall have the opportunity to obtain a paper copy of an electronic document generated on the Unified Portal through the applicant's personal account.

Paper copies of electronic documents are intended for submission by applicants when making a traditional request to obtain public services (in person, by post or by facsimile communication).

State bodies shall have the opportunity to verify the authenticity of paper copies of electronic documents received from applicants and obtain information thereon by entering a unique identification number through the official website of the Electronic Document Repository or by scanning the QR code contained in the electronic document generated on the Unified Portal and in the mobile applications of mobile communication operators, commercial banks and payment system operators through the Unified Portal.

State bodies shall ensure the authenticity and relevance of the information provided through departmental information systems and databases.

The Ministry shall take measures to prevent distortion of information contained in electronic documents generated on the Unified Portal and shall ensure the conformity of information in electronic form obtained from departmental information systems.

The information contained in electronic documents shall be deemed legally valid. State bodies are strictly prohibited from refusing to accept copies of electronic documents generated on the Unified Portal and in the mobile applications of mobile communication operators, commercial banks and payment system operators through the Unified Portal.

The satisfaction level of the population and business entities with the electronic public services and facilities of state bodies on the Unified Portal shall be assessed.

The satisfaction level of the population and business entities with the electronic public services and facilities of state bodies on the Unified Portal shall be assessed in accordance with the following key indicators:

public assessment of the quality of electronic services;

timely provision of electronic public services;

availability of access to public services;

level of satisfaction with public services and facilities.

In accordance with the results of the rating assessment, the satisfaction level of the population and business entities with the electronic public services and

facilities of state bodies on the Unified Portal shall be determined by rating score as follows:

from 71 to 100 points – “excellent”;

from 55 to 71 points – “satisfactory”;

below 55 points – “unsatisfactory”.

The scores accumulated during the assessment shall be calculated taking into account the operation, quality of provision and effectiveness of electronic public services and facilities on the Unified Portal.

The rating of the satisfaction level of the population and business entities with the electronic public services and facilities of state bodies on the Unified Portal shall be generated automatically, without human intervention, by state bodies in a special module of the Digital Control Information System of the Inspection for Control in the Sphere of Informatization and Telecommunications (hereinafter referred to as Uzkomnazorat), no later than the 25th day of the month following each half-year.

The rating of the satisfaction level of the population and business entities with the electronic public services and facilities of state bodies on the Unified Portal shall be publicly announced by Uzkomnazorat through its official website and mass media based on the results of each half-year.

Uzkomnazorat shall:

monitor compliance with the technically established procedures in the process of effectively providing electronic public services;

regularly publish the rating of the satisfaction level of the population and business entities with the services and facilities on the Unified Interactive Public Services Portal, generated every half-year without human intervention.

Heads of state bodies shall be personally responsible for the timely and high-quality formation of databases, digitization of data, timely provision of data and documents in digital form, preventing unjustified refusal to provide electronic services and preventing their poor-quality provision.

In this regard, heads of state bodies shall:

continuously carry out work on digitizing the information necessary for the population, business entities and state bodies;

form digital databases and their backup copies;

continuously provide information contained in digital databases to the Interagency Integration Platform;

establish a system for notifying the Digital Government Projects Management Center at least 3 days in advance about preventive measures in information systems.

Applicants shall be held liable in accordance with the procedure established by legislation for providing inaccurate information and submitting requests containing slander and insults for the provision of electronic public services.

CHAPTER III. LEGAL GUARANTEES AND LAW ENFORCEMENT MECHANISMS FOR ENSURING THE SECURITY OF PERSONAL DATA

3.1-§. Protection and Ensuring the Security of Personal Data

The state guarantees the protection of personal data. In this regard, a threat to the security of personal data shall mean a set of conditions and factors creating the possibility of destruction, alteration, blocking, copying, unauthorized provision to third parties, unauthorized dissemination and other unlawful actions as a result of unauthorized access to personal data, including accidental access, in the process of processing personal data.

The owner and (or) operator, as well as a third party, shall take legal, organizational and technical measures ensuring the following for the protection of personal data:

the exercise of the subject's right to protection against interference with their private life;

the integrity and preservation of personal data;

compliance with the confidentiality of personal data;

prevention of unlawful processing of personal data.

For the purpose of ensuring the protection of personal data, the owner and (or) operator shall:

1) classify personal data into publicly accessible and non-publicly accessible data;

2) establish the procedure for processing and using personal data;

3) determine the persons having the right to process personal data or access personal data;

4) ensure the installation of information security tools and the updating of the software of technical means processing non-publicly accessible personal data;

5) maintain an event log of database management systems;

6) ensure the recording of actions of users having the right to access non-publicly accessible personal data;

7) apply means for monitoring the integrity of non-publicly accessible personal data;

8) in the presence of the subject's consent, transfer non-publicly accessible personal data to other persons through secure communication channels and (or) encryption means, except in cases provided for by legislative acts;

9) ensure the use of cryptographic information protection means for the secure storage of non-publicly accessible personal data;

10) use means of identification and (or) authentication of users when working with non-publicly accessible personal data;

11) if the owner and (or) operator is a legal entity, appoint an authorized person organizing the processing of personal data or establish a structural unit;

12) approve internal documents defining the policy of the owner and (or) operator concerning the processing and protection of personal data;

13) establish the procedure for blocking and destroying personal data based on an application from the personal data subject.

The organization and implementation of information security in the process of processing personal data shall be carried out on the basis of state standards of the Republic of Uzbekistan in the field of information security.

Owners and (or) operators shall determine the required level of protection of personal data when processing personal data in databases.

The determination of the required level of protection of personal data when processing personal data in databases shall be carried out in accordance with the procedure established by the Regulation on Determining the Level of Protection of Personal Data in the Processing of Personal Data, approved by Resolution No. 570 of the Cabinet of Ministers of the Republic of Uzbekistan dated October 5, 2022.

Owners and (or) operators shall implement organizational and technical measures to protect personal data based on threats to the security of such data when processing personal data.

Ensuring the security of personal data shall be carried out by owners and (or) operators or persons designated by them as responsible.

Personal data processed in databases shall consist of special, biometric, genetic and publicly accessible data in accordance with Articles 25, 26 and 29 of the Law of the Republic of Uzbekistan “On Personal Data”.

Only the personal data of employees of owners and (or) operators shall be processed in the databases of employees of owners and (or) operators.

The processing of personal data of subjects who are not employees of the owner and (or) operator shall be carried out in a separate database.

Threats to the security of personal data shall mean a set of conditions and factors that may result in the alteration, addition, use, provision, dissemination, transfer, depersonalization, destruction, copying of personal data, as well as other unlawful actions, as a result of unauthorized access, including accidental access, to the database.

Threats associated with the presence of undeclared (unannounced) capabilities in the system software of a personal data database shall be considered Type 1 threats.

Threats associated with the presence of undeclared (unannounced) capabilities in the application software of a personal data database shall be considered Type 2 threats.

Threats not associated with the presence of undeclared (unannounced) capabilities in the system and application software of a personal data database shall be considered Type 3 threats.

The type of threats to the security of personal data relating to a database shall be determined by the owner and (or) operator in accordance with this document.

There are 4 levels of protection of personal data when processing personal data in databases.

For Level 1 protection of personal data to be established when processing personal data in databases, at least one of the following conditions shall exist:

when Type 1 threats exist for databases and special and (or) biometric and (or) genetic data are processed in databases;

when Type 2 threats exist for databases and special data of more than 50,000 subjects who are not employees of the owner and (or) operator are processed.

For Level 2 protection of personal data to be established when processing personal data in databases, at least one of the following conditions shall exist:

when Type 1 threats exist for databases and publicly accessible data are processed in databases;

when Type 2 threats exist for databases and special data of employees of the owner and (or) operator or special data of fewer than 50,000 subjects who are not employees of the owner and (or) operator are processed;

when Type 2 threats exist for databases and biometric and (or) genetic data are processed in databases;

when Type 2 threats exist for databases and publicly accessible data of more than 50,000 subjects who are not employees of the owner and (or) operator are processed;

when Type 3 threats exist for databases and special data of more than 50,000 subjects who are not employees of the owner and (or) operator are processed.

For Level 3 protection of personal data to be established when processing personal data in databases, at least one of the following conditions shall exist:

when Type 2 threats exist for databases and publicly accessible data of employees of the owner and (or) operator or publicly accessible data of fewer than 50,000 subjects who are not employees of the owner and (or) operator are processed;

when Type 3 threats exist for databases and special data of employees of the owner and (or) operator or special data of fewer than 50,000 subjects who are not employees of the owner and (or) operator are processed;

when Type 3 threats exist for databases and biometric and (or) genetic data are processed.

For Level 4 protection of personal data to be established when processing personal data in databases, the following condition shall exist:

when Type 3 threats exist for databases and publicly accessible data are processed in the database.

To ensure Level 4 protection of personal data when processing personal data in databases, the following requirements shall be fulfilled:

organizing a security regime for the premises where databases are located, preventing uncontrolled entry or stay in such premises by persons who do not have the right of access to them;

ensuring the security of material objects containing personal data;

approval by the head of the owner and (or) operator of a document determining the list of persons who require access to personal data processed in databases for the performance of their official (employment) duties;

protecting personal data against existing threats, using, where necessary, information security means that have undergone the procedure for assessing their compliance with the requirements of legislation in the field of information security.

To ensure Level 3 protection of personal data when processing personal data in databases:

the requirements established for ensuring Level 4 protection of personal data when processing personal data in databases shall be fulfilled;

an official (employee) responsible for ensuring the security of personal data in the database shall be appointed.

To ensure Level 2 protection of personal data when processing personal data in databases:

the requirements established for ensuring Level 3 protection of personal data when processing personal data in databases shall be fulfilled;

access to the information in the electronic message log of the database shall be granted only to employees or authorized persons who require access to such log for the performance of their official (employment) duties.

To ensure Level 1 protection of personal data when processing personal data in databases:

the requirements established for ensuring Level 2 protection of personal data when processing personal data in databases shall be fulfilled;

changes in the authority of an employee of the owner and (or) operator to access personal data in databases shall be automatically recorded in the electronic security log;

a structural unit responsible for ensuring the security of personal data in databases shall be established, or the functions of ensuring such security shall be assigned to one of the structural units.

It is known that, pursuant to legislation, personal data of citizens of the Republic of Uzbekistan shall be stored while ensuring the basic principles of the Law of the Republic of Uzbekistan “On Personal Data”.

The following personal data shall be stored within the territory of the Republic of Uzbekistan:

biometric data of individuals;

genetic data of individuals;

data of individuals using the services of telecommunications operators operating within the territory of the Republic of Uzbekistan.

Personal data not covered by part two of this Article may be stored and processed outside the territory of the Republic of Uzbekistan if one of the following conditions is fulfilled:

recognition of a foreign state as a state ensuring an equivalent level of protection of personal data;

adoption and compliance by the operator with standard contractual clauses or binding corporate rules that meet the requirements approved by the authorized state body;

compliance by the operator with international standards in the field of management and storage of personal data, the list of which shall be approved by the authorized state body.

The list of foreign states ensuring an equivalent level of protection of personal data has been approved by Resolution No. 415 of the Cabinet of Ministers dated July

29, 2026, pursuant to which the Department of Migration and Personalization under the Ministry of Internal Affairs (hereinafter referred to as the authorized state body) has been designated as responsible for preparing proposals on the inclusion of foreign states in or their removal from the List, and the following has been established:

personal data and depersonalized data shall be automatically transferred across borders to states included in the List through information systems established on the basis of international agreements, without additional permits and without notifying the authorized state body, provided that measures are taken to prevent data leakage;

any transfer of personal data in any form to foreign states not included in the List shall be permitted by the operator and the owner of the personal data database provided that the legal, organizational and technical conditions established by the authorized state body are fulfilled;

if a data leakage incident is identified during the cross-border transfer of personal data, the operator of the personal data database shall notify the authorized state body thereof within 24 hours from the time such incident is identified and shall provide detailed information within 72 hours on the causes of the data leakage and the measures taken to eliminate them[22].

It is known that the confidentiality of personal data means the mandatory requirement to be complied with by the owner and (or) operator or another person who has obtained permission to access personal data, concerning the inadmissibility of disclosure and dissemination of personal data without the subject's consent or in the absence of another lawful basis.

The owner and (or) operator, as well as other persons who have obtained permission to access personal data, shall not disclose or disseminate personal data to third parties without the subject's consent.

Personal data that may be freely accessed with the subject's consent or to which the requirements concerning confidentiality do not apply shall constitute publicly accessible personal data.

For the purpose of providing information to the population, publicly accessible sources of personal data may be created (including biographical reference books, telephone and address directories, publicly accessible electronic information resources).

The following may be included in publicly accessible sources of personal data with the subject's written consent: their surname, first name, patronymic, year and place of birth, address, subscriber number, information about their profession, as well as other personal data disclosed by the subject.

Information about the subject may be removed from publicly accessible sources of personal data upon their request, in the same form in which the consent was given or in writing, including in the form of an electronic document, as well as pursuant to a decision of the authorized state body or a court.

[22] Resolution № 415 of the Cabinet of Ministers dated July 29, 2026 "On Approval of the List of Foreign Countries Ensuring an Equivalent Level of Protection of Personal Data" // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

In ensuring the confidentiality of personal data, material objects containing biometric and genetic data, as well as technologies for storing such data outside personal data databases, are of exceptional importance. Biometric data shall mean personal data describing the anatomical and physiological characteristics of the subject; genetic data shall mean personal data relating to the inherited or acquired characteristics of the subject, which are the result of an analysis of the biological profile of the subject or of another element that makes it possible to obtain alternative information; and material objects storing data in electronic form shall mean flexible magnetic disks, optical disks, hard (non-removable) magnetic disks, electronic memory disks (flash), electronic means of authentication (tokens, tablets and others).

Any material objects used for the purpose of processing biometric and genetic data shall be marked with the designation “confidential” or “for official use” in accordance with the procedure established by legislation. When biometric and genetic data are stored in electronic form, such data must be encrypted and protected by cryptographic or other methods. The owner and (or) operator shall ensure the accounting of material objects on which biometric and genetic data are stored during the processing of such data. The owner and (or) operator shall take appropriate security measures to prevent the theft, deletion, destruction, unauthorized acquisition, alteration and uncontrolled leaving of material objects on which biometric and genetic data are recorded.

When taking security measures, biometric and genetic data shall:

1) comply with fire safety requirements, sanitary rules, norms and hygiene standards, and shall also be guaranteed against flooding;

2) have reliable means of protection excluding the possibility of access by unauthorized persons;

3) be stored in safes, metal cabinets or metal racks;

4) be stored in premises whose entrance doors and windows are equipped with security alarm systems connected to a security service and video surveillance devices.

When personal data are deleted from material objects on which biometric and genetic data are recorded, such material objects shall not be removed from the register.

Material objects that have not been removed from the register may subsequently be reused for the purpose of processing personal data, except for material objects intended for single use and rendered unfit for use. Such material objects shall be destroyed in accordance with the established procedure.

A material object shall be used within the period established by the owner and (or) operator who recorded biometric and genetic data on it, but not exceeding the period of operation established by the manufacturer.

Copying biometric and genetic data shall be carried out on technical devices authorized for the processing of such data and with the direct participation of responsible employees of the owner and (or) operator.

If, together with biometric and genetic data, a material object also contains additional personal data related to them, such data must be certified with an enhanced qualified electronic signature and (or) protected by other information

technologies that make it possible to preserve the integrity and immutability of the data recorded on the material object.

Identification information about the device used in the process of processing biometric and genetic data in the database (IP address, MAC address and other identifiers) shall be recorded.

The type of material object used for processing biometric and genetic data shall be determined by the owner and (or) operator.

When biometric and genetic data are stored outside personal data databases, the following technological and other requirements shall be ensured:

1) access for authorized persons of the owner and (or) operator to the personal data stored on the material object;

2) the use of electronic signature means or other information technologies that make it possible to preserve the integrity and immutability of biometric and genetic data recorded on the material object;

3) verification of the existence of the subject's written consent to the processing of their biometric and genetic data or other grounds specified in legislative acts for the processing of biometric and genetic data.

When biometric and genetic data are removed from a personal data database for separate storage, the grounds for their unauthorized and repeated recording shall be required to be registered.

The owner and (or) operator shall have the right, based on the methods of protecting biometric and genetic data in their databases, to establish additional requirements for technologies for storing such data outside personal data databases that do not contradict legislative acts[23].

[23] Regulation "On the Requirements for Material Carriers Containing Biometric and Genetic Data and Technologies for Storing Such Data Outside Personal Data Databases", approved by Resolution № 570 of the Cabinet of Ministers dated October 5, 2022 // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

3.2-§. Liability for Violation of Legislation on Personal Data

Persons guilty of violating legislation on personal data shall be held liable in accordance with the established procedure.

Such liability may take the following forms:

disciplinary;

administrative;

criminal;

civil.

Pursuant to the Labor Code of the Republic of Uzbekistan, information concerning facts, events and circumstances in the life of an employee, as well as their family members, provided to the employer in connection with employment relations shall constitute the employee's personal data.

The following information concerning an employee shall constitute personal data:

surname, first name, patronymic, date and place of birth;

personal identification number of an individual (if available);

education (when and which educational organizations they graduated from, diploma numbers, field of training or specialty according to the diploma, qualification);

work performed since the commencement of employment (including military service);

address at the place of permanent or temporary residence registration;

passport details (series, number, by whom and when issued) and identification ID-card details;

personal telephone number, e-mail address;

attitude toward military duty, military registration information (for citizens in the reserve and persons subject to conscription for military service);

taxpayer identification number;

number of the individual accumulative pension account;

results of mandatory medical examinations;

grounds for termination of the employment contract with the employee;

marital status, surnames, first names, patronymics and dates of birth of close relatives;

other information concerning facts, events and circumstances in the life of the employee and (or) their family members that became known to the employer.

Information concerning the employee's personal data shall constitute confidential information.

When processing personal data (when performing a single action or a set of actions involving the collection, systematization, storage, alteration, supplementation, use, provision, dissemination, transfer, depersonalization and destruction of personal data), the employer and its representatives shall:

comply with the provisions of legislation on personal data when determining the scope and content of the employee's personal data being processed;

obtain all personal data of the employee directly from the employee. If the employee's personal data may be obtained only from third parties, the employee shall be notified thereof in advance in writing and their written consent shall be obtained, except in cases where personal data (results of medical examinations, conclusions based on qualification and other assessments within the framework of professional development, and others) are obtained from the third parties to whom such data were sent by the employee's employer in accordance with legislation;

notify the employee of the purposes of obtaining personal data, the presumed sources and methods of obtaining them, as well as the nature of the personal data to be obtained and the consequences of the employee's refusal to provide written consent to their obtaining;

ensure the protection of the employee's personal data against unlawful use or loss at the expense of the employer's own funds;

familiarize employees and their representatives, against signature, with the documents available at the employer that establish the procedure for processing employees' personal data, as well as their rights and obligations in this area;

develop, together with employees' representatives, measures to protect employees' personal data.

Unless otherwise provided by this Code and other laws, the employer and its representatives shall not have the right to obtain or process personal data concerning the employee's membership in public associations or activities in a trade union.

The use of the employee's personal data by representatives of the employer shall be carried out only in accordance with the employee's employment duties.

Representatives of the employer carrying out the processing of employees' personal data shall not disclose personal data entrusted to them or which became known to them in connection with the performance of their employment duties.

The terms of an employment contract, other agreements between the employee and the employer, or provisions of internal documents that provide for the employee's refusal to have their personal data protected or worsen the employee's position in the field of protection of their personal data in comparison with legislation shall be invalid.

The procedure for storing, using and providing employees' personal data shall be established by the employer in compliance with the requirements of this Code and other laws.

When providing the employee's personal data, the employer shall comply with the following requirements:

not disclose the employee's personal data to a third party without their written consent, except where such disclosure is necessary for the purpose of preventing a threat to the life and health of the employee, as well as in other cases provided for by this Code and other laws;

not disclose the employee's personal data for commercial purposes without their written consent;

warn persons receiving the employee's personal data that such data may be used only for the purposes for which they were disclosed and require confirmation from such persons that this rule has been complied with. Persons receiving the

employee's personal data shall comply with the confidentiality regime. This rule shall not apply to the exchange of employees' personal data in accordance with the procedure established by this Code and other laws;

provide the employee's personal data within a single organization or by a single individual entrepreneur in accordance with an internal document with which the employee must be familiarized against signature;

allow access to employees' personal data only to specially authorized persons, provided that such persons shall have the right to obtain only the personal data of the employee necessary for the performance of specific employment duties;

not request information concerning the employee's state of health, except for information relating to the issue of the employee's ability to perform their employment duties;

provide the employee's personal data to employees' representatives in accordance with the procedure established by this Code and other laws and limit such information only to the personal data necessary for the performance of their duties by the specified representatives.

For the purpose of ensuring the protection of the personal data stored by the employer, the employee shall have the following rights:

to receive complete information about their personal data and the processing of such data;

to have free access to their personal data, including the right to receive copies of any record containing the employee's personal data, except in cases provided for by law;

to designate a representative for the protection of their personal data;

to have access to medical documents reflecting the state of their health;

to require the removal or correction of inaccurate personal data, or the supplementation of incomplete data, as well as data processed in violation of the requirements of this Code or other laws;

to require the employer to notify all persons to whom the employee's inaccurate or incomplete personal data had previously been disclosed of all exclusions, corrections or supplements made to such data;

to appeal against all unlawful decisions, actions (inaction) of the employer in the processing and protection of their personal data, including to appeal to a court.

If the employer refuses to remove, correct or supplement the employee's personal data, the employee shall have the right to notify the employer in writing of their disagreement with the relevant grounds.

If the violation by the employer of the procedure for processing and protecting the employee's personal data results in the employee being unlawfully deprived of the opportunity to work or leads to a reduction in the amount of remuneration for the employee's work, the obligation to compensate for the employee's lost wages shall be imposed on the employer through whose fault the violation was committed.

If the employer disseminates information that tarnishes the reputation of the employee and does not correspond to reality, the employer shall be obliged to refute such information.

If, as a result of the violation of these very provisions, the employer is an employee of another higher-level organization, such employee shall be held liable for violating the applicable legislative acts and internal labor regulations. At the same time, employees of human resources management and development units of organizations may also be subject to disciplinary liability if they fail to comply with the procedures for processing employees' personal data or if, as a result of violating the procedure for working with information systems provided to them, the requirements of legislation on personal data are violated, provided that there are no signs of a crime or administrative offense in the actions of such employees.

According to legislation, the use of mass media for the purpose of disclosing other secrets protected by law or committing other acts entailing criminal or other liability in accordance with the law shall not be permitted [24].

The owner of a website and (or) a webpage of a website or another information resource, including a blogger, shall not allow their website and (or) webpage or other information resource on the Internet global information network, where information freely accessible to everyone is posted, to be used for the disclosure of information constituting another secret protected by law, the unlawful processing of personal data using artificial intelligence technologies, the dissemination thereof through mass media, telecommunications networks or the Internet global information network, the dissemination of information aimed at encouraging or otherwise involving citizens, including minors, in committing unlawful acts that threaten their life and (or) health or the life and (or) health of other persons, or for the purpose of committing other acts entailing criminal or other liability in accordance with the law[25].

As a result of the violation of these requirements and the norms established by legislation on personal data, administrative or criminal liability may arise, in particular:

Pursuant to Article 46^2 of the Code of the Republic of Uzbekistan on Administrative Liability, the unlawful collection, systematization, storage, modification, supplementation, use, provision, dissemination, transfer, depersonalization and destruction of personal data, as well as failure to comply with the requirements concerning the collection, systematization and storage of personal data on technical devices physically located within the territory of the Republic of Uzbekistan and in personal data databases registered in accordance with the established procedure in the State Register of Personal Data Databases when processing personal data of citizens of the Republic of Uzbekistan using information technologies, including on the Internet global information network, –

shall entail the imposition of a fine in the amount of seven times the basic calculated amount on citizens and fifty times the basic calculated amount on officials.

[24] Law № LRU–78 of the Republic of Uzbekistan dated January 15, 2007 "On Amendments and Additions to the Law of the Republic of Uzbekistan 'On Mass Media'" // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

[25] Law № 560-II of the Republic of Uzbekistan "On Informatization" dated December 11, 2003 // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

The unlawful processing of personal data using artificial intelligence technologies, their dissemination through mass media, telecommunications networks or the Internet global information network, –

shall entail the imposition of a fine in the amount of fifty to one hundred times the basic calculated amount, with confiscation of the instruments used to commit the administrative offense.

Pursuant to Article 141² of the Criminal Code of the Republic of Uzbekistan, the unlawful collection, systematization, storage, modification, supplementation, use, provision, dissemination, transfer, depersonalization and destruction of personal data, as well as failure to comply with the requirements concerning the collection, systematization and storage of personal data on technical devices physically located within the territory of the Republic of Uzbekistan and in personal data databases registered in accordance with the established procedure in the State Register of Personal Data Databases when processing personal data of citizens of the Republic of Uzbekistan using information technologies, including on the Internet global information network, if such acts were committed after the imposition of an administrative penalty for the same acts, –

shall be punishable by a fine in the amount of one hundred to one hundred and fifty times the basic calculated amount, or deprivation of a certain right for up to three years, or correctional labor for up to two years.

The same acts:

a) committed by a group of persons upon prior conspiracy;

b) repeatedly or by a dangerous recidivist;

c) for mercenary or other base motives;

d) committed using an official position;

e) resulting in grave consequences, –

shall be punishable by a fine in the amount of one hundred and fifty to two hundred times the basic calculated amount, or correctional labor for a period of two to three years, or restriction of liberty for a period of one to three years, or deprivation of liberty for up to three years.

In this regard, a form of periodic dissemination of mass information having a permanent title and published or broadcast at least once every six months in printed form (newspapers, magazines, newsletters, bulletins and others) and (or) electronic form (television, radio, video and newsreel programs, websites on the Internet global information network), hereinafter referred to as "published", registered in accordance with the procedure established by legislation, as well as other forms of periodic dissemination of mass information, shall constitute mass media[26], **Artificial intelligence** – a set of technological solutions that enables the imitation of human knowledge and skills, including independent learning and the search for solutions, as well as obtaining results comparable to those of human intellectual activity in

[26] Law № LRU–78 of the Republic of Uzbekistan dated January 15, 2007 "On Amendments and Additions to the Law of the Republic of Uzbekistan 'On Mass Media'" // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

performing specific tasks[27], **Telecommunications network** – a set of equipment interconnected through communication lines or communication channels and carrying out telecommunications[28], **Internet global information network** (hereinafter referred to as the **Internet network**) – a global international network consisting of a multitude of networks interconnected by means of gateways, using a single address and name space and operating in accordance with a unified TCP/IP protocol[29] shall be understood as being considered.

Тўлиқ таржима:

1. The main direct object of the cybercrime – the constitutional rights and freedoms of other persons concerning personal data.

2. The additional direct object of the cybercrime – social relations protecting information and communication technologies.

3. The optional direct object of the cybercrime – other person(s), society and the state, including public security, inviolability of property and others;

4. The subject of the cybercrime – a sane individual who has attained the age of 16.

5. The subjective aspect of the cybercrime – intentional.

6. The objective aspect of the cybercrime – is committed by unlawfully collecting, systematizing, storing, modifying, supplementing, using, providing, disseminating, transferring, depersonalizing and destroying personal data using information and communication technologies, including on the Internet global information network, as well as by failing to comply with the requirements concerning the collection, systematization and storage of personal data on technical devices physically located within the territory of the Republic of Uzbekistan and in personal data databases registered in accordance with the established procedure in the State Register of Personal Data Databases when processing personal data of citizens of the Republic of Uzbekistan.

7. The purpose of the cybercrime – mercenary or other base motives, hostility, hooliganism, revenge, material or (and) moral interest.

8. The means (instrument) of the cybercrime – information and communication technologies.

9. The essential elements of the cybercrime:

1) the social dangerousness of the act;
2) the unlawfulness of the act;
3) the presence of guilt in the act;
4) the punishability of the act;
5) an administrative penalty has been imposed for such an act and it is being repeated within one year;
6) communication;

[27] Law № 560-II of the Republic of Uzbekistan "On Informatization" dated December 11, 2003 // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

[28] Law № LRU–1015 of the Republic of Uzbekistan "On Telecommunications" dated December 27, 2024 // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

[29] Rules for the Provision of Telecommunications Services, approved by Order № 287-mh of the Minister of Digital Technologies of the Republic of Uzbekistan dated January 6, 2026 (registered on January 26, 2026, № 3762) // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

7) information;
8) cyberspace, including cyber environment;
9) information and communication technologies.

The absence of any one of these elements excludes the classification of the act as a cybercrime.

10. Completion of the cybercrime –

1) from the moment personal data are unlawfully collected;
2) from the moment personal data are unlawfully systematized;
3) from the moment personal data are unlawfully stored;
4) from the moment personal data are unlawfully modified;
5) from the moment personal data are unlawfully used;
6) from the moment personal data are unlawfully provided;
7) from the moment personal data are unlawfully disseminated;
8) from the moment personal data are unlawfully transferred;
9) from the moment personal data are unlawfully depersonalized;
10) from the moment personal data are unlawfully destroyed;
11) from the moment one of the acts concerning failure to comply with the requirements for the collection, systematization and storage of personal data on technical devices physically located within the territory of the Republic of Uzbekistan and in personal data databases registered in accordance with the established procedure in the State Register of Personal Data Databases, when processing personal data of citizens of the Republic of Uzbekistan using information and communication technologies, including on the Internet global information network, is committed.

11. The type of cybercrime according to its structure – a cybercrime with a formal composition under the first part and paragraphs “a, b, c, d” of the second part, and a cybercrime with a material composition under paragraph “e” of the second part.

12. The type of cybercrime according to its specific characteristics and degree of social dangerousness – a cybercrime that does not pose a great social danger.

13. The type according to the system of punishments – cybercrimes for which the Criminal Code provides for punishment in the form of a fine, deprivation of a certain right, correctional labor, restriction of liberty or deprivation of liberty for the socially dangerous act.

14. The subject matter of the crime – personal data.

15. The most common methods of committing the cybercrime:

1) demonstratively on a telecommunications or Internet network;
2) by posting on a telecommunications or Internet network;
3) as a result of using information and communication technologies as an instrument or means of committing a crime.

These methods may take the following forms, in particular, personal data may be collected, stored, modified, supplemented, depersonalized, destroyed, blocked or processed in other ways in a personal data database. These data, in turn, may be in the form of biographical, biometric, genetic and special data.

Under the current legislation, the procedure for organizing the activities of the structural unit of the owner and (or) operator of a personal data database that ensures the processing and protection of personal data (hereinafter referred to as the unit) or an authorized person thereof[30], the procedure for processing and protecting personal data, the principles, purposes and conditions of processing personal data, the rights and obligations of the owner and (or) operator of a personal data database[31], the procedure for providing public services for registering personal data databases in the State Register of Personal Data Databases, removing them from the register, and making amendments and additions to the register[32], the requirements for ensuring the security of personal data during their processing, determining their levels of protection based on threats to their security and ensuring the respective level of protection, as well as the procedure for storing, using and accounting for biometric and genetic data on material carriers and the requirements imposed on technologies for storing biometric and genetic data outside personal data databases[33], and relations in the field of personal data[34] have been established.

The commission of the act by a group of persons upon prior conspiracy, repeatedly or by a dangerous recidivist, for mercenary or other base motives, using official position, or causing grave consequences shall be considered aggravating circumstances of liability.

The following digital traces may be obtained and analyzed for the detection of this crime:

Server IP & Geo-location: the geographical coordinates of the server where the database is located; if the IP address belongs to a foreign country, this shall constitute evidence of the objective aspect of the offense;

Database Logs (Query History): the history showing who, when and through which request (SQL query) obtained or modified the data;

API Call Logs: traces of software interfaces used to transfer data to third parties (for example, advertising agencies);

Encryption Metadata: unencrypted open files indicating a violation of the requirement for depersonalization (anonymization) of data;

---

[30] The Model Procedure for Organizing the Activities of the Structural Unit or Authorized Person of the Owner and (or) Operator of a Personal Data Database Ensuring the Processing and Protection of Personal Data, approved by Order № 19-mh of the Minister of Justice of the Republic of Uzbekistan dated November 14, 2023 (registered on November 15, 2023, № 3477) // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

[31] The Model Procedure for the Processing of Personal Data, approved by Order № 20-mh of the Minister of Justice of the Republic of Uzbekistan dated November 15, 2023 (registered on November 15, 2023, № 3478) // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

[32] Administrative Regulation for the Provision of Public Services for Maintaining the State Register of Personal Data Databases, approved by Resolution № 71 of the Cabinet of Ministers dated February 8, 2020 // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

[33] Resolution № 570 of the Cabinet of Ministers of the Republic of Uzbekistan dated October 5, 2022 "On Approval of Certain Regulatory Legal Documents in the Field of Processing Personal Data" // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

[34] Law № LRU–547 of the Republic of Uzbekistan "On Personal Data" dated July 2, 2019 // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

User Access Control (ACL) Logs: traces of access to the system by persons who do not have the right to access the data.

In addition, messages on social networks, audio or video files and traces thereof, data traces on the devices of witnesses, victims and other participants, as well as digital traces related to the leakage of information from state information systems and resources may also assist in detecting this crime. Based on the legislation on appeals of individuals and legal entities, the submission of their personal data to the official of the organization against whom a complaint concerning their personal data is being made may also constitute the elements of this offense. Therefore, based on the victim's application, it is necessary to inspect and examine the devices of the suspect, perpetrator or other subject.

In order to uncover and investigate this cybercrime, evidence can be gathered by conducting forensic computer-technical expertises and/or submitting queries to the Personalization Agency to technically verify whether personal data databases are registered in the State Register of Personal Data Databases, whether data is being transmitted to foreign servers, and whether security protocols were adhered to during data destruction or modification processes. Additionally, forensic accounting and financial expertises can determine mercenary profits obtained from selling personal data databases, such as identifying illicit transactions on the DarkNet.

Pursuant to the Regulation "On the Procedure for Exercising State Control Over Compliance with Special Conditions for Processing Personal Data of Citizens of the Republic of Uzbekistan", approved by Cabinet of Ministers Resolution No. 707 of September 5, 2018, there is also full capability to collect essential evidence regarding compliance with statutory requirements by owners and/or operators when processing citizens' personal data using information technologies (including processing over the Internet). This includes verifying that data is collected, systematized, and stored on technical equipment physically located within the territory of the Republic of Uzbekistan and within databases registered in the State Register of Personal Data Databases in accordance with established procedure[35].

To fully expose and investigate this category of cybercrime, the following expertises may also be conducted:

Forensic Computer-Technical Expertise: This constitutes the primary technical tool for establishing the operational mechanics of a cybercrime and determining the geographical location of a database. It investigates server IP addresses, Database Management Systems (DBMS), and network traffic. It determines whether personal data is physically stored on servers located within the territory of Uzbekistan or transmitted to foreign servers (cloud storage); technically verifies non-compliance with statutory requirements for personal data collection,

[35] Regulation "On the Procedure for Exercising State Control Over Compliance with Special Conditions for Processing Personal Data of Citizens of the Republic of Uzbekistan", approved by Cabinet of Ministers Resolution № 707 of September 5, 2018 // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

systematization, and storage; uncovers digital footprints left during illegal de-identification or data destruction processes; and proves instances of unauthorized database access and copying (e.g., administrator logins, timestamp logs) executed through the abuse of official position.

Forensic Examination of Electronic Documents: This expertise verifies the legal and technical registration status of personal data databases. It examines records within the State Register of Personal Data Databases, digital certificates, and electronic data processing agreements. It identifies instances where a database is operated without statutory registration in the State Register or used in violation of registered requirements, providing documentary evidence of administrative procedural non-compliance under the law.

Forensic Philological or Forensic Linguistic Expertise: This discipline analyzes the content and underlying purpose of personal data usage by evaluating textual information extracted from databases as well as user correspondence. It determines through textual analysis whether data was harvested or processed for mercenary or self-serving motives—such as selling information to advertising agencies or blackmailing individuals. Furthermore, it provides a linguistic evaluation establishing that the collected data constitutes personal data capable of directly identifying a specific natural person.

Forensic Phonographic and Forensic Portrait Expertises: In cases where personal data includes biometric data (voice recordings or facial images), these expertises examine biometric features contained in stolen or unlawfully distributed audio and video files. They verify whether an individual's biometric data (voice or facial image) was processed or disseminated without consent, thereby identifying violations associated with the most sensitive category of personal data (biometrics).

Forensic Financial Expertise: This type of expertise is applied to quantify pecuniary gain derived from illicit data trade and establish severe consequences. It examines bank transactions, electronic wallets, and corporate financial statements. It calculates self-serving profits accrued from data sales as well as direct material damages inflicted on victims as a result of data breaches.

 Forensic Examination of Video Materials: Ordered when personal data is collected, stored, or distributed in video format, this expertise identifies biometric data by analyzing facial features and physical movements to confirm their status as biometric personal data. It examines video metadata (creation timestamp, device model, GPS coordinates)—which is critical for determining whether content was generated within Uzbekistan (in line with data localization mandates) or abroad. Additionally, it conducts forensic editing and artificial intelligence (Deepfake) analysis to expose whether a video was manipulated or artificially enhanced using AI tools to alter or illegally fabricate personal data.

CONCLUSION

Based on the data collected from the research findings, the following scientific-practical and fundamental conclusions have been reached:

I. Scientific-theoretical conclusions

1. While personal information defines the confidentiality regime of information, personal data serves as a functional-legal criterion for identifying a specific individual; therefore, it is proposed to consolidate the concept of the "identification status of information" in information law doctrine and legislation as an independent and distinct legal category.

For reference: *In Article 4, Item 1 of the General Data Protection Regulation (EU) 2016/679 (GDPR) of the European Parliament and of the Council, the confidentiality (Confidentiality) and identification status (Identifiability) of information are strictly delineated. According to the doctrine of "Informational Self-Determination" (Informationelle Selbstbestimmung – Information Self-Determination) established by the Federal Constitutional Court of Germany, while confidentiality of information is a tool for limiting the legal regime, identification status is an independent categorical criterion determining the legal-functional connection of information with a specific natural person.*

2. The information protection regime must be tied not to its material carrier (paper, plastic, or digital format), but to the potential of the information to identify a specific individual. Therefore, in national legal doctrine and theory, it is proposed to recognize personal data not as a tangible object, but as an intangible (immaterial) good possessing a special legal regime, and to apply protection standards uniformly regardless of form.

For reference: *In the doctrine of the German Civil Code (Bürgerliches Gesetzbuch – BGB) and the French Civil Code (Code civil), information is classified as "Droits incorporels" (incorporeal rights and non-material goods). In the practice of the French Court of Cassation and the Federal Court of Justice of Germany, it is strictly established that the protection standard applies not to the material carrier of data (paper, plastic, or digital carrier), but to the intangible content of information and its legal potential to identify a person.*

3. The personal status of information does not have a static form; rather, it is a dynamic process in which the probability of identification changes as a result of data interconnection and processing in information and communication systems. On this basis, it is proposed to introduce the theory of a "dynamic continuum" of personal data into scientific circulation and legislation, as well as to develop a mechanism for determining the protection level of information based on the real identification risk index at the source.

For reference*: In accordance with the judicial precedent set by the Court of Justice of the European Union (CJEU) in the case Breyer v Bundesrepublik Deutschland (C-582/14), the doctrine of the "Dynamic Contextual Test" has been formed in digital jurisprudence. According to it, the personal status of information is not a static fact, but a dynamic process arising from its integration with additional data in information and communication systems.*

4. In the cyber environment, an individual can be singled out (segmented) based on their digital traces, behavior, and preferences even without their full name or classical identifiers. In this regard, it is proposed to supplement the theory of indirect identification with the principle of " singularization" and to recognize the very isolation of a person's unique digital profile as the processing of personal data. In a word, apart from the first name, surname, patronymic, or data directly linked to

a person, the very possibility of knowing personal data and identifying said person through digital traces and digital evidence left in the cyber environment constitutes the composition of personal data; even if direct identification of the person is not possible, if there is a possibility to distinguish them from other individuals through a combination of various digital traces, such data must be evaluated as indirectly identifying data.

***For reference**: Recital 26 of Regulation (EU) 2016/679 (GDPR) and Section 1798.140 of the California Consumer Privacy Act (CCPA) in the US advance the principle of "Singling out" (segmentation/isolation), as does the principle of "Sonderung" in German legal doctrine. According to this, even if a person's full name is not disclosed, the mere possibility of distinguishing them from the general public through their digital traces and behavioral profile is evaluated as the processing of indirect personal data.*

5. In information security systems, in addition to the unlawful dissemination or transfer of data, unauthorized access to an information system or database (including by compromising a login and password) constitutes an independent and serious threat. In this regard, it is proposed to recognize "unauthorized access" as an independent element of a violation of the processing and use regimes for personal data.

***For reference:** According to the ISO/IEC 27001 and ISO/IEC 27701 standards of the International Organization for Standardization, the NIST Privacy Framework system of the US National Institute of Standards and Technology, and the principles in Article 5 of Regulation (EU) 2016/679 (GDPR), the concepts of "Data Life Cycle Governance" and "Lifecycle Audit" are applied in information law. Here, legal liability and security standards are defined separately for each stage of the continuous chain from the origin (genesis) of data to its absolute destruction.*

6. The processing of personal data is not a collection of separate, disconnected actions, but a unified and continuous dynamic process from the origin (genesis) of the data to its absolute destruction. Building upon this basis, it is proposed to integrate the concept of the "institutional life cycle" of personal data into information law doctrine and to establish separate security and liability standards for each stage.

***For reference:** According to Article 2 (Illegal Access) of the Council of Europe Convention on Cybercrime of 2001 (Budapest Convention, ETS No. 185) and Title 18, Section 1030 of the United States Code – the Computer Fraud and Abuse Act (CFAA), unauthorized access (unauthorized access / exceeding authorized access) to information systems and databases is considered an independent cyber-delict with a formal legal definition as a violation of information system sovereignty and access regime, regardless of consequences such as data leaks.*

7. In computerized and automated systems, human control over personal data is the primary guarantee of constitutional freedoms and personal privacy. In this regard, it is proposed to scientifically substantiate the concept of "human digital and informational autonomy" in digital jurisprudence and fundamental rights theory, and to include it in the list of inalienable human rights.

***For reference:** Based on the legal practice of the European Court of Human Rights (ECHR) regarding Article 8 of the 1950 Convention for the Protection of Human Rights and Fundamental Freedoms, as well as the landmark decisions of the Federal Constitutional Court of Germany in 1983 and 2008, the concepts of "Digital and Informational Autonomy" and the "Right to guarantee the confidentiality and integrity of information technology systems" are recognized in fundamental rights theory as "fourth-generation" human rights, guaranteeing an individual's right to sovereign control in the digital environment.*

8. Modern artificial intelligence and neural network systems process data not in traditional static databases, but within a cyber environment created through a dynamic algorithmic and software environment. Based on this technological reality, it is proposed to introduce the concept of “cyber environment” into information law doctrine and to precisely regulate in legislation the sources for ensuring data privacy within this environment.

For reference: *Within the framework of Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (EU AI Act) and Regulation (EU) 2022/2065 (Digital Services Act – DSA), the concept of “Algorithmic Environment Governance” is advanced. According to this concept, the dynamic software environment itself within neural networks and AI systems (Cyberspace / Algorithmic Architecture) is considered an independent object of legal regulation and audit.*

9. Face-ID and artificial intelligence-based systems can process biometric or personal data in real-time in random-access memory (RAM) and immediately delete it, without saving it to permanent storage (database). Building upon this basis, it is proposed to create a legal protection theory for information processed in temporary and operational memory, and to apply personal data protection standards to such data.

For reference: *According to the decision of the Court of Justice of the European Union (CJEU) in the SABAM v. Scarlet Extended SA case (C-70/10) and US federal court practice, the theory of “Legal Protection of Volatile Data / Ephemeral Data” applies in cyber-jurisprudence. Under this theory, the processing and deletion of biometric or personal data in random-access memory (RAM) within fractions of a second, without being saved to permanent storage, is also legally recognized as “processing”, and full protection standards are applied to it.*

10. Avatars, Deepfake images, and voice models created by artificial intelligence algorithms based on the physiological features of a real person form the individual's digital persona and digital identity. Therefore, it is proposed to provide a legal definition for the concept of “synthetic biometric data” in doctrine and legislation, and to establish a mechanism prohibiting its unauthorized generation and use.

For reference: *Article 50 of the EU AI Act (mandatory labeling and transparency of generative AI systems and Deepfake content), alongside provisions in US federal and state legislation (such as the NUDITY Act and TAKE IT DOWN Act), defines the legal status of synthetically generated media products. In doctrine, avatars and Deepfake models generated by AI based on a real person's biometric parameters, voice, and physiological characteristics are classified as the individual's Digital Identity. Establishing a mechanism to prohibit the unauthorized generation and use of such synthetic biometric data without consent aims to protect the individual's absolute non-property rights.*

11. A user's web navigation history, search queries, and network logs enable the high-accuracy identification of a specific individual when cross-referenced with various sources. In this regard, it is proposed to classify passive and active digital footprints left by an individual under the category of indirect personal data and to establish a requirement for obtaining consent when collecting them.

For reference: *According to Article 4 and Recital 30 of Regulation (EU) 2016/679 (GDPR), as well as the theory of “Passive and Active Digital Fingerprinting” under Directive 2002/58/EC of the European Parliament and of the Council on privacy and electronic communications (ePrivacy Directive), the combination of a user's web navigation history and*

network logs allows for the identification of an individual. Therefore, a mechanism is established to obtain informed and explicit consent for the collection of such data.

12. Although metadata of information sessions, network protocols, and IP addresses appear anonymous on their own, they fully reveal a person's identity when combined with the databases of telecommunication operators or providers. For this reason, it is proposed to substantiate the theory of metadata as "quasi-personal data" and to subject its use to a special legal regime.

For reference: *According to the "Metadata Profiling" theory established in the decisions of the European Court of Human Rights (ECtHR) in Malone v. the United Kingdom and Big Brother Watch and Others v. the United Kingdom, as well as the CJEU judgment in Tele2 Sverige AB (C-203/15), metadata of information sessions—although seemingly anonymous in isolation fully exposes an individual's private life when integrated with telecom operators' databases, and is therefore subject to an enhanced legal regime.*

13. The concept of data immutability and undeletability in blockchain technology enters into a fundamental conflict with the "Right to be forgotten" in personal data protection. To resolve this conflict, it is proposed to establish a doctrine for protecting rights in decentralized systems through algorithmic anonymization, hashing, and off-chain storage of information.

For reference: *The doctrine of "Decentralized Compliance Architecture" has been formed based on Article 17 (Right to erasure / Right to be forgotten) of Regulation (EU) 2016/679 (GDPR) and the legal opinions of the European Commission within the European Blockchain Partnership (EBP). This doctrine justifies resolving the conflict between blockchain's immutability feature and the right to be forgotten through "Off-chain data storage" (storing data off-network while leaving only hash codes on the blockchain) and Zero-Knowledge Proofs (ZKP) cryptographic algorithms.*

14. In Web3 and InterPlanetary File Systems (IPFS), data is not stored on a single server, which creates complexity in defining the classic concepts of data owner and operator. In this regard, it is proposed to establish the theory of "virtual controllership" and joint liability for decentralized and distributed environments, as well as to introduce relevant legal entity standards into legislation.

For reference: *Based on Article 26 (Joint controllers) of Regulation (EU) 2016/679 (GDPR) and the EU Data Governance Act (EU 2022/868), the theories of "Decentralized Joint Controllership" and "Virtual Data Control" are applied to Web3 and distributed storage systems (IPFS). Under this framework, joint legal personality and liability are assigned to Decentralized Autonomous Organizations (DAOs) and node operators.*

15. Cryptographic addresses and smart contracts make it possible to draw precise conclusions about an individual's financial behavior, wealth, and connections through their transaction history. For this reason, it is proposed to recognize financial and digital identifiers on the blockchain network as a special (financial) category of personal data and to establish a regime for their protection.

For reference: *Pursuant to Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on Markets in Crypto-Assets (MiCA) and the Financial Action Task Force (FATF) "Travel Rule" guidelines, public keys on the blockchain network and smart contract transactions are qualified as "Financial Personal Data" (a special category of financial personal data).*

16. While pseudonymization is a reversible process through additional keys, complete de-identification irreversibly breaks the link between data and the individual. Taking this distinction into account, it is proposed to clearly delineate the legal consequences of the concepts of "temporary pseudonymization" and

“irreversible anonymization” within the scientific framework and legislation, and to establish different protection standards for them.

For reference: *The doctrine of “Irreversible Anonymisation vs. Reversible Pseudonymisation” is established in Article 4(5) of Regulation (EU) 2016/679 (GDPR) and Guidelines 05/2020 of the European Data Protection Board (EDPB). As a reversible process, pseudonymization remains under the regime of personal data, whereas irreversible anonymization strips the data of its personal data status, and distinct protection standards are applied to each.*

17. Modern artificial intelligence and Big Data analytics tools have the potential to re-identify an individual by cross-referencing multiple de-identified open databases. To prevent this threat, it is proposed to introduce the theory of “Algorithmic De-anonymization” for assessing the risk of re-identification and to implement legal provisions prohibiting re-identification.

For reference: *The theory of “Algorithmic Re-identification / Linkage Attack” is advanced within the framework of the National Institute of Standards and Technology (NIST) recommendations of the U.S. Department of Commerce and the principles of Regulation (EU) 2016/679 (GDPR). To counter this, the mathematical model of “Differential Privacy” and legal prohibition mechanisms against re-identifying anonymized databases are applied.*

18. The separate study of legal and technical knowledge in the information society does not allow for a comprehensive assessment of threats in the cyber environment, including cyberspace. In this regard, it is proposed to recognize “Cyberalogy”, an original author-developed concept, as an interdisciplinary conceptual methodology and fundamental doctrine of information and cyber law, and to consolidate it within the research system.

For reference: *Research at the Max Planck Institute for the Study of Crime, Security and Law and the Oxford Internet Institute shows the development of “Cyber-jurisprudence” and “Techno-Legal Interdisciplinary Methodology” at the intersection of information and cyber law. Our proprietary development, “Cyberalogy”, aims to comprehensively study threats in the cyber environment from both a technical-systemic and a legal-doctrinal perspective.*

19. Data leakage from databases is not merely an organizational shortcoming of the data owner, but a systemic security crisis leading to the violation of the data subject's constitutional rights. On this basis, it is proposed to classify a “Data Breach” as an independent legal fact and a hazardous event entailing legal liability, as well as to consolidate the obligation to notify of data breaches.

For reference: *Based on Articles 33 and 34 of Regulation (EU) 2016/679 (GDPR) and Data Breach Notification Laws across all 50 U.S. states, according to the “Data Breach Crisis Governance” theory, a data breach is a distinct legal fact. In international practice, a mandatory breach notification procedure requiring notification to the supervisory authority within 72 hours of a breach is established, alongside independent liability for failure to comply.*

20. Along with the illegal dissemination or transfer of personal data in cyberspace, knowingly downloading (accepting) such data from illegal sources also violates information privacy. Therefore, it is proposed to establish the concept of “unlawful data acceptance” in doctrine and criminal law practice, and to provide it with an appropriate legal assessment.

For reference: *Under Sections 202a (Ausspähen von Daten – Data Espionage) and 202d (Datenhehlerei – Data Fence / Dealing in Stolen Data) of the German Criminal Code (Strafgesetzbuch – StGB), as well as within US cybercrime case law, the concept of “Unlawful Data Acquisition / Illicit Data Receipt” has been established. According to this concept, knowingly*

downloading (accepting) or storing leaked or stolen personal databases from illegal sources is qualified as an independent tort and a distinct criminal offense.

21. If online pseudonyms (nicknames) or handles used on the internet are proven to belong exclusively to a specific individual and serve to identify them in society, they function as personal data. Based on this, it is proposed to clarify the legal status of digital pseudonyms and virtual identities at the intersection of personal data protection and intellectual property law.

For reference: *Under Article 4(1) of the European Union General Data Protection Regulation (EU GDPR 2016/679), "online identifiers", including network pseudonyms, are classified as personal data if they enable the identification of an individual. Furthermore, according to Section 12 of the German Civil Code (Bürgerliches Gesetzbuch – BGB) and the Nom de plume / Pseudonym doctrine developed in French legal practice, pseudonyms are subject to a distinct protection regime operating simultaneously at the intersection of non-property personal rights (as a means of individualization) and intellectual property objects (copyright).*

22. Human DNA, RNA, and fundamental biological data constitute an individual's most sensitive and unalterable digital and biological property. In this regard, it is proposed to theoretically substantiate the concept of "biological information sovereignty" concerning human biological materials and digitized genetic code, and to assign them the highest level of legal protection.

For reference: *In accordance with the principles of UNESCO's Universal Declaration on the Human Genome and Human Rights (1997) and the Council of Europe's Oviedo Convention on Human Rights and Biomedicine (ETS No. 164), the genetic code is considered an integral part of human dignity. According to the concepts of "Biological Information Sovereignty" and "Genetic Privacy" in legal doctrine, the digital format of DNA and RNA sequences (Digital Sequence Information – DSI) is classified as a highly sensitive category that requires absolute inviolability and a supreme level of legal protection.*

23. Human genetic information is not strictly individual; it encompasses shared biological markers that belong to an individual's biological relatives, descendants, and family members. Therefore, it is proposed to scientifically establish the "trans-subjective" (collective or familial) nature of genetic and biological data, and to formulate a legal mechanism that accounts for the interests of relatives when processing genetic data.

For reference: *According to the "Shared Genetic Data / Relational Privacy" theory established in international bio-law and the Geneva doctrine, disclosing a single individual's genetic code inherently reveals the genetic risks of their biological relatives as well. Consequently, judicial practice in the UK and the US (e.g., ABC v St George's Healthcare NHS Trust) has recognized genetic data as possessing a "trans-subjective" (collective or familial) character, driving the adoption of legal mechanisms to protect the informational interests of relatives.*

24. "Consent" obtained by exploiting an individual's psychological vulnerabilities through phishing and social engineering methods does not reflect the genuine will and intent of the person. On this ground, it is proposed to reinforce the legal doctrine of the absolute invalidity (nullity) of information consent obtained under the influence of psychological manipulation, deception, or mistake.

For reference: *Under Article 7 of Regulation (EU) 2016/679 (GDPR) and the European Data Protection Board's (EDPB) Guidelines 03/2022 on "Dark Patterns" and social engineering, the doctrine of "Vitiated Consent" is applied. Consent obtained through psychological manipulation, phishing, or digital misdirection (Dark Patterns) fails to meet the criteria of being "freely given, specific, and informed", and is consequently deemed void ab initio.*

25. Personal data processed in electronic and paper formats holds equal legal force and protection status under UNCITRAL models and international standards (GDPR). Drawing on this international experience, it is proposed to scientifically develop and fully implement the principle of “functional equivalence” of information formats within national legislation and legal practice.

For reference: *Pursuant to the “Functional Equivalence Principle” codified in Article 5 of the UNCITRAL Model Law on Electronic Commerce (1996) and Article 2 of the EU GDPR, whether information exists in physical (paper) or electronic form does not affect its legal validity or level of legal protection.*

26. Due to the employee's economically and organizationally vulnerable position in employment relations, their consent to the processing of personal data may not always be freely given or objective. Consequently, it is proposed to advance the doctrine of “invalidation of forced or subordinate consent” within labor and information law, as well as to establish a prohibition on requesting excessive personal data in employment contracts.

For reference: *Under the “Imbalance of Power” doctrine articulated in the European Data Protection Board's (EDPB) Opinion 2/2017 and the official commentaries on Article 7 of the EU GDPR, consent given within an employment relationship is presumed not to be freely given due to the inherent element of subordination. Accordingly, processing in employment contexts relies on legal obligations or contractual necessity rather than employee consent.*

27. The Personal Identification Number of an Individual (PINFL) and tax records serve as critical integrators that define an individual's financial and civil profile in society. To ensure the security of this data, it is proposed to establish a theoretical basis for an institutional and enhanced protection regime specifically tailored to fiscal and financial personal data.

For reference: *Under the doctrine of “National Identification Numbers Governance”, which operates in the Scandinavian countries (e.g., Sweden and Finland) and Section 38 of the German Federal Data Protection Act (Bundesdatenschutzgesetz – BDSG), national identification numbers and tax profiles are classified as cross-sectoral integrators. Consequently, they are subject to specialized institutional and enhanced protection regimes, including mandatory cryptographic restrictions and rigorous access auditing.*

28. Automated scoring and profiling of an individual by algorithms and automated systems based on financial, social, or behavioral traits directly impact the fundamental right to non-discrimination. In this regard, it is proposed to incorporate into legal doctrine the “right to object to automated and algorithmic profiling” alongside the mandatory right to demand human intervention (*Human-in-the-loop*).

For reference: *Under the principles of the “Right not to be subject to automated decision-making” and “Human-in-the-loop” (human oversight and intervention) enshrined in Article 22 of Regulation (EU) 2016/679 (GDPR) and Article 14 of Regulation (EU) 2024/1689 (EU AI Act), an individual has the right to object to decisions based solely on automated processing and algorithmic scoring (profiling) that produce legal effects, and to demand human review of such decisions.*

29. Outdated, irrelevant, or disproportionately retained personal data in the digital space exerts an unjustified negative impact on an individual's future digital life. Therefore, it is proposed to research and implement the doctrine of the “right to be forgotten” – which entails the deletion of data from digital memory upon the expiration of its retention period or at the request of a citizen – by adapting it to the national legal system.

For reference: *The concept of the "Right to be forgotten / Right to erasure" is enshrined in Article 17 of the EU GDPR and the landmark ruling of the Court of Justice of the European Union (CJEU) in Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD) (Case C-131/12). This doctrine grants individuals the legal right to request the deletion of outdated or disproportionate information concerning their digital history from search engines and other data sources.*

30. Biometrics and medical metrics collected through telemedicine and wearable smart gadgets are processed on external cloud servers, directly encroaching upon the most intimate sphere of private life. In this regard, it is proposed to develop a specialized doctrinal regime and stringent encryption standards for medical bio-telemetric and remote healthcare data.

For reference: *Under the US Health Insurance Portability and Accountability Act (HIPAA Privacy and Security Rules) and the EU's European Health Data Space (EHDS) regulation, the theory of "mHealth and Telemetry Data Governance" is advanced. Under this framework, real-time medical metrics (ePHI) collected via wearable smart devices and telemedicine are classified within the "intimate privacy sphere" and are subjected to high-level security controls, including End-to-End and AES-256 encryption standards.*

31. Personal messages and media files transmitted through modern Over-the-Top (OTT) services and platforms (Telegram, WhatsApp, etc.) are processed across cross-border servers. Accounting for this global infrastructure, it is proposed to formulate a legal doctrine for securing personal data privacy and ensuring End-to-End Encryption (E2EE) within cross-platform data exchanges.

For reference: *In the European Court of Human Rights (ECHR) landmark ruling Podchasov v. Russia (Application №. 10222/23), guarantees of End-to-End Encryption (E2EE) were recognized as an indispensable safeguard of Article 8 (right to respect for private life and correspondence) of the European Convention on Human Rights. Under this precedent, the cross-border inviolability of messages transmitted across OTT platforms is legally and technically guaranteed through E2EE cryptographic standards.*

32. For Big Data and digital commerce companies, users' personal data is increasingly becoming a high-value commercial and market asset. To regulate this economic-legal phenomenon, it is proposed to legally define the balance between personal data as a commercial asset (economic resource) and as an inalienable non-property personal right.

For reference: *Under Directive (EU) 2019/770 of the European Parliament and of the Council on certain aspects concerning contracts for the supply of digital content and digital services (Digital Content Directive), as well as within digital economy doctrine, the concept of "Data as a Counter-Performance" has been established. This theory defines the legal boundaries required to maintain a reasonable balance between the commercial and market asset value of data and an individual's inalienable non-property rights.*

33. While public authorities generally collect personal data on the basis of public interest and legal obligations, the private sector collects it primarily for commercial interests and contractual performance. In this regard, it is proposed to establish a doctrinal differentiation between public and private data controllers in information law regarding their legal status, liabilities, and statutory powers.

For reference: *Under Article 6(1) of Regulation (EU) 2016/679 (GDPR)—specifically distinguishing between Public Interest / Legal Obligation and Legitimate Interests / Contract Performance—as well as within the enforcement practices of the French National Commission on Informatics and Liberty (Commission Nationale de l'Informatique et des Libertés – CNIL), the doctrine of "Public vs. Private Controller Status" has been developed. According to this*

framework, the legal bases, obligations, and degrees of liability for data processing differ strictly between public and private sector controllers.

34. Across e-government platforms and public services portals, citizens' data is automatically exchanged between various ministries and agencies on a cross-integration basis. Therefore, to ensure transparency toward citizens within the e-government architecture, it is proposed to clearly distinguish the concepts of the "single responsible controller" and the "transit data operator", establishing strict boundaries of liability.

For reference: *Under Estonia's Public Information Act and the architecture of its renowned X-Road decentralized data exchange framework, the doctrine of "Data Owner vs. Data Transit Node" is applied. Within this e-government system, the legal powers and boundaries of liability are strictly differentiated between the primary controller (single responsible operator) and transit data operators (data processors / transit nodes).*

35. During the training of artificial intelligence and Large Language Models (LLMs), thousands of personal data points are processed and ingested en masse from public and private sources without prior authorization. To mitigate this technological risk, it is proposed to establish a specialized legal regime governing the use of personal data during the AI model training phase and the "Data Ingestion" process.

For reference: *Under Article 53 of Regulation (EU) 2024/1689 (EU AI Act) and the enforcement decision of Italy's data protection authority (Garante) in the OpenAI (ChatGPT) case, the doctrine of "AI Data Ingestion & Unlearning" was established. According to this doctrine, utilizing personal data during the training phase of Large Language Models (LLMs) strictly requires an explicit legal basis (such as the right to opt out or text and data mining [TDM] exceptions).*

36. When specific acts in cyberspace (such as unlawful data acquisition or downloading) are not explicitly defined in criminal legislation, any resulting ambiguities must be resolved in favor of the accused. Therefore, it is proposed to advance the legal doctrine on the impact of criminal law gaps on constitutional principles and to precisely adapt statutory definitions (*dispositions*) to the cyber environment.

For reference: *Under the fundamental constitutional principles of In dubio pro reo (any doubt or ambiguity is resolved in favor of the accused) and Nullum crimen sine lege (no crime without law), as codified in the Rome Statute and international criminal law, strict legality applies. If emerging cyber acts are not explicitly framed as clear offense elements within the law, interpreting such ambiguities to the detriment of the accused is strictly prohibited.*

37. Classifying emerging cyber offenses in cyberspace by analogy when they are not explicitly defined by statute violates international human rights standards. In this regard, it is proposed to strictly enforce the principle of statutory clarity (*lex certa*) and the absolute prohibition of analogy in the classification of cybercrimes.

For reference: *Under the principle of legality (Principle of Legality) and statutory clarity (Lex Certa) as established in European Court of Human Rights (ECHR) precedents and European criminal law doctrine, the application of criminal law statutes by analogy or expansive interpretation (Ban on Analogy in Criminal Law) is strictly prohibited.*

38. Even if ransomware does not exfiltrate or disseminate data, restricting access by encrypting it severely infringes upon an individual's information sovereignty. Consequently, it is proposed to classify the blocking of data access and instances of cyber-extortion as an aggravated form of unlawful personal data processing.

For reference: *Under Article 4 (Data Interference) of the Council of Europe's 2001 Convention on Cybercrime (Budapest Convention) and the US Department of Justice's (DOJ) legal classification of ransomware, unlawfully encrypting data to restrict access (Ransomware / Extortion) is evaluated as a severe violation of data availability and integrity—specifically categorized as a "Cyberalogy" scenario.*

39. Minors lack the full capacity to comprehend cyber threats, online risks, and the legal consequences of disclosing their personal data. Accounting for these psychological and age-related characteristics, it is proposed to formulate the doctrine of "enhanced information privacy for minors" and to introduce a specialized parental (guardian) consent mechanism for processing their data.

For reference: *Under Article 8 of Regulation (EU) 2016/679 (GDPR) and the US Children's Online Privacy Protection Act (COPPA), the doctrine of "Enhanced Child Privacy Standards" has been established. According to this framework, processing the personal data of minors under the age of 13 or 16 strictly requires verifiable parental (or guardian) consent.*

40. When personal data crosses national borders and is transferred to foreign servers, the direct regulatory authority and oversight of national jurisdictions become constrained. In this regard, it is proposed to incorporate the theory of "extraterritorial jurisdiction" into information law and to tighten regulatory requirements for foreign entities processing the personal data of national citizens abroad.

For reference: *Under the "Extraterritorial Jurisdiction / Targeting Principle" codified in Article 3(2) of Regulation (EU) 2016/679 (GDPR), if a foreign entity located outside the EU offers goods or services to, or monitors the behavior of, individuals within the EU, the requirements of the regulation apply mandatorily to that foreign controller or processor regardless of its physical location.*

41. The widespread deployment of biometric identification (Face-ID) and intelligent video surveillance systems in public spaces and public transit erodes an individual's boundaries of anonymity and privacy. Consequently, it is proposed to formulate a legal theory defining the limits of information privacy within the "public cyberspace" and to establish strict legal and proportionality boundaries for biometric data collection in public areas.

For reference: *Under Article 5 of Regulation (EU) 2024/1689 (EU AI Act), the use of real-time remote biometric identification systems (Mass Surveillance) in publicly accessible spaces is recognized as a fundamental threat to human rights. Accordingly, such practices are strictly prohibited with narrow exceptions, thereby securing explicit legal guarantees for public anonymity.*

42. The automated bulk collection (scraping) of personal data from open web sources and social networks by automated scripts, bots, and parsers to build databases severely compromises individual data protection rights. To curb this practice, it is proposed to establish clear legal boundaries for web scraping and to legally classify unauthorized automated scraping of publicly available data as unlawful collection.

For reference: *Under the joint statement on "Mass Data Scraping Unlawfulness" issued by global data protection authorities – including members of the European Data Protection Board (EDPB) and regulatory authorities across Italy, France, and the UK – alongside key precedents following hiQ Labs, Inc. v. LinkedIn Corp., the mere accessibility of personal data on the public internet does not constitute legal authorization for mass automated extraction by bots and scripts.*

43. Personal email addresses, IP telephony details, and messenger IDs serve as direct identifiers that enable targeting and unsolicited outreach (spam) to individuals. In this regard, it is proposed to reinforce the classification of network communication identifiers as personal data and to explicitly prohibit their commercial use without the data subject's prior consent.

For reference: *Under the "Opt-in Direct Marketing" principle codified in Article 13 of Directive 2002/58/EC of the European Parliament and of the Council on privacy and electronic communications (ePrivacy Directive), utilizing email addresses, messenger IDs, or other electronic communication identifiers for commercial or marketing purposes strictly requires the individual's prior, freely given opt-in consent.*

44. Bank card credentials, transaction histories, and PIN codes simultaneously constitute elements of banking secrecy and personal data objects. Accounting for this intersection, it is proposed to formulate the "duality theory" regarding the proportionality of banking secrecy and personal data regimes, and to integrate the highest protective standards of both frameworks.

For reference: *Under Directive (EU) 2015/2366 on payment services (PSD2), the Payment Card Industry Data Security Standard (PCI DSS), and financial law doctrine, a "Dual-Regime Protection Strategy" is applied. Within this framework, financial credentials situated at the intersection of banking secrecy and personal data protection are subjected to the most rigorous, comprehensive security standards.*

45. Voters' digital registries, political preferences, and voting histories fall into the category of highly sensitive personal data. Consequently, it is proposed to formulate a "digital data privacy" concept within electoral rights and democratic processes, establishing robust mechanisms to safeguard voter databases against political manipulation.

For reference: *Under Article 9 of Regulation (EU) 2016/679 (GDPR) – which classifies political opinions as a special category of personal data and the "Electoral Data Protection Governance" doctrine established following the UK Information Commissioner's Office (ICO) investigation into Cambridge Analytica, the unauthorized processing of voter databases for political profiling and psychographic micro-targeting is strictly prohibited.*

46. The publishing of unanonymized personal data within public registers on open data portals by state authorities poses a direct threat to citizen security and privacy. In this regard, it is proposed to establish a "mandatory preliminary anonymization" concept when constructing open registers and Open Data resources.

For reference: *Under Directive (EU) 2019/1024 on open data and the re-use of public sector information (Open Data Directive) and GDPR provisions, the principle of "Privacy by Open Data" is enforced. Under this framework, mandatory and irreversible pre-anonymization (mandatory pre-anonymisation) of personal data is required prior to the publication of public registers.*

47. The absence of a mandatory framework to evaluate the risks posed to personal privacy and data security prior to deploying information and communication systems, mobile applications, and state IT infrastructure creates significant legal vulnerabilities. To address this gap, it is proposed to establish a theoretical model and procedural framework for mandatory "Privacy Impact Assessment" (PIA) audits before initiating high-risk digital and technological projects.

For reference: *Under Article 35 of Regulation (EU) 2016/679 (GDPR), which codifies the "Data Protection Impact Assessment" (DPIA / PIA), and in alignment with the ISO/IEC 29134*

standard, a mandatory procedure is established requiring comprehensive legal and technical PIA audits for any new technological or information system capable of posing high risks to the rights and freedoms of data subjects prior to its operational deployment.

48. Inadequate or superficial anonymization (depersonalization) procedures allow data sets to be cross-referenced, enabling the re-identification of individuals. To address this risk, it is proposed to establish a formal legal classification evaluating the irreversibility of depersonalization techniques and to recognize only absolute, non-reversible methods as legally binding anonymization.

For reference: *Under the criteria established in Opinion 05/2014 on Anonymisation Techniques issued by the Article 29 Data Protection Working Party (now EDPB), depersonalization mechanisms (such as k-anonymity, l-diversity, and t-closeness) achieve true legal status as anonymized data only when they eliminate the risk of re-identification into an absolute, irreversible state.*

49. Overly absolute restrictions on personal data risk stifling the digital economy and artificial intelligence innovation, whereas an absence of regulatory boundaries compromises fundamental human rights. To resolve this tension, it is proposed to theoretically codify the principle of "proportionate and balanced regulation" within the digital economy and AI domain.

For reference: *Under Article 52 of the Charter of Fundamental Rights of the European Union and the "Risk-Based Proportionality Approach" framework established in Regulation (EU) 2024/1689 (EU AI Act), legal protection of human rights and technological innovation (facilitated via Regulatory Sandboxes) are advanced symmetrically through strict adherence to the principle of proportionality.*

50. Ensuring personal data privacy cannot be achieved through legal norms alone; it necessitates the seamless integration of law, software engineering, cryptography, and cybersecurity. Building upon this foundational premise, it is proposed to formalize the concept of "Cyberalogical Comprehensive Protection" (*Кибералогик комплекс муҳофаза*) as an interdisciplinary conceptual framework situated at the convergence of information law and cybersecurity sciences.

For reference: *According to Lawrence Lessig's foundational doctrine "Code is Law", Article 25 of Regulation (EU) 2016/679 (GDPR) codifying "Privacy by Design and by Default", and your proprietary "Cyberalogy" (Кибералогия) research methodology, personal data protection cannot rely solely on statutory mandates. Instead, robust guarantees require an integrated synthesis of legal, cryptographic, and technical mechanisms within a unified cyberalogical architecture.*

51. It is necessary to expand the concept of "personal data" based on the principle of technological neutrality. To achieve this, the definitions of "personal data" set forth in Article 3 of the Law "On Personal Data," Article 46^2 of the Code of Administrative Responsibility, and Article 141^2 of the Criminal Code should be broadened under the technology-neutrality principle to clarify their substantive scope.

Implementation Mechanism:

The first paragraph of Article 3 of the Law "On Personal Data" shall be amended to read as follows:

"personal data – any information expressed in analog, electronic, digital, virtual, or any other form that enables the direct or indirect identification of a specific

natural person, regardless of the processing or automation methods used or the technological environment applied;";

For reference: *Under Article 4(1) of the European Union's General Data Protection Regulation (GDPR), personal data is defined as "any information relating to an identified or identifiable natural person". The regulation operates on the principle of full technological neutrality: whether data exists in paper, electronic, or virtual formats, or the specific methods used to process it, is legally immaterial.*

Beyond direct identifiers (such as full names or identification numbers), the GDPR explicitly recognizes indirect identifiers including IP addresses, browser cookies, geolocation data, and other digital telemetry as personal data. A consistent approach is codified in the United Kingdom's Data Protection Act 2018 (UK GDPR) and Japan's Act on the Protection of Personal Information (APPI), where the legal focus remains squarely on the capacity of data to identify an individual rather than the automation tools or technical environments used.

At the international policy level, the OECD Privacy Guidelines and the modernized Council of Europe Convention 108+ similarly mandate comprehensive data protection safeguards irrespective of the processing technology or storage environment.

52. It is proposed to expand the statutory definitions (*dispositions*) of the first paragraphs of Article 141^2 of the Criminal Code (CC) and Article 46^2 of the Code of Administrative Responsibility (CAR) by incorporating new alternative offenses, specifically unlawful acquisition, possession, and enabling unauthorized access.

Implementation Mechanism:

In the dispositions of Article 141^2 of the CC and Article 46^2(1) of the CAR, the word "destruction" shall be followed by inserting the words:

", as well as their unlawful acquisition, possession, unauthorized access, or use by any method, or enabling unlawful access to them".

For reference: *Under the criminal and administrative legal frameworks of the European Union and the United States, personal data offenses extend beyond unlawful dissemination or destruction to classify unauthorized access, possession, and unlawful processing as independent criminal acts.*

Specifically, under Sections 202a (Data espionage) and 202b (Data interception) of the German Criminal Code (Strafgesetzbuch), unlawfully obtaining protected data and facilitating unauthorized access incur distinct criminal liability. Sections 1 and 2 of the United Kingdom's Computer Misuse Act 1990 similarly treat unauthorized access or attempting unauthorized access to computer systems and data as standalone offenses.

Furthermore, the United States Computer Fraud and Abuse Act (CFAA, 18 U.S.C. § 1030) establishes strict criminal penalties for intentionally accessing a protected computer without authorization, obtaining data, or trafficking in access devices (access device fraud). Adopting this international legal standard ensures early detection and prevention of preparatory and preliminary offenses that threaten personal data security.

53. It is necessary to adapt the definition of a "personal data database" to artificial intelligence and algorithmic environments. To achieve this, the concept of "database" in Article 3 of the Law "On Personal Data" should be rephrased to encompass AI models, neural networks, and virtual-algorithmic architectures.

Implementation Mechanism:

The relevant paragraph of Article 3 of the Law "On Personal Data" shall be amended to read as follows:

"**personal data database** – structured personal data and its virtual collections that enable the determination and (or) identification of a person, formed within traditional and digital information systems, software and environmental complexes,

artificial intelligence models, and algorithmic environments, regardless of their form or storage method";

For reference: *In the legislation of the European Union, the United Kingdom, and other developed jurisdictions, as well as under international standards, definitions of personal data databases and processing environments maintain a broad, technology-neutral scope that encompasses artificial intelligence and algorithmic systems.*

Specifically, under Article 4(6) of the EU General Data Protection Regulation (GDPR), a "filing system" refers to any structured set of personal data accessible according to specific criteria, whether centralized, decentralized, or dispersed on a functional or geographical basis. Furthermore, under Regulation (EU) 2024/1689 (EU AI Act) and European Data Protection Board (EDPB) guidelines, training datasets used in AI models (training data), vector databases maintained in neural networks, and algorithmic processing environments are explicitly recognized as personal data systems subject to comprehensive data protection requirements.

Similarly, the UK Data Protection Act 2018 and Singapore's Personal Data Protection Act (PDPA) do not restrict the definition of a database to traditional repositories, extending it to cover all virtual datasets processed within algorithmic and artificial intelligence systems that serve to identify individuals.

54. It is proposed to amend Part 2 of Article 141^2 of the Criminal Code (CC) by incorporating the commission of the offense through the use of artificial intelligence, neural networks, and generative technologies (Deepfake) as an aggravating circumstance.

Implementation Mechanism:

Part 2 of Article 141^2 of the CC shall be supplemented with paragraph "e" reading as follows:

"e) committed through or with the application of artificial intelligence systems, neural networks, synthetic media, or generative digital technologies (Deepfake);"

For reference: *In the legislation of the European Union, the United States, and several other developed jurisdictions, the unlawful processing, falsification, or dissemination of personal data via artificial intelligence, generative technologies, and deepfakes is recognized as a factor that sharply escalates the social danger of the act, thereby constituting an aggravating circumstance.*

Specifically, Regulation (EU) 2024/1689 (EU AI Act) classifies non-compliance with transparency mandates regarding deepfakes and synthetic media, as well as the non-consensual artificial synthesis of an individual's image or voice, as a severe legal violation. In the United States, at both state (e.g., California and Texas statutory frameworks) and federal levels (including legislative acts such as the TAKE IT DOWN Act and the DEEPFAKES Accountability Act), the unauthorized generation and distribution of content using generative AI and deepfakes involving an individual's likeness or personal data incurs heightened criminal and civil liability.

Similarly, the Cyberspace Administration of China (CAC) enforces regulations on Deep Synthesis Technologies, strictly prohibiting the unauthorized modification or falsification of personal identification features via AI and imposing severe penalties for non-compliance. Establishing this legal standard serves to mitigate systemic threats posed by generative technologies to human dignity, honor, and personal privacy.

55. It is necessary to establish clear legal and quantitative criteria for the ambiguous statutory term "resulting in grave consequences" provided in paragraph "d" of Part 2, Article 141^2 of the Criminal Code (CC). To achieve this, a relevant clarification should be incorporated into the corresponding Resolution of the Plenum of the Supreme Court of the Republic of Uzbekistan.

Implementation Mechanism:

A clarification with the following content shall be added to the relevant Resolution of the Plenum of the Supreme Court:

"For the purposes of paragraph 'd' of Part 2, Article 141^2 of the Criminal Code, 'grave consequences' shall be understood to mean, in particular: instances resulting in the leakage or unlawful dissemination of personal data of more than 1,000 data subjects; causing material or financial damage on an especially large scale; inflicting irreparable harm to an individual's honor and dignity; or driving a person to a state of suicide or resulting in suicide".

For reference: *In international criminal jurisprudence and court practice, to prevent the term "grave consequences" resulting from data breaches from remaining a purely subjective evaluative concept, it is widely defined through clear quantitative parameters (number of affected subjects, monetary scale of loss) and qualitative indicators (psychological and moral harm, suicide, or irreparable loss of reputation).*

Specifically, Article 83 of the European Union's General Data Protection Regulation (GDPR) establishes the number of data subjects affected, the scale of damage, and the level of societal risk as primary criteria when assessing liability and imposing sanctions. In U.S. and UK judicial practice (within Data Breach Litigation and precedents under the Computer Misuse Act), mass data breaches involving extensive monetary or moral harm are automatically qualified as aggravating factors.

Similarly, Article 226-16 and related provisions of the French Penal Code prescribe heightened criminal penalties when the unlawful processing of personal data leads to a severe deterioration in a person's life conditions or poses a threat to life. Defining precise quantitative and qualitative thresholds at the Supreme Court Plenum level – such as data leaks affecting over 1,000 subjects, damage on an especially large scale, or circumstances leading to suicide – eliminates unwarranted administrative discretion and ensures a uniform, predictable application of the law.

56. It is proposed to introduce a technical and legal digital audit mechanism for foreign platforms to ensure the enforcement of Article 27^1 of the Law "On Personal Data", while also establishing a mandatory 72-hour breach notification requirement for data operators.

Implementation Mechanism:

1. Adopt a Resolution of the Cabinet of Ministers approving the *"Regulation on the Procedure for Conducting Technical and Legal Audits of Foreign Digital Platforms and Entities Processing Personal Data of Citizens of the Republic of Uzbekistan for Compliance with Article 27^1 Requirements".*

2. Supplement the Law "On Personal Data" with Article 27^2 reading as follows:

"**Article 27^2. Obligation to report information security incidents (data breaches)**

The operator shall, within no more than 72 hours from the moment of discovering unauthorized disclosure, leakage, or access to personal data, mandatorily notify the authorized state body and the affected data subjects".

For reference: *Imposing a mandatory 72-hour notification timeframe (Data Breach Notification) on operators following a data breach or security incident is an internationally recognized gold standard.*

Under Article 33 of the EU General Data Protection Regulation (GDPR), data controllers are required to notify the supervisory authority without undue delay and, where feasible, no later

than 72 hours after becoming aware of a breach. Article 34 of the GDPR further mandates direct notification to data subjects without undue delay if the breach poses a high risk to their rights and freedoms.

Identical 72-hour (or stricter) notification mandates are codified in the UK Data Protection Act 2018 (UK GDPR), Article 38 of Brazil's General Personal Data Protection Law (LGPD), and Singapore's Personal Data Protection Act (PDPA). In the United States, state-level privacy statutes (such as California's CCPA/CPRA), along with standards from the International Telecommunication Union (ITU) and ISO/IEC 27001 / ISO/IEC 27701, treat rapid incident disclosure as a primary risk mitigation mechanism. Incorporating this rule into national legislation significantly enhances early containment of cyber incident repercussions and strengthens safeguards for data subjects.

57. It is proposed to introduce an explicit legal prohibition against employer monitoring of employees' personal devices, accounts, and communications into Article 176 of the Labor Code, while also establishing an explicit "Right to Disconnect" under a new Article 176[1].

Implementation Mechanism:

1. Article 176 of the Labor Code shall be supplemented with the following paragraph:

"The employer is prohibited from collecting, monitoring, or demanding personal correspondence, communications, or personal data of an employee contained on their personal means of communication, personal devices, or during off-duty hours".

2. The Labor Code shall be supplemented with Article 176[1] reading as follows:

"**Article 176[1]. The employee's right to disconnect**

An employee has the right to disconnect from corporate communications, electronic mail, and notifications during non-working hours, rest days, and public holidays. The employer shall not compel an employee to establish contact during these periods nor impose disciplinary measures for failing to respond.";

For reference: *In European and international labor and data protection law, protecting an employee's privacy and establishing strict limits on monitoring personal devices (Bring Your Own Device – BYOD), personal accounts, and off-duty communications represent fundamental statutory guarantees.*

In landmark rulings such as Bărbulescu v. Romania (2017) and Barbules v. France, the European Court of Human Rights (ECtHR) established that employers must adhere strictly to principles of necessity and proportionality when monitoring workplace communications and must refrain from unjustified interference in an employee's private sphere. Furthermore, under Article 88 of the EU General Data Protection Regulation (GDPR) and European Data Protection Board (EDPB) guidelines, employers lack the legal right to monitor or gather data from an employee's personal devices or accounts.

Additionally, the "Right to Disconnect" (Droit à la déconnexion) was pioneered in Article L. 2242-17 of the French Labor Code in 2016 to guarantee digital disconnection outside working hours. Identical guarantees have since been enacted across Belgium, Spain (Organic Law 3/2018), Portugal, Italy, Ireland, and within Australia's 2024 amendments to the Fair Work Act.

At the global policy level, the International Labour Organization (ILO) and the European Parliament (2021 Resolution on the Right to Disconnect) recognize off-duty disconnection as a foundational safeguard necessary to protect occupational mental health, maintain work-life balance, and eliminate algorithmic overreach in employment relations.

58. It is proposed to establish strict regulatory oversight and explicit subject consent mechanisms for the transfer of PINFL (ЖШШШИР) and tax secrets by tax authorities to commercial third parties (commercial banks, fintechs), while also explicitly prohibiting the misuse of the Unified Electronic Voters' Register for electioneering, political propaganda, or spam.

Implementation Mechanism:

1. Article 132 of the Tax Code shall be supplemented with the following paragraph:

"Personal data regarding an individual's PINFL and information constituting tax secrecy may be disclosed to commercial entities (banks, fintechs) only after obtaining the direct consent of the taxpayer, verified via their Electronic Digital Signature (EDS) or two-factor authentication (SMS code or biometrics)".

2. The relevant provision of the Election Code shall be supplemented with a cross-referencing norm enforcing responsibility under Article 46^2 of the Code of Administrative Responsibility (CAR):

"Utilizing the electronic voters' register and personal data contained therein for pre-election campaigning, political propaganda, or direct advertising notifications is prohibited and entails administrative liability in accordance with Article 46^2 of the Code of Administrative Responsibility".

For reference: *In international banking, fintech, and electoral legal frameworks, processing an individual's financial, tax, or voting registry data strictly requires explicit, verified opt-in consent (explicit opt-in consent) and is tightly restricted to its designated legal purpose.*

Under Regulation (EU) 2015/2366 (PSD2) and GDPR provisions, transferring financial or tax information to third-party service providers (TPPs/Fintechs) requires Strong Customer Authentication (SCA)—verified via two-factor confirmation or biometric identification. In the United States, under the Gramm-Leach-Bliley Act (GLBA) and Internal Revenue Service (IRS) regulations (26 U.S.C. § 7216), disclosing tax return information or tax identification numbers to commercial or credit entities requires formal written consent (Consent to Disclose Tax Return Information) validated through secure digital signature protocols. Identical mandates are enforced under the UK Open Banking Standard and Monetary Authority of Singapore (MAS) regulations.

Regarding electoral registries, guidelines issued by the European Data Protection Board (EDPB), the UK Electoral Commission, and the UK Information Commissioner's Office (ICO) prohibit leveraging state voter rolls (Full Register) for political profiling, unsolicited direct marketing, or campaign spam without explicit opt-in consent. Enforcing these statutory rules prevents the commercialization or political exploitation of citizens' PINFL identifiers, tax records, and electoral registry entries.

59. It is proposed to establish strict retention limits and automated deletion protocols for personal data processed through the Single Interactive State Services Portal (my.gov.uz), while also institutionalizing the role of the Data Protection Officer (DPO) across public authorities and private entities managing large-scale databases.

Implementation Mechanism:

1. Adopt a Resolution of the Cabinet of Ministers approving the *"Regulation on the Procedure for Processing Personal Data in the Provision of State Services via the Single Interactive State Services Portal (my.gov.uz) and their Automated Anonymization and Deletion Upon Completion of Service"*.

2. Supplement the Law "On Personal Data" with Article 28^1 reading as follows:

"**Article 28^1. Data Protection Officer (DPO)**

State authorities, banks, and private entities managing large-scale personal data databases shall establish the position of Data Protection Officer (DPO), responsible for ensuring personal data protection and monitoring compliance with applicable data privacy legislation".

For reference: *In the European Union and other advanced legal jurisdictions, enforcing data retention limits, storage limitation, and automated erasure (data retention and automatic deletion) upon fulfilling the designated processing purpose is codified as a binding statutory requirement.*

Specifically, under Article 5(1)(e) of the EU General Data Protection Regulation (GDPR), the principles of "storage limitation" and "purpose limitation" mandate that public and e-government systems retain personal data only for as long as strictly necessary to fulfill the service purpose. In digital governance frameworks such as Estonia's e-Estonia infrastructure automated algorithms irreversibly anonymize or purge user telemetry once service execution completes (data minimization & storage limitation by design). Equivalent technical standards are operational under the UK Government Digital Service (GDS) and Singapore's GovTech platform to eliminate excessive data accumulation on public portals and mitigate breach exposure.

Regarding institutional oversight, appointing a Data Protection Officer (DPO) within organizations handling large volumes of personal data represents a global benchmark. Under Articles 37–39 of the GDPR, public sector bodies and private organizations engaged in systematic, large-scale processing or monitoring must designate an independent DPO to audit internal compliance, liaise with supervisory authorities, and guide privacy impact assessments.

Mandatory DPO appointments are similarly codified under Section 11 of Singapore's Personal Data Protection Act (PDPA), the UK Data Protection Act 2018 (UK GDPR), Brazil's General Personal Data Protection Law (LGPD, Article 41), and the Philippine Data Privacy Act. Establishing this statutory role within national legislation ensures structured, independent internal compliance mechanisms across critical data holders, including telecommunications providers, banking institutions, and state authorities.

60. It is proposed to establish strict regulatory frameworks for protecting genetic and DNA data as special categories of personal data, while also requiring commercial banks and payment organizations to store only irreversible mathematical vector hashes rather than raw biometric images.

Implementation Mechanism:

1. Adopt a Cabinet of Ministers Resolution approving the *"Regulation on the Procedure for the Collection, Storage, Processing, and Protection of Personal Genetic and DNA Data of Citizens"*.

2. Adopt a Joint Resolution of the Central Bank and the Ministry of Digital Technologies approving the *"Regulation on the Cryptographic Algorithmization and Irreversible Hashing of Biometric Data in the Financial, Banking, and Fintech Sectors"*.

For reference: *In the European Union, the United States, and other technologically advanced jurisdictions, genetic, DNA, and biometric data possess a highly sensitive character and are granted heightened statutory protection under specialized legal regimes.*

Under Article 9 of the EU General Data Protection Regulation (GDPR), processing genetic data and biometric identifier sets is prohibited as a general rule and permitted only under strict exceptions such as explicit informed consent, public health necessities, or law enforcement imperatives subject to specialized governmental oversight.

In the United Kingdom, the collection, retention, and handling of DNA samples are regulated by the Human Tissue Act 2004 and the Data Protection Act 2018. In the United States, the Genetic Information Nondiscrimination Act (GINA) together with Health Insurance Portability and Accountability Act (HIPAA) privacy standards prohibit leveraging genetic data for discriminatory practices in commercial, insurance, or employment contexts.

Regarding financial and fintech security, storing raw biometric records (e.g., facial images, fingerprints, or voiceprints) is strictly prohibited across leading jurisdictions. Instead, converting raw biometric inputs into irreversible mathematical vectors or cryptographic template hashes (one-way cryptographic hash/template) is codified as mandatory.

Under GDPR Article 9 guidelines issued by the European Data Protection Board (EDPB), biometric platforms must implement Privacy by Design and data minimization principles by immediately purging raw source images post-extraction, retaining solely non-reversible vector templates.

In the United States, standards set by the National Institute of Standards and Technology (NIST SP 800-63B and NIST FRVT/FATE), alongside Illinois's Biometric Information Privacy Act (BIPA), mandate the storage of one-way encrypted hashes rather than raw biometric media. Furthermore, ISO/IEC 24745 (Biometric information protection) establishes international technical benchmarks for cancellable and irreversible biometrics. Implementing these controls eliminates the risk of raw biometric leaks or subsequent identity synthesis (e.g., deepfakes or biometric fraud) in the event of a system breach.

61. It is proposed to statutorily grant citizens the right to demand the erasure or de-indexing of outdated, inaccurate, or unlawfully processed personal data from search engines and digital sources ("Right to be Forgotten"), while also prohibiting pre-ticked consent boxes (Opt-out) in favor of explicit, affirmative consent (Opt-in).

Implementation Mechanism:

1. Supplement the Law "On Personal Data" with Article 18^1 reading as follows:

"**Article 18^1. Right to demand erasure of personal data from digital sources and search indices ("Right to be forgotten")**

The data subject has the right to demand that the operator or search engines remove (de-index) links and digital copies of their personal data processed in violation of legal requirements, or which are inaccurate, outdated, or no longer relevant.";

2. Supplement Article 18 of the Law "On Personal Data" with the following paragraph:

"Consent to the processing of personal data must be given solely through an independent, active, and explicitly expressed action of the subject (Opt-in). Pre-ticked boxes in electronic interfaces or silence shall produce no legal consequences and shall not be recognized as valid consent.";

For reference: *In the European Union and jurisdictions with advanced privacy frameworks, the right to demand the erasure or de-indexing of outdated, inaccurate, or unlawfully processed personal data ("Right to be forgotten" / "Right to erasure") is recognized as a fundamental privacy right.*

This legal doctrine was established by the Court of Justice of the European Union (CJEU) in the landmark 2014 case Google Spain v. AEPD and Mario Costeja González (C-131/12) and subsequently codified under Article 17 of Regulation (EU) 2016/679 (GDPR). Under GDPR Article 17, data subjects may request de-indexing and erasure when personal data is no longer necessary for its original purpose, when consent is withdrawn, or when processing is unlawful. Equivalent rights are codified in Section 10.3 of the Russian Federal Law "On Information,

Information Technologies and Information Protection", the UK Data Protection Act 2018, and within the privacy frameworks of Argentina, South Korea, and Turkey.

Regarding digital user interfaces, international standards strictly prohibit pre-selected consent boxes (pre-ticked boxes/Opt-out) and manipulative interface designs (Dark Patterns), mandating explicit, active consent (Opt-in).

Under Articles 4(11) and 7 of the GDPR, valid consent requires a "clear affirmative action", explicitly excluding silence, inactivity, or pre-ticked checkmarks. The CJEU reaffirmed this principle in Planet49 GmbH (C-673/17, 2019), ruling that pre-selected checkboxes for cookie consent fail to constitute valid legal consent. Similar restrictions against deceptive design patterns are enforced under the UK GDPR and California's Privacy Rights Act (CPRA). Enacting these standards ensures genuine user autonomy and robust control over digital personal data.

62. It is proposed to establish a statutory age threshold for digital consent in cyberspace, requiring parental or legal guardian consent to process the personal data of minors under 16 years of age.

Implementation Mechanism:

Supplement Article 18 of the Law "On Personal Data" with the following paragraph:

"The processing of personal data of minors under the age of 16 in personal data databases shall be carried out with the consent of their parents or legal guardians, confirmed in written or electronic form.";

For reference: *Establishing a clear digital age of consent (Age of digital consent) to safeguard minors' personal data across online platforms and digital services is an internationally recognized standard.*

Under Article 8 of the European Union General Data Protection Regulation (GDPR), the baseline age threshold for parental consent regarding information society services is set at 16 years, while allowing EU Member States to establish a national threshold between 13 and 16 years (e.g., 16 years in Germany, France, the Netherlands, and Lithuania; 14 years in Italy and Spain; and 13 years in the United Kingdom).

In the United States, digital privacy for minors is regulated under the Children's Online Privacy Protection Act (COPPA), which mandates obtaining verifiable parental consent (verifiable parental consent) prior to collecting or processing personal information from children under 13 years of age.

Furthermore, specialized regulatory frameworks—such as the UK Age Appropriate Design Code (Children's Code) and the Cyberspace Administration of China's (CAC) provisions on the protection of minors' personal information online—require digital platforms to combine parental consent protocols with robust age verification (age verification) mechanisms. Codifying this standard into national legislation creates a comprehensive safeguard against digital threats, online manipulation, and the unauthorized commercial exploitation of minors' personal data.

63. It is proposed to establish turnover-based administrative financial sanctions against legal entities for mass personal data breaches and gross violations of privacy legislation, inserting a dedicated financial sanction mechanism into the Law of the Republic of Uzbekistan "On Personal Data".

Implementation Mechanism:

Supplement the Law of the Republic of Uzbekistan "On Personal Data" with a financial sanction provision reading as follows:

"Legal entities that permit a mass breach of personal data databases (data breach) or commit gross violations of legislative requirements shall be subject to a judicial financial fine ranging from 1 percent to 3 percent of their total annual

turnover (revenue) for the preceding financial year, applied upon application by the authorized body.";

For reference: *In the European Union and leading global jurisdictions, financial sanctions imposed on corporate bodies for mass data breaches and systemic privacy violations are pegged directly to total global annual turnover (global annual turnover).*

Under Article 83(5) of the EU General Data Protection Regulation (GDPR), severe infringements carry administrative fines of up to €20 million or up to 4 percent of the undertaking's total global annual turnover for the preceding financial year, whichever is higher.

Under the UK Data Protection Act 2018 (UK GDPR), maximum fines for major breaches similarly reach £17.5 million or 4 percent of global annual turnover. Brazil's General Personal Data Protection Law (LGPD, Article 52) empowers supervisory authorities to levy fines of up to 2 percent of a legal entity's annual turnover in Brazil (up to 50 million BRL per violation). Singapore's Personal Data Protection Act (PDPA) enforces penalty caps of up to 10 percent of an organization's annual turnover in Singapore for major data breaches.

Calculating financial penalties as a percentage of annual turnover prevents large corporations and data handlers from treating compliance fines as nominal operating costs, compelling substantial, continuous investment in cyber infrastructure and data protection governance.

64. It is proposed to mandate periodic, mandatory cybersecurity audits for state and private entities categorized under the register of critical information infrastructure (CII), while also establishing a judicial enforcement mechanism for the irreversible destruction of unlawfully collected personal data databases through the Bureau of Mandatory Enforcement (MIB) and cybersecurity specialists.

1. Mandatory Cybersecurity Audits for Critical Infrastructure

Implementation Mechanism:

Adopt a Joint Resolution of the Cabinet of Ministers and the Cybersecurity Center approving the *"Procedure for Conducting Periodic Cybersecurity and Data Protection Audits in Entities of Critical Information Infrastructure.";*

For reference: *Across advanced legal jurisdictions, including the European Union and the United States, entities forming part of Critical Information Infrastructure (CII) are subject to mandatory cybersecurity and data protection compliance audits.*

Under the EU NIS2 Directive (Directive on measures for a high common level of cybersecurity across the Union) and Article 32 of the General Data Protection Regulation (GDPR), critical infrastructure operators and essential service providers must undergo independent external or internal security audits at least annually to evaluate data processing resilience and system integrity.

In the United States, cybersecurity audits and stress testing are mandated under standards promulgated by the Cybersecurity and Infrastructure Security Agency (CISA) and the NIST Cybersecurity Framework (CSF 2.0).

Similarly, Singapore's Cybersecurity Act and Estonia's digital governance laws require registered CII entities to undergo annual technical and organizational compliance audits conducted by accredited independent auditors, with formal audit reports submitted to supervisory authorities. Implementing these controls mitigates system vulnerabilities and prevents mass data breaches arising from cyberattacks on state and essential private infrastructure.

2. Irreversible Destruction of Unlawfully Processed Personal Data

Implementation Mechanism:

Supplement the legal framework governing personal data protection and judicial execution with the following provision:

“The irreversible destruction (erasure) of personal data databases and their source media whether held in digital environments or physical storage that have been unlawfully collected, acquired, or processed shall be executed on the basis of a court writ of execution by the Bureau of Mandatory Enforcement (MIB) with the mandatory participation of certified cyber-forensic experts”.;

For reference: *International judicial and enforcement practices utilize technical-legal protocols such as complete data destruction and algorithmic disgorgement—to permanently eliminate unlawfully acquired personal data and derivative models.*

Under Articles 17 and 58 of the EU GDPR and corresponding judicial enforcement standards, simple file deletion is insufficient; data sanitization must be executed under the supervision of digital forensics specialists pursuant to international technical standards such as ISO/IEC 27040 and NIST SP 800-88 (Guidelines for Media Sanitization utilizing Purge, Cryptographic Erase, and Physical Destruction methods).

In the United States, enforcement orders issued by the Federal Trade Commission (FTC) and federal courts enforce “algorithmic disgorgement” – requiring the destruction not only of unlawfully gathered data, but also of artificial intelligence models trained on such data. Physical hardware (hard drives, server arrays) is rendered completely unrecoverable at the chip and magnetic media levels under the oversight of U.S. Marshals and cybersecurity experts.

In the United Kingdom, High Court Enforcement Officers and specialists from the Information Commissioner's Office (ICO) oversee the execution of court orders and issue tamper-proof Certificates of Destruction (Certificate of Destruction). Incorporating this mechanism into national enforcement procedures prevents the resurrection, cloning, or illicit retention of unauthorized databases post-judgment.

65. It is proposed to develop a single national standard (O‘zDst) for personal data de-identification, pseudonymization, and algorithmic protection, and for the Uzbek Agency for Technical Regulation to adopt the standard: **“O‘zDst: Methods and Technical Requirements for Data Anonymization, Pseudonymization, and Algorithmic De-identification.”**

For reference: *In the practice of leading technology and data protection countries such as the European Union and the United States, strict standardization of anonymization and pseudonymization processes is mandatory when processing personal data and using it for scientific, statistical, or commercial purposes.*

In particular, the EU General Data Protection Regulation (GDPR, Article 4(5) and Article 89) recognizes pseudonymization as a key technical safeguard for ensuring data security and mitigating risks. Internationally, digital standards such as ISO/IEC 20889 (Privacy-enhancing data de-identification and anonymization techniques) and ISO/IEC 27555 are widely applied, specifically regulating mathematical and algorithmic methods of anonymization (k-anonymity, l-diversity, t-closeness, differential privacy).

In the United States, requirements for algorithmic data de-identification are established based on NIST IR 8053 (De-Identification of Personal Information), developed by the National Institute of Standards and Technology (NIST), as well as the Department of Health and Human Services (HHS) HIPAA Safe Harbor and Expert Determination standards.

In the United Kingdom, the “Anonymisation and Pseudonymisation Code of Practice” adopted by the Information Commissioner’s Office (ICO) provides technical guidance and criteria to reduce the re-identification risk of anonymized data to zero.

The adoption of a unified O‘zDst standard in national legislation and the standardization system will enable the secure use of data in developing the digital economy, Big Data, and artificial intelligence systems while preserving citizens' right to privacy.

66. Prohibiting the mass collection (scraping) of citizens' personal data from websites and open registries via automated software (parsers, bots, scripts), and

simultaneously proposing the addition of a qualifying offense to Article 462 of the Code of Administrative Responsibility with the following content:

“The mass collection (scraping), systematization, and compiling into databases of personal data from open sources and web resources via automated software tools (scripts, bots, parsers) without the data subject's consent – shall result in.”;

For reference:: *In modern cyber legislation and judicial practice of the European Union, the US, and Asian countries, the unauthorized mass collection of personal data (Data Scraping) from open sources and social networks via automated programs (parsers, bots, web scrapers) is considered a serious violation of personal privacy and data security. Specifically, under the EU's GDPR, the public availability of data on the internet does not grant the right to automatically collect and convert it into commercial, systematized databases without the data subject's consent or a lawful basis. The European Data Protection Board (EDPB) and the Italian Data Protection Authority (Garante) have imposed fines worth hundreds of millions of euros on Clearview AI and industry scraping companies for collecting facial images and personal data from open sources via bots. In the United States, under the federal Computer Fraud and Abuse Act (CFAA) and state court practice (for instance, litigation involving Meta, LinkedIn, and HiQ Labs), systematic automated scraping of open data, violation of website Terms of Service, and bypassing security barriers (anti-bot mechanisms) are recognized as unlawful acts. Similarly, Singapore's PDPA and China's Personal Information Protection Law (PIPL) mandate obtaining the data subject's consent to use automated scraping tools for training artificial intelligence models or forming databases. Based on this international experience, introducing a specific qualifying offense into administrative legislation will serve to comprehensively protect citizens' data in open sources from spam attacks, phishing, deepfake databases, and unlawful profiling.*

67. Prohibiting the unencrypted storage and transmission of patient medical and biometric data in medical institutions, as well as information and communication systems and platforms within the e-health sector, by making End-to-End Encryption (E2EE) mandatory; and proposing the approval of the “Instruction on Cryptographic Protection and Encryption of Patients' Personal and Medical Data in the Healthcare System and Electronic Medical Databases” by a joint decision of the Ministry of Health, the State Security Service, and the Ministry of Digital Technologies.

For reference:: *In the legislation of the European Union, the United States, and other countries with digitized healthcare systems, patients' medical and biometric data are categorized as “sensitive” data (requiring the highest level of protection), making the use of End-to-End Encryption (E2EE) and cryptographic security tools a mandatory standard for their storage and transmission.*

Specifically, under the US Health Insurance Portability and Accountability Act (HIPAA) and its Security Rule, all electronic protected health information (ePHI) at rest and in transit must be protected using NIST-approved encryption standards (such as AES-256) and secure protocols (TLS 1.3).

Under Articles 9 and 32 of the EU General Data Protection Regulation (GDPR), healthcare entities operating eHealth platforms are required to store medical and biometric data in encrypted and pseudonymized forms based on the principle of “Privacy by Design.”

In the United Kingdom, the Data Security and Protection Toolkit approved by the National Cyber Security Centre (NCSC) and NHS Digital requires end-to-end cryptographic protection (E2EE) across electronic healthcare systems.

Furthermore, in Estonia's e-Health system, patients' digital medical records and biometric data are not only cryptographically encrypted, but access logs are also immutably recorded using blockchain technology (KSI Blockchain).

Applying such international best practices to the national healthcare sector will reliably safeguard medical confidentiality and personal privacy against cyberattacks, mass data leaks, and unauthorized access.

68. Transitioning the State Register of Personal Data Databases of registered owners or operators into an open access mode, enabling citizens to check in real time which organizations are registered to process their data; and to achieve this, it is expedient to amend Article 9 of the Law "On Personal Data" to establish the operation of an open, unified electronic portal of the State Register (personaldata.uz) in real-time mode, as well as to create a mechanism for citizens to search for and verify operators processing their data.

For reference: *In the practice of the European Union, the United Kingdom, and countries with advanced digital governance, the register of personal data database operators is maintained as an open and transparent electronic resource. This allows citizens to verify and access information in real time regarding which legal entities are processing their data.*

Specifically, under Articles 13 and 14 of the EU GDPR and in the practice of national supervisory authorities in EU member states (e.g., France's CNIL, Germany's BfDI), information regarding the status of operators, processing purposes, and Data Protection Officers (DPO) is made available to the public via open online registers.

In the United Kingdom, the Information Commissioner's Office (ICO) maintains a publicly accessible electronic database known as the "Register of fee payers / Data controllers", enabling any citizen to search online and confirm whether a specific company or government agency is legally registered to process personal data.

Furthermore, through the open portal managed by Singapore's PDPC and the "Data Tracker" service within Estonia's "e-Estonia" system, citizens not only view the register of operators but also receive real-time notifications whenever public or private entities request or process their personal data.

Reflecting this international experience in national legislation and within the centralized electronic portal (personaldata.uz) will serve to enhance transparency and accountability in the digital environment, while effectively guaranteeing citizens' right to exercise control over their own data.

69. Strict prohibition must be established against telecommunications operators and providers disclosing subscribers' real-time location and geolocation data (Location-Based Services) to commercial organizations and third parties. To this end, it is necessary to introduce rules into the Law "On Telecommunications", related legislative acts, and licensing terms and conditions stipulating that telecommunications operators and providers are prohibited from selling, transferring for payment, or disclosing free of charge subscriber and user geolocation and network location data to third parties for commercial purposes, with the exception of operational-search activities provided for by law.

For reference: *In the legislation of the European Union, the United States, and countries with advanced digital infrastructure, location and network positioning data of subscribers (Location Data / Cell Tower Logs) maintained by telecommunications operators and providers are classified as specially protected "electronic communications data", and selling or transferring them to third parties for commercial purposes is strictly prohibited.*

Specifically, under the EU ePrivacy Directive (2002/58/EC) and Articles 6 and 9 of the GDPR, location data may only be processed if necessary for service provision or with the subscriber's explicit, informed, and specific opt-in consent; transferring this data to third parties for commercial purposes is banned.

In the United States, the Federal Communications Commission (FCC) and Federal Trade Commission (FTC) have imposed hundreds of millions of dollars in financial penalties on telecom operators (AT&T, Verizon, T-Mobile) for unlawfully selling subscriber geolocation data to commercial data brokers, classifying geolocation as "Customer Proprietary Network Information" (CPNI) under Section 222 of the Communications Act.

In the United Kingdom, under the Investigatory Powers Act 2016 and Privacy and Electronic Communications Regulations (PECR), access to geolocation and traffic data is restricted strictly to authorized state authorities operating under judicial warrants for national security, operational-search, and investigative purposes.

Enshrining this international practice into national telecommunications and licensing legislation will reliably safeguard citizens against unlawful surveillance, intrusive location-based targeted marketing, and violations of personal privacy.

70. Establishing unified standards for the collection, securing, and forensic examination of digital evidence in cases of cybercrime and personal data breaches is necessary; to achieve this, it is proposed to approve the "Unified Methodology for Handling Digital Evidence and Conducting Forensic Computer-Technical Examinations in Cases of Personal Data Legislation Violations and Cybercrime."

For reference: In the practice of countries with advanced digital forensics sectors such as the European Union, the United States, the United Kingdom, and South Korea unified, strictly algorithmized standards (Chain of Custody) govern the collection, securing, preservation, and judicial-procedural examination of digital evidence related to cybercrimes and data breaches.

Specifically, the international standards ISO/IEC 27037 (Guidelines for identification, collection, acquisition, and preservation of digital evidence) and ISO/IEC 27042 (Guidelines for the analysis and interpretation of digital evidence) are globally recognized as the unified methodology for acquiring digital evidence, ensuring source integrity (hash verification), and conducting analysis.

In the United States, based on NIST SP 800-86 (Guide to Integrating Forensic Techniques into Incident Response) and Rule 902 of the Federal Rules of Evidence, the evidence collection process and forensic methodologies are strictly standardized to guarantee that digital evidence is deemed admissible in court.

The European Union's Budapest Convention on Cybercrime, the E-evidence Regulation, and the ACPO Good Practice Guide for Digital Evidence developed by the UK National Police Chiefs' Council define clear stages for conducting forensic computer-technical examinations of log files, server memory (RAM dumps), encrypted traffic, and network packets following data breaches.

Approving a unified methodology in national procedural and sectoral legislation will prevent digital evidence from being falsified or losing its evidentiary value in court due to procedural errors in cases involving cybercrimes and the unlawful dissemination of personal data, while elevating the quality of cyber-forensic examinations to international standards.

71. Granting citizens the right to be informed of the reasons and to demand human review (Human-in-the-loop) when automated AI algorithms reject scoring and bank credit applications; it is necessary to introduce a statutory provision stipulating that in the event of an adverse decision made by automated and artificial intelligence scoring systems, citizens have the right to receive an explanation regarding the logic and reasons behind the decision, as well as the right to request a review of said decision by a human (bank employee).

For reference: *In the legislation and judicial practice of the European Union, the United States, and countries with digitized banking and financial sectors, when decisions affecting human rights and interests are made by artificial intelligence and automated algorithms in critical processes such as scoring, credit allocation, hiring, and insurance, citizens are guaranteed the*

right to know the reasons and logic behind such decisions, as well as the right to demand direct human intervention in reviewing the decision (Human-in-the-loop).

Specifically, under Article 22 of the EU General Data Protection Regulation (GDPR), data subjects have the right not to be subject to a decision based solely on automated processing (including profiling/scoring) that produces legal effects concerning them. The regulation grants citizens the authority to request an explanation of the logic behind the decision ("Right to Explanation") and to require the operator to involve a human in reviewing the decision ("Right to Human Intervention").

A similar principle is provided for under the EU Artificial Intelligence Act (EU AI Act, adopted in 2024), where financial credit and scoring systems are classified as "High-risk AI systems," making human oversight and transparency mandatory conditions.

In the United States, under the Fair Credit Reporting Act (FCRA) and the rules of the Consumer Financial Protection Bureau (CFPB), when banks and financial institutions deny credit based on algorithmic scoring or AI models, they are required to provide consumers with an Adverse Action Notice containing clear, understandable, and reasoned grounds for the rejection, strictly prohibiting sole reliance on "black box" AI algorithms.

Furthermore, mechanisms to appeal and review automated decisions are guaranteed under the UK Data Protection Act 2018 and Canada's PIPEDA legislation. Incorporating such international best practices into national banking and financial legislation as well as personal data protection standards will reliably safeguard citizens against algorithmic discrimination, discriminatory scoring errors, and the opacity of AI systems.

72. Establishing an extrajudicial debt freezing mechanism for online loans fraudulently issued in a citizen's name as a result of leaks of personal or biometric data. Under this mechanism, the law must stipulate that upon submission by the citizen of proof that a fraudulent online loan was issued in their name, that a report was submitted to law enforcement agencies regarding the fraud, and that a criminal case has been initiated, the bank or microfinance organization must immediately suspend the accrual of interest and penalties on said loan, as well as cease all debt collection measures until a final judicial decision in the criminal case is rendered.

For reference: *In countries with advanced banking, fintech, and cybersecurity legislation such as the European Union, the United States, the United Kingdom, and Singapore a legislative mechanism for an automatic and immediate extrajudicial debt freeze ("Credit Freeze" / "Fraud Freeze") is established for loans unlawfully issued in a citizen's name resulting from personal or biometric data leaks, identity theft, or synthetic identity fraud executed via deepfake technologies.*

Specifically, in accordance with the US Fair Credit Reporting Act (FCRA – 15 U.S.C. § 1681c-1) and Federal Trade Commission (FTC) requirements, when a citizen files a report with the police or competent authorities (Identity Theft Report) and presents documentation of a criminal case or investigation, financial institutions are obligated to immediately halt all collection activities and the accrual of interest and penalties.

Under the Mandatory Reimbursement Requirement established by the UK Financial Conduct Authority (FCA), the Monetary Authority of Singapore's (MAS) Shared Responsibility Framework, and Article 18 of the updated EU Consumer Credit Directive II, in cases where a criminal investigation has been initiated, it is strictly prohibited to attribute the debt to the citizen or negatively alter their credit history until investigative and judicial proceedings are concluded.

Applying this experience to national legislation governing banks and microfinance organizations will provide prompt and effective protection for innocent citizens targeted by cyber fraud from bank and collector pressure, as well as financial loss.

73. In order to limit mobile applications from accessing system resources—including contacts, gallery, geolocation, and microphone—that are not directly related to their functional purpose, it is necessary to introduce a provision into the

Law “On the Protection of Consumer Rights” and relevant technical regulations prohibiting developers and providers from requiring consumers to give access to personal data, phone memory, contacts, and media files that are not required for the execution of the core functions of a mobile or digital product.

For reference: *In the European Union, the United States, and leading Asian countries, compelling users to grant mobile applications access to non-essential system resources (contacts, gallery, geolocation, microphone) on their devices is strictly prohibited and regulated based on the principles of “data minimization” and “Privacy by Default.”*

Specifically, under Article 5(1)(c) and Article 25 of the EU GDPR, mobile applications are only entitled to access the minimum data and resources required to fulfill their direct and declared functions. Guidelines enforced by the European Data Protection Board (EDPB) and app store supervisors (Apple App Store & Google Play Store Privacy Guidelines) prohibit demanding unnecessary permissions or denying services when such permissions are withheld (the “take-it-or-leave-it” practice), backed by substantial fines.

In the United States, under Section 5 of the Federal Trade Commission Act (FTC Act – Unfair or Deceptive Acts or Practices) and the California Consumer Privacy Act (CCPA/CPRA), requiring consumers to grant access to contacts, media, and geolocation that are not essential to the core service is recognized as an unfair and deceptive commercial practice.

Furthermore, under the “Provisions on the Necessary Scope of Personal Information Required for Mobile Internet Applications” issued by the Cyberspace Administration of China (CAC), an exhaustive list of necessary permissions is explicitly defined for 39 types of mobile applications (online shopping, fintech, navigation, etc.), prohibiting access to all other system resources.

Incorporating this international practice into national legislation on consumer protection and technical regulation will serve to prevent the covert collection, leakage, and tracking (profiling) of citizens' private photographs, contacts, and audio-video resources via mobile applications.

74. In order to prohibit the mandatory collection of the Personal Identification Number of a Physical Person (PINFL) in everyday, commercial, and non-essential services—including retail trade, marketplaces, and promotional campaigns it is necessary to approve, by a decision of the Cabinet of Ministers, an exhaustive and closed list of spheres and services in which the collection and processing of PINFL data by state and commercial organizations is permitted.

For reference: *In the legislation of countries with advanced digital identity systems such as the European Union, the United States, South Korea, and Scandinavian nations the collection of national or single identification numbers (Social Security Number – SSN, National Identity Number, PIN) in everyday, commercial, and retail spheres (marketplaces, bonus and promotional programs, online shopping) is strictly prohibited, and their processing is permitted solely within a closed list of spheres and services established by law.*

Specifically, under Article 87 of the EU GDPR, the processing of national identification numbers is subject to a specific regime, requiring EU member states to apply it only in vital areas such as public administration, taxation, pensions, and banking/finance. In Finland and Sweden, requesting a national identification number for routine commercial services or marketplaces is deemed a severe violation of the principle of “data minimization”.

In South Korea, under Article 24-2 of the Personal Information Protection Act (PIPA), collecting and processing citizens' Resident Registration Numbers (RRN) in any service provision outside the notary and financial sectors—including e-commerce and retail—is strictly prohibited and subject to heavy financial sanctions.

In the United States, under the Privacy Act and the Social Security Number Protection Act, requiring or publicly displaying an SSN in the private sector, routine retail, or promotional campaigns is recognized as an unlawful act.

Establishing a sectoral and closed list of permitted spheres for collecting PINFL data based on this international experience is crucial to preventing mass leaks, profiling, and fraudulent misuse of citizens' single identifiers through the databases of marketplaces, lotteries, and retail chains.

75. To make remote and mass access to personal data databases by law enforcement agencies during operational-search and investigative activities subject to judicial authorization, it is necessary to introduce a procedure into the Code of Criminal Procedure and the Law "On Operational-Search Activity" stipulating that remote or mass access to digital and electronic personal data databases and telecom operators' data repositories by operational-search and investigative bodies, as well as obtaining data therefrom, may only be executed on the basis of a judge's warrant (decision).

For reference: *In the procedural legislation and judicial practice of democratic states adhering to the rule of law—such as the European Union, the United States, the United Kingdom, and South Korea—remote, mass, or direct access by law enforcement agencies to operators' and private-sector personal data databases, telecommunications, and internet traffic repositories is strictly restricted by prior judicial warrants.*

Specifically, according to landmark rulings of the European Court of Human Rights (ECtHR — Big Brother Watch and Others v. the UK, Roman Zakharov v. Russia) and conclusions of the Court of Justice of the European Union (CJEU — Digital Rights Ireland, SpaceNet), granting state bodies unrestricted, automated, or mass access to telecommunications and digital databases is held to be entirely incompatible with Article 8 of the European Convention on Human Rights (right to respect for private and family life).

Under the EU Data Protection Law Enforcement Directive (LED 2016/680), access to digital databases by investigative authorities is permitted only under a specific court decision in the presence of an active criminal case, a specific individual, and reasonable suspicion.

In the United States, under the Fourth Amendment to the US Constitution and the Supreme Court's landmark decision in Carpenter v. United States (2018), government acquisition of telecommunications and geolocation data repositories without a judicial warrant (probable cause warrant) is deemed a violation of constitutional rights.

In the United Kingdom, under the Investigatory Powers Act 2016 (IPA), access to digital databases and telecommunications networks must pass a two-step approval process (a "double lock" mechanism) involving the Investigatory Powers Commissioner and an independent judge.

Incorporating these international legal standards into the national Code of Criminal Procedure and operational-search legislation will prevent disproportionate or unchecked interference by state bodies into citizens' digital footprints and personal data, elevating judicial authorization guarantees to a new level in the digital age.

76. In order to introduce a mandatory insurance practice covering cyber risks and compensation for damages resulting from personal data leaks for operators processing large volumes of personal data databases specifically data belonging to 100,000 or more citizens it is necessary to introduce provisions into the Law "On Insurance Activity" and the Law "On Personal Data" requiring operators processing personal data of over 100,000 data subjects to maintain a mandatory cyber-insurance contract for compensating damages caused to third parties due to personal data leaks.

For reference: *In the legislation and insurance markets of countries with large digital economies and data infrastructures—such as the European Union, the United States, the United Kingdom, and Singapore—cyber insurance (Cyber Insurance) aimed at covering cyber risks and*

damages resulting from data breaches for operators and organizations handling large-scale personal data databases (Big Data) is widely utilized as one of the most effective financial and legal mechanisms.

Specifically, Article 82 of the EU GDPR imposes an obligation on operators to fully compensate citizens who have suffered material or non-material damage due to data leaks; consequently, in the EU, holding a Cyber Liability Insurance policy is required by regulatory bodies and auditors as a mandatory Risk Management standard for telecom, banking, fintech, and healthcare operators managing databases of more than 100,000 subjects.

In the United States, under state legislation (for instance, California's CCPA/CPRA) and Federal Trade Commission (FTC) requirements, the obligation to compensate citizens for damages caused by mass leaks (identity theft, financial losses, and legal costs) as well as providing credit monitoring services to victims rests entirely on the operator, forcing large data operators to enter into multi-million dollar cyber-insurance contracts.

Under Singapore's Personal Data Protection Act (PDPA) and Cybersecurity Act, operators of Critical Information Infrastructure (CII) and large databases are obligated to implement financial coverage and insurance mechanisms to remedy the consequences of personal data breaches.

Incorporating this international experience into national insurance and personal data protection legislation will incentivize operators handling data of over 100,000 citizens to strengthen their cybersecurity systems while ensuring guaranteed and prompt payout of insurance coverage to citizens for material and non-material damage in the event of mass leaks.

77. In order to strengthen the level of protection of learners' personal data in digital educational platforms across higher and specialized secondary educational institutions, it is necessary to approve the “Instruction on the Protection and Security of Learners' Personal Data in Educational Institutions and Their Digital Systems” by a joint decision of the Ministry of Higher Education, Science and Innovations, the Ministry of Preschool and School Education, as well as the State Security Service, the Ministry of Internal Affairs, and the Ministry of Digital Technologies.

For reference: *In the legislation and technical standards of countries with rapidly developing digital education and EdTech sectors—such as the European Union, the United States, the United Kingdom, and South Korea—special departmental and sectoral security instructions and regulations apply to protect the personal and biometric data of learners (students, pupils, and minors) across digital platforms, Learning Management Systems (LMS), and proctoring systems.*

Specifically, in the United States, based on the Family Educational Rights and Privacy Act (FERPA) and the Children's Online Privacy Protection Act (COPPA), the Department of Education and the Federal Trade Commission (FTC) have established special security guidelines (K-12 and Higher Ed Cybersecurity Guidelines) for higher and secondary educational institutions and digital platforms. Under these guidelines, disclosing learners' grades, academic history, and personal data to third parties, as well as using such data for commercial profiling or advertising, is strictly prohibited.

In the European Union, in accordance with Article 8 of the GDPR concerning minors' data and the recommendations of the European Data Protection Board (EDPB), biometric (facial recognition), audio-video, and geolocation data collected on distance learning and online exam (proctoring) platforms must be collected strictly to the minimum extent necessary (data minimization) solely for the educational process and automatically erased once the necessary period expires.

In South Korea, under the “Personal Information Processing and Security Guidelines for the Educational Sector” adopted by the Ministry of Education and the Personal Information Protection Commission (PIPC), all school and university platforms, digital textbooks, and online evaluation systems are mandated to undergo cybersecurity audits at least once a year and strictly adhere to encryption standards.

Approving a sectoral and departmental protection Instruction for the national education system based on this international practice will play a crucial role in preventing data leaks and the unauthorized use of young people's, students', and pupils' personal data, online exam biometrics, and academic databases via digital educational platforms, while establishing a comprehensive cybersecurity environment across the digital infrastructure of educational institutions.

78. In order to ensure mandatory notification of users and to provide them with the ability to opt out when utilizing tracking cookies and scripts on websites, it is necessary to introduce a provision into Article 18 of the Law "On Personal Data" stipulating that the use of online identifiers, tracking scripts, and cookies on web resources is permitted only after users are provided with an easy and free mechanism to opt out of the use of such files and scripts.

For reference: *In jurisdictions with advanced digital privacy and web technology regulations such as the European Union, the United Kingdom, the United States, and California the use of online identifiers, behavior tracking scripts, and tracking cookies by web resources and platforms is strictly regulated at the source.*

Specifically, in accordance with Article 5 of the EU ePrivacy Directive (2002/58/EC) and the requirements of the GDPR, websites and online platforms must obtain active, freely given, and explicit opt-in consent from the user before launching non-essential (functional, analytical, advertising, and tracking) cookies and scripts.

Based on rulings by the European Data Protection Board (EDPB) and the Court of Justice of the European Union (CJEU — Planet49), methods such as pre-ticked boxes, mandatory banners, or implied consent schemes like "continuing to use the site constitutes consent" (Dark Patterns) are recognized as strictly unlawful. Furthermore, websites are mandated to offer a "Reject All" option that is as visually prominent, easy, and accessible in a single click (one-step) as the "Accept All" option.

Under the UK Information Commissioner's Office (ICO) guidelines and the California Consumer Privacy Act (CCPA/CPRA) in the US, websites are required to provide a free and unobstructed mechanism on their homepages granting users the right to restrict the tracking and sale of their data ("Do Not Sell or Share My Personal Information").

Incorporating these international legal and technical standards into the Law "On Personal Data" will curb practices such as systematic profiling without users' knowledge or consent, harvesting data on personal interests and behavior, and transferring online identifiers to third parties, thereby effectively safeguarding citizens' digital privacy across the national web sector.

79. In order to ensure the automatic anonymization of personal data belonging to parties and procedural participants in court decisions published in open court registers and information systems using artificial intelligence-based de-identification systems, it is necessary to introduce provisions into the Code of Criminal Procedure, Code of Civil Procedure, Code of Economic Procedure, and the Code of Administrative Responsibility prescribing a procedure for placing court decisions and procedural documents in open information sources only after being processed by software tools that automatically anonymize and de-identify personal data and eliminate the risk of re-identification.

For reference: *In countries with developed legislation ensuring judicial openness and transparency while safeguarding personal privacy and reputation such as the European Union, the United States, the United Kingdom, and South Korea anonymization and de-identification (pseudonymization / de-identification) of personal data in court decisions published in open registers is an absolutely mandatory procedural and technical standard.*

Specifically, under Articles 6 and 89 of the GDPR and Council of Europe guidelines on the digitalization of justice, in the practice of the Court of Justice of the European Union (CJEU) and

Supreme Courts of EU member states (Germany, France, Netherlands), the names, addresses, and identifiers of parties, witnesses, and victims in all publicly released court decisions are automatically de-identified. Judicial departments in France and Netherlands have implemented specialized Natural Language Processing (NLP) and AI algorithms to detect and anonymize personal data from texts, reducing the real-time risk of re-identification attacks (or the mosaic effect) to zero.

In US federal and state courts (PACER / CM/ECF systems), under the Federal Rules of Civil Procedure (Rule 5.2) and Federal Rules of Criminal Procedure (Rule 49.1), redacting personal identification numbers (SSNs), dates of birth, names of minors, and financial account numbers in publicly released procedural documents is a procedural duty imposed on attorneys and court clerks, non-compliance with which is treated as contempt of court.

In the United Kingdom (The National Archives – Court Decisions Database), AI systems are utilized to auto-anonymize contextual information that could potentially lead to re-identification.

Incorporating this international procedural and technical experience into the national Criminal Procedure Code, Civil Procedure Code, Economic Procedure Code, and Code of Administrative Responsibility will maintain judicial openness and transparency while preventing citizens' private personal secrets, medical, financial, and family data from being publicly exposed online or resulting in digital stigma through open judicial records.

80. In order to prohibit the storage and processing of genetic data on foreign servers by private medical institutions and laboratories conducting DNA and genetic testing, it is necessary to introduce a condition into the licensing requirements for medical and laboratory activities prohibiting the storage and processing of data obtained from DNA and genetic materials of citizens of the Republic of Uzbekistan on foreign servers and cloud hostings, as well as the transfer of such data to foreign genomics centers.

For reference: *In the legislation and licensing standards of nations that prioritize national biosecurity and the protection of genomic data such as the European Union, the United States, China, South Korea, and France human DNA, RNA, and genomic sequencing data are regulated under a special regime as integral components of national sovereignty and biosecurity.*

Specifically, Article 9 of the EU GDPR classifies genetic data as a special category of data subject to heightened protection. Under France's Bioethics Law (Loi de bioéthique), Public Health Code, and Tax Code, laboratories and medical centers conducting genetic testing are strictly prohibited from storing citizens' genetic data on cloud servers located outside the country or transferring it cross-border; this condition serves as a core requirement for granting a medical license.

In the United States, under the Health Insurance Portability and Accountability Act (HIPAA Privacy Rule), Executive Order 14117 (Preventing Access to Americans' Bulk Sensitive Personal Data, 2024), and the BIOSECURE Act, processing bulk DNA and genetic data of Americans at foreign genomics centers, foreign servers, and hostings is declared a threat to national security.

In China, under the Regulations on the Management of Human Genetic Resources and the Data Security Law (DSL), exporting, processing on foreign servers, or unlawfully transferring digitized DNA data and genetic materials of Chinese citizens outside the country by private or public laboratories incurs criminal liability.

In France, Germany, and South Korea, licensing terms compel medical laboratories to store genomic sequencing data exclusively in certified Local Sovereign Data Centers.

Introducing a provision into medical and laboratory licensing requirements based on this international practice prohibiting the transfer of DNA and genetic data to foreign servers, cloud hostings, and foreign genomics centers will ensure the reliable protection of Uzbekistan citizens'

genetic passports, genomic databases, and biological security against external information threats and bio-strategic risks.

81. In order to identify operators of illegal bots on Telegram and other messengers that allow searches using individuals' phone numbers, passport details, and vehicle license plate numbers, as well as to bring them to administrative or criminal liability under the law, it is necessary to establish an operational mechanism involving the Ministry of Internal Affairs, the State Security Service, and the Cybersecurity Center to detect and block illegal OSINT bots and "probiv" (data-lookup) services, ensuring the enforcement of liability measures against their operators under Article 46^2 of the Code of Administrative Responsibility and Article 141^2 of the Criminal Code.

For reference: *In the criminal law and investigative practices of jurisdictions where cybercrime prevention and the regulation of illegal personal data trafficking are well-established such as the European Union, the United States, the United Kingdom, and Singapore taking systematic and rapid action against illegal "probiv" services on messaging platforms (Telegram, etc.) and darknet sources, OSINT bots (Doxxing / Data Broker Bots), and the trade of leaked databases is designated as a mandatory function of state cybersecurity and law enforcement agencies.*

Specifically, under the European Union's Budapest Convention on Cybercrime and through specialized operational bodies of Europol (Europol EC3 – European Cybercrime Centre), Telegram bots and aggregators distributing citizens' personal and biometric data, vehicle registries, and financial records for commercial or illegal purposes are blocked without delay, and their creators and operators face criminal charges for mass privacy violations and cybercrime.

In the United States, the Federal Bureau of Investigation (FBI Cyber Division) and the Department of Justice (DOJ), acting under the Computer Fraud and Abuse Act (CFAA, 18 U.S.C. § 1030) and the Identity Theft and Assumption Deterrence Act, execute seizures of domain and bot infrastructure used for mass lookups while applying severe financial and criminal sanctions against operators.

In the United Kingdom, the National Cyber Security Centre (NCSC) and the National Crime Agency (NCA), operating under direct Notice and Takedown procedures with application providers and Telegram management, automatically block bots that enable the illegal searching (OSINT) of citizens' phone numbers, passport information, or residential addresses.

In Singapore, under the Protection from Online Falsehoods and Manipulation Act and the Online Safety Act, the police Cybercrime Unit is authorized to issue rapid Blocking Orders targeting bots integrated with illicit databases.

Integrating this international operational-investigative and forensic experience into the practices of the Ministry of Internal Affairs, the State Security Service, and the Cybersecurity Center will eradicate the proliferation of illegal OSINT bots and lookup services on Telegram and other messengers, guarantee the inevitability of penalty enforcement under Article 46² of the Code of Administrative Responsibility and Article 141² of the Criminal Code, and effectively safeguard citizens against digital harassment (Doxxing / Cyberstalking) and fraud risks.

82. In order to impose an obligation on hosting providers and cloud service operators to immediately freeze illegal personal data databases detected on their servers and notify the competent authority, it is necessary to introduce a provision into the Law "On Informatization" requiring hosting and cloud service providers to freeze such resources and restrict access to them within 24 hours of receiving a notification from the competent authority regarding the storage or dissemination of illegal personal data databases on their information resources.

For reference: *In jurisdictions with major data centers and cloud infrastructure such as the European Union, the United States, the United Kingdom, and Singapore holding hosting and cloud service providers (Cloud Service Providers / Hosting Providers) accountable under a "Notice and Takedown" or "Notice and Action" obligation to immediately freeze, restrict access to, and alert regulatory authorities upon detecting illicit personal data or mass leaked databases on their servers is enshrined in law.*

Specifically, under the EU Digital Services Act (DSA 2022, Articles 6, 9, and 16) and GDPR requirements, hosting and cloud providers must block access to illicit resources and data immediately (in practice, within 24 hours) upon receiving notice from a competent authority or data subject regarding the storage of illegal content or personal data databases. Failure to comply strips the provider of its safe harbor liability immunity and subjects it to substantial financial penalties as an accomplice in distributing illegal data.

In the United States, under the legal framework for online copyright and digital privacy protection along with principles applied by the Federal Trade Commission (FTC), server operators hosting leaked personal and financial databases are required to localize or remove them promptly upon receiving notification.

Under the UK Online Safety Act 2023 and Ofcom regulatory standards, cloud service providers (AWS, Azure, Google Cloud, and local hostings) are mandated to follow a strict 24-hour response algorithm for identifying and freezing illegal personal data stores.

Singapore's Personal Data Protection Act (PDPA) similarly demands immediate and full compliance with directives issued by the competent authority (PDPC) to suspend and block illegal databases maintained on hosting servers.

Introducing this international legal standard into the Law "On Informatization" will enhance the accountability of hosting and cloud providers, ensure that illegal personal data stores and leaked databases are frozen within 24 hours and restricted across the information space without delay, and reliably strengthen national cybersecurity and citizens' digital privacy.

83. In order to limit the retention period of biometric video stream data obtained through Face-ID and surveillance video systems in public places specifically, establishing a procedure to retain such data for no more than 30 days and automatically delete it upon expiration of this period it is necessary to approve, by a decision of the Cabinet of Ministers, a Special Regulation providing for the procedure of storing, utilizing, and automatically destroying biometric information (video streams) obtained through "Safe City" systems and public surveillance equipment after the specified retention period expires.

For reference: *In jurisdictions that prioritize human rights and biometric data protection such as the European Union, the United Kingdom, the United States, and South Korea the retention periods for video streams and biometric images obtained through public video surveillance and Face-ID systems are strictly limited by law and sectoral regulations, making automatic and irreversible erasure (Automatic Erasure / Purging) mandatory upon expiration.*

Specifically, in the European Union, under Article 5 of the GDPR (the "Storage Limitation" principle) and the guidelines of the European Data Protection Board (EDPB Guidelines 3/2019 on processing of personal data through video devices), the retention period for video recordings in public places and "Safe City" systems is set to not exceed 30 days by default. Unless investigative proceedings have been initiated for a specific crime or administrative offense, video streams must be automatically deleted from the system once the 30-day period expires. Furthermore, under Article 5 of the EU AI Act (2024), the use of Real-time Remote Biometric Identification systems in public spaces is severely restricted, and unjustified, long-term storage of collected biometric images is prohibited.

In the United Kingdom, pursuant to the Investigatory Powers Act and the Surveillance Camera Code of Practice, images from public surveillance cameras and Face-ID streams are retained for a maximum of 31 days, after which auto-deletion is mandatory.

Under Article 25 of South Korea's Personal Information Protection Act (PIPA) and Cabinet regulations on managing video materials in public areas, the retention limit for CCTV and Face-ID data is established at 30 days, with heavy financial fines imposed for retaining data beyond this period or failing to erase it on time.

Approving a Special Regulation based on this international legal and technical experience to cap the retention period of biometric video streams in "Safe City" and public surveillance systems at 30 days and mandate their automatic destruction will protect citizens' constitutional rights to personal privacy and freedom of movement, prevent mass surveillance risks, and ensure the secure management of digital video data repositories.

84. In order to guarantee citizens the right to withdraw previously given consent for the processing of their personal data at any time through a simplified procedure including via a single click, SMS, or personal user account it is necessary to introduce a provision into Article 19 of the Law "On Personal Data" stipulating that data subjects have the right to revoke (withdraw) their previously given consent for personal data processing at any time, and that the procedure and interface for withdrawing consent must not be more complex than the procedure for granting it.

For reference: *In jurisdictions with advanced data protection legislation such as the European Union, the United States (California), the United Kingdom, and Singapore a citizen's right to withdraw (revoke) previously granted consent for personal data processing represents a critical guarantee of information sovereignty and personal privacy. A fundamental principle embedded in these legal frameworks is that "withdrawal of consent must be as easy as giving consent".*

Specifically, under Article 7(3) of the EU General Data Protection Regulation (GDPR), data subjects have the right to withdraw their consent at any time, and this process must be identical in form and convenience (simplified) to the process of granting consent. If consent was obtained via a single click on a website or mobile application or via SMS, the operator is obligated to provide the withdrawal option through the exact same interface (e.g., a single click, a button in a personal account, or a reply SMS). Creating dark patterns or artificial obstacles to complicate consent withdrawal leads to severe administrative fines under the GDPR.

Guidelines from the UK Data Protection Act 2018 and the Information Commissioner's Office (ICO) similarly mandate that consent withdrawal buttons must be clearly and conveniently positioned within the user interface.

Under California's CCPA/CPRA, websites are required to provide a clear homepage hyperlink ("Do Not Sell or Share My Personal Information") as a single-click mechanism for users to revoke consent and restrict data usage.

Under Section 16 of Singapore's Personal Data Protection Act (PDPA), upon receiving a notice of consent withdrawal, the operator must immediately cease data collection and processing without imposing unnecessary bureaucratic hurdles.

Incorporating this international standard into Article 19 of the Law "On Personal Data" will ensure that citizens maintain complete control over their digital footprints and personal data while curbing unauthorized data misuse by operators.

85. In order to prohibit the collection of excessive personal data such as drivers' passport details, PINFL, and other unnecessary personal data in parking lots and toll roads in addition to vehicle license plate numbers, it is necessary to approve the "Data Minimization Standard for Collecting Personal Data in Transport and Parking Infrastructure" by a joint decision of the Ministry of Transport and the Ministry of Digital Technologies.

It is advisable to clearly specify the following conditions in the developed "Data Minimization Standard for Collecting Personal Data in Transport and Parking Infrastructure":

- **Sole Permissible Automatic Identifier:**
  - Vehicle license plate number (via Automatic Number Plate Recognition cameras – ANPR).
- **Prohibited Data Scope:**
  - Passport/ID-card details of the driver or owner;
  - PINFL (Personal Identification Number of a Physical Person);
  - Driver's license series and number;
  - Mandatory collection and storage of biological/biometric data through facial recognition.
- **Exceptions (Exempted Procedure):**
  - Integration with special security systems at the request of competent law enforcement agencies within the framework of combating administrative offenses or crime is exempted (even in this case, public parking operators shall not retain the PINFL themselves, but rather interact with the unified database of competent authorities via secure API).
- **Data Retention Period:**
  - After a vehicle departs the parking lot and payment is successfully processed, transaction logs associated with the used license plate number must be retained temporarily (e.g., 30 or 90 days) solely in compliance with financial auditing requirements, followed by mandatory automatic deletion (anonymization).

For reference: *In advanced jurisdictions such as the European Union (Article 5(1)(c) and (e) of the GDPR), the United States (California – CCPA/CPRA), the United Kingdom (ICO), and Singapore (Section 16 of the PDPA), the principles of "Data Minimization" and "Storage Limitation" are strictly enforced within transport and parking infrastructure. According to international standards, parking and toll road operators must limit their service operations to registering only a single minimal and proportionate identifier the license plate number via ANPR. Mass collection and storage of a driver's PINFL, passport/ID card details, or biometric data via facial recognition is deemed a disproportionate infringement on personal privacy. Furthermore, per UK ICO guidelines, upon completion of payment and service, transaction data must be stored for a limited period solely for financial audit purposes and subsequently automatically erased or anonymized under a strict Data Retention policy. Introducing this national standard will prevent risks of mass personal data breaches in transport infrastructure and ensure secure digital identification.*

86. In order to restrict the disclosure of suspects' and defendants' honor, dignity, and personal data in the mass media and social networks prior to a court verdict entering into legal force, it is necessary to introduce a provision into the Law "On Mass Media", the Law "On Informatization", and Article 46^2 of the Code of Administrative Responsibility prohibiting the dissemination of personal data, facial images, and direct identifying features of suspects or defendants by mass media, internet users, journalists, and bloggers without their consent before a lawful court verdict is passed, except in cases provided by law.

For reference: *In advanced jurisdictions such as the European Union (Article 6 of the General Data Protection Regulation – GDPR and Directive 2016/680), the United States (international human rights precedents), the United Kingdom (Contempt of Court Act 1981 and*

Data Protection Act 2018), and Singapore (Administration of Justice (Protection) Act), the "presumption of innocence" and the "right to privacy" are recognized as inextricably linked fundamental principles. According to international standards, publicly portraying a person as a "criminal", or disclosing their facial image, full name, place of residence, and other identifying information in the media and social networks before a final guilty verdict takes legal effect is strictly prohibited. International practice (specifically in German and French law) mandates that facial images of individuals suspected of committing crimes be blurred and their names anonymized (showing only the first letter of the surname) in media coverage. Violations of these requirements by media outlets or bloggers inflict irreparable moral damage on a person's honor and dignity and are treated as unlawful interference with the administration of justice. Incorporating these provisions will practically guarantee citizens' constitutional protections regarding the presumption of innocence and their fundamental right to privacy.

87. In order to establish a procedure for processing, storing, closing, deleting, or managing a deceased person's personal data, digital assets, electronic accounts, and digital profiles by heirs in accordance with the law, it is necessary to introduce provisions into the Civil Code and the Law "On Personal Data" prescribing the legal status of a deceased person's personal data, digital assets, electronic accounts, and digital profiles, the procedure for processing, storing, deleting, or managing them, as well as the grounds and conditions for transferring these rights to heirs by will or by law.

Under these provisions, a deceased person's digital assets and related property rights must be included in the estate in accordance with the law, while access to personal data, electronic accounts, and digital profiles must be granted on the basis of documents confirming inheritance rights, taking into account the expressed will of the deceased, their right to personal privacy, and the rights and legitimate interests of third parties.

For reference: *In advanced jurisdictions such as the European Union (GDPR and France's 2016 Digital Republic Act), the United States (Revised Uniform Fiduciary Access to Digital Assets Act – RUFADAA), and through precedents set by the Supreme Courts of the United Kingdom and France, the status of a deceased person's "digital estate" and personal data is regulated by law.*

Under international standards, digital assets (crypto-assets, monetized accounts, domains, and copyrights) are fully included in the estate as property rights. However, heirs' access to non-property electronic accounts, social media profiles, and personal correspondence (e-mails, instant messengers) is limited by the deceased person's lifetime instructions (post-mortem privacy instructions) as well as third parties' rights to confidentiality and privacy.

Legislation in France and the United States grants citizens the right to give advance instructions to convert their accounts to "memorialized status", delete them, or entrust their management to a designated representative upon death.

88. In the context of rapid developments in artificial intelligence and digital transformation in the Republic of Uzbekistan, it is necessary to adopt the National Cyberalogy and Digital Privacy Strategy for 2026–2030 to comprehensively ensure the protection of personal data, cybersecurity, and formulate a unified state policy on digital rights protection.

To this end, it is proposed to draft and submit a Draft Decree of the President of the Republic of Uzbekistan "On Approval of the National Strategy for Comprehensively Ensuring the Protection of Personal Data in the Era of Artificial Intelligence and Digital Transformation for 2026–2030";

For reference: *In advanced jurisdictions such as the European Union (EU AI Act, GDPR, and European Digital Rights Declaration), the United States (Blueprint for an AI Bill of Rights and NIST AI Risk Management Framework), the United Kingdom (National AI Strategy and Data Protection and Digital Information Framework), and Singapore (Model AI Governance Framework and National AI Strategy 2.0), protecting personal data during the expansion of artificial intelligence (AI) and digitalization is regulated at a strategic level.*

According to international experience, ensuring citizens' personal privacy, digital sovereignty, and algorithmic transparency and accountability when using massive datasets (Big Data) to train machine learning algorithms represents a key priority.

In the aforementioned jurisdictions, mechanisms have been established to prevent bias and discrimination when processing personal data through AI systems, implement differential privacy standards, and perform early risk assessments based on the concept of "cyberalogy" an interdisciplinary analytical domain linking technical and legal fields.

89. In order to ensure the confidentiality of personal data and strengthen cybersecurity in the context of rapid developments in artificial intelligence and digital transformation, it is proposed to introduce a system of data classification and digital marking (data tagging) within the technical protection measures provided for in Article 27 of the Law "On Personal Data".

For information: *In jurisdictions such as the European Union (GDPR), the United States (NIST SP 800-60 and CUI), and Singapore (PDPC), the protection of personal data is executed by categorizing data according to its sensitivity level (public, confidential, special/sensitive) and applying metadata tagging at both software and system levels. Implementing these technical and organizational measures serves to automatically prevent unauthorized access and mitigate the risk of data leaks.*

LIST OF REFERENCES

1. Constitution of the Republic of Uzbekistan // lex.uz – National Database of Legislation of the Republic of Uzbekistan.
2. Criminal Code of the Republic of Uzbekistan // lex.uz – National Database of Legislation of the Republic of Uzbekistan.
3. Law of the Republic of Uzbekistan “On Informatization” dated December 11, 2003, № 560-II // lex.uz – National Database of Legislation of the Republic of Uzbekistan.
4. Law of the Republic of Uzbekistan “On Personal Data” dated July 2, 2019, № LRU-547 // lex.uz – National Database of Legislation of the Republic of Uzbekistan.
5. Law of the Republic of Uzbekistan “On Amendments and Additions to the Law of the Republic of Uzbekistan 'On Mass Media'” dated January 15, 2007, № LRU-78 // lex.uz – National Database of Legislation of the Republic of Uzbekistan.
6. Law of the Republic of Uzbekistan “On Regulatory Legal Acts” dated April 20, 2021, № LRU-682 // lex.uz – National Database of Legislation of the Republic of Uzbekistan.
7. Law of the Republic of Uzbekistan “On Telecommunications” dated December 27, 2024, № LRU-1015 // lex.uz – National Database of Legislation of the Republic of Uzbekistan.
8. Resolution of the Cabinet of Ministers “On Approval of the List of Foreign States Ensuring Equal Protection of Personal Data” dated July 29, 2026, № 415 // lex.uz – National Database of Legislation of the Republic of Uzbekistan.
9. Regulation “On Requirements for Physical Media Containing Biometric and Genetic Data and Technologies for Storing Such Data Outside Personal Data Databases”, approved by Resolution of the Cabinet of Ministers dated October 5, 2022, № 570 // lex.uz – National Database of Legislation of the Republic of Uzbekistan.
10. Administrative Regulation on Rendering Public Services for Maintaining the State Register of Personal Data Databases, approved by Resolution of the Cabinet of Ministers dated February 8, 2020, № 71 // lex.uz – National Database of Legislation of the Republic of Uzbekistan.
11. Resolution of the Cabinet of Ministers “On Approval of Certain Regulatory Legal Acts in the Field of Personal Data Processing” dated October 5, 2022, № 570 // lex.uz – National Database of Legislation of the Republic of Uzbekistan.
12. Model Procedure for Personal Data Processing, approved by Order of the Minister of Justice of the Republic of Uzbekistan dated November 15, 2023, № 20-mh (registered on Nov 15, 2023, Reg. № 3478) // lex.uz – National Database of Legislation of the Republic of Uzbekistan.
13. Model Procedure for Organizing the Activities of a Structural Unit or Authorized Person Ensuring the Processing and Protection of Personal Data of the Owner and (or) Operator of a Personal Data Database, approved by Order of the

Minister of Justice of the Republic of Uzbekistan dated November 14, 2023, № 19-mh (registered on Nov 15, 2023, Reg. № 3477) // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

14. Regulation “On the Procedure for Exercising State Control over Compliance with Special Conditions for Processing Personal Data of Citizens of the Republic of Uzbekistan”, approved by Resolution of the Cabinet of Ministers dated September 5, 2018, № 707 // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

15. Rules for the Provision of Telecommunications Services, approved by Order of the Minister of Digital Technologies of the Republic of Uzbekistan dated January 6, 2026, № 287-mh (registered on Jan 26, 2026, Reg. № 3762) // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

16. Ғ. Мирзо. Шахсга доир маълумотлар ҳимояси: халқаро ҳуқуқ, миллий қонунчилик ва амалий тажриба. – Т.: “Куч-адолатда” газетаси, 2023 йил 27 январь 4-сон // http://pravacheloveka.uz/uz/news/m9732.

17. А. Савельев Проблемы применения законодательства о персональных данных в эпоху «Больших данных» (Big Data) // Право. Журнал Высшей школы экономики. 2015. №1. URL: https://cyberleninka.ru/article/n/problemy-primeneniya-zakonodatelstva-o-personalnyh-dannyh-v-epohu-bolshih-dannyh-big-data.

18. Бачило, И. Л. Б32 Информационное право : учебник для магистров / И. Л. Бачило. — 3-е изд., перераб. и доп. — М. : Издательство Юрайт, 2015. — 564 с.

19. Paul M. Schwartz ва Daniel J. Solove. The PII Problem: Privacy and a New Concept of Personally Identifiable Information. New York University Law Review, Vol. 86, p. 1814, 2011.

20. Л. Терещенко. Правовой режим информации. Диссертация. – Москва, 2011. - 55 с.

21. Arthur R. Miller, The Assault on Privacy, 15 Law Quadrangle (formerly Law Quad Notes) - (1970). Available at: https://repository.law.umich.edu/lqnotes/vol15/iss2/6.

22. https://eur-lex.europa.eu/eli/reg/2016/679/oj.

23. https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai.

24. https://reestr.uz/kr/projects/1376?type=passport.

25. https://my.gov.uz/uz/reyestr?limit=30&service_type=electronic.

26. https://my.gov.uz/uz/statistics.

27. https://my.gov.uz/uz/for-foreigners.

28. https://my.gov.uz/uz.

29. https://my.gov.uz/uz/page/mission.

Annex 1

SCHEME
for the Procedure for Including and Removing Owners and (or) Operators Who Have Violated Special Conditions for Processing Personal Data of Citizens of the Republic of Uzbekistan in and from the Register of Violators of Rights of Personal Data Subjects

Stage	Subject	Measures	Implementation Deadline
Stage 1	Center for Mass Communications and the competent state authority in the field of personal data	Conducts monitoring of the activities of owners and (or) operators processing personal data on the World Wide Web in order to identify violations of the special conditions for processing the personal data of citizens of the Republic of Uzbekistan.	Continuously
	Legal entities or individuals	Submitting information to the Center in accordance with established procedures, including by filing an application regarding organizations processing personal data on websites and (or) website pages and resources of the Internet where violations of the special conditions for processing personal data are present under the legislation of the Republic of Uzbekistan.	Continuously
Stage 2	Center for Mass Communications	Upon identifying instances where owners and (or) operators processing personal data on the World Wide Web violate the special conditions for processing the personal data of citizens of the Republic of Uzbekistan using information technologies, including on the World Wide Web, submits information to the competent state authority in the field of personal data to issue an expert opinion.	Within 24 hours from the moment of identification
	Competent state authority in the field of personal data	Upon receiving the information submitted by the Center, the competent state authority in the field of personal	Within 24 hours from the moment of identification

		data provides the “Uzcomnazorat” State Inspectorate with an expert opinion regarding the violation of special conditions for processing the personal data of citizens of the Republic of Uzbekistan by owners and (or) operators processing personal data.	
Stage 3	“Uzcomnazorat” State Inspectorate	Issues an appropriate binding instruction to the owner or operator of the personal data database specifying a precise timeframe to remedy the deficiencies identified on the basis of the submitted expert opinion.	Within one day from the date of receipt of the opinion
	Owner or operator of the personal data database	The owner or operator of the personal data database takes measures to remedy the deficiencies specified in the instruction and submits information to the “Uzcomnazorat” State Inspectorate in a timely manner.	Within the timeframes specified in the representation
Stage 4	“Uzcomnazorat” State Inspectorate	In the event that the violations specified in the instruction are not remedied within the period set forth in the instruction, information regarding the owner and (or) operator of the personal data database is entered into the “Register of Violators of Rights of Personal Data Subjects”.	After the expiration of the period specified in the instruction
Stage 5	“Uzcomnazorat” State Inspectorate	Following the entry into the “Register of Violators of Rights of Personal Data Subjects”, submits a representation to the Ministry for Development of Information Technologies and Communications to restrict access to the Internet information resources of the owner or operator of the personal data database.	Within 12 hours
	Ministry for Development of Information	Following the entry into the “Register of Violators of Rights of Personal Data Subjects”, executes	Within 12 hours

	Technologies and Communications	the restriction of access to the Internet information resources of the owner or operator of the personal data database.	
Stage 6	Center for Mass Communications and the competent state authority in the field of personal data	The competent state authority in the field of personal data, in cooperation with the Center, examines the information provided by the owner and (or) operator regarding the remediation of deficiencies on the Internet information resource and submits an expert opinion to the "Uzcomnazorat" State Inspectorate.	Within 24 hours
	"Uzcomnazorat" State Inspectorate	Based on the opinion of the competent state authority in the field of personal data, removes the Internet information resource from the "Register of Violators of Rights of Personal Data Subjects" and submits a representation to the Ministry for Development of Information Technologies and Communications.	Within 24 hours
	Ministry for Development of Information Technologies and Communications	Upon the removal of the owner and (or) operator of the personal data database (or the identification data of the information resource) from the "Register of Violators of Rights of Personal Data Subjects", removes access restrictions based on the representation of the state control authority.	Within 12 hours

Annex 2

Institutional framework of foreign countries on personal data

№	Foreign Country Name	Data Protection Authority (DPA)	Supervisory Body	Monitoring Body	Restricting Authority (Administrative/Judicial)	Coordinating Body
1.	Great Britain	Information Commissioner's Office (ICO)	ICO	ICO	ICO and Court System	Department for Digital, Culture, Media and Sport (DCMS)
2.	France	National Commission on Informatics and Liberty (CNIL)	CNIL	CNIL	CNIL and Courts	State Secretariat for Digital Affairs
3.	Germany	Federal Commissioner for Data Protection and Freedom of Information (BfDI)	BfDI (Federal and State level)	BfDI Inspections	BfDI and Administrative Courts	Federal Ministry of the Interior and Community (BMI)
4.	Italy	Data Protection Guarantor (Garante)	Garante	Garante	Garante and Courts	Ministry of Technological Innovation
5.	Spain	Data Protection Agency (AEPD)	AEPD	AEPD	AEPD and Courts	Ministry of Economic Affairs and Digital Transformation
6.	Netherlands	Personal Data Authority (AP)	AP	AP	AP and Courts	Ministry of the Interior and Kingdom Relations
7.	Belgium	Data Protection Authority (GBA/APD)	GBA/APD	GBA/APD	GBA/APD and Courts	Ministry of Justice

8.	Austria	Data Protection Authority (DSB)	DSB	DSB	DSB and Courts	Federal Ministry of Justice
9.	Ireland	Data Protection Commission (DPC)	DPC	DPC	DPC and Courts	Ministry of Climate Action and Public Transport
10.	Sweden	Privacy Protection Authority (IMY)	IMY	IMY	IMY and Courts	Ministry of Justice
11.	Denmark	Data Protection Agency (Datatilsynet)	Datatilsynet	Datatilsynet	Datatilsynet and Courts	Ministry of Justice
12.	Finland	Office of the Data Protection Ombudsman	Ombudsman	Ombudsman	Ombudsman and Courts	Ministry of Justice
13.	Portugal	National Data Protection Commission (CNPD)	CNPD	CNPD	CNPD and Courts	Ministry of Justice
14.	Poland	Personal Data Protection Office (UODO)	UODO	UODO	UODO and Courts	Ministry of Digitalization
15.	Czech Republic	Office for Personal Data Protection (UOOU)	UOOU	UOOU	UOOU and Courts	Ministry of the Interior
16.	Hungary	National Authority for Data Protection and Freedom of Information (NAIH)	NAIH	NAIH	NAIH and Courts	Ministry of Justice
17.	Romania	National Authority for Quality and Data Protection (ANSPDCP)	ANSPDCP	ANSPDCP	ANSPDCP and Courts	Ministry of Research and Innovation

18.	Greece	Hellenic Data Protection Authority (HDPA)	HDPA	HDPA	HDPA and Courts	Ministry of Justice
19.	Croatia	Personal Data Protection Agency (AZOP)	AZOP	AZOP	AZOP and Courts	Ministry of Public Administration
20.	Slovakia	Office for Personal Data Protection	Office	Office	Office and Courts	Ministry of Justice
21.	Slovenia	Information Commissioner (IP)	IP	IP	IP and Courts	Ministry of Public Administration
22.	Bulgaria	Commission for Personal Data Protection (CPDP)	CPDP	CPDP	CPDP and Courts	Ministry of the Interior
23.	Estonia	Data Protection Inspectorate (AKI)	AKI	AKI	AKI and Courts	Ministry of Justice
24.	Latvia	State Data Inspectorate (DVI)	DVI	DVI	DVI and Courts	Ministry of Justice
25.	Lithuania	State Data Protection Inspectorate (VDAI)	VDAI	VDAI	VDAI and Courts	Ministry of Justice
26.	Cyprus	Personal Data Protection Commissioner	Commissioner	Commissioner	Commissioner and Courts	Ministry of the Interior
27.	Malta	Information and Data Protection Commissioner (IDPC)	IDPC	IDPC	IDPC and Courts	Ministry of Justice
28.	Norway	Data Protection Authority (Datatilsynet)	Datatilsynet	Datatilsynet	Datatilsynet and Courts	Ministry of Local Government and Modernisation

29.	Switzerland	Federal Data Protection and Information Commissioner (FDPIC)	FDPIC	FDPIC	FDPIC and Courts	Federal Chancellery / Ministry of Justice
30.	Iceland	Data Protection Authority (Persónuvernd)	Persónuvernd	Persónuvernd	Persónuvernd and Courts	Ministry of the Interior
31.	Liechtenstein	Data Protection Authority (DSS)	DSS	DSS	DSS and Courts	Ministry of Justice
32.	Serbia	Commissioner for Information and Personal Data	Commissioner	Commissioner	Commissioner and Courts	Ministry of Public Administration
33.	Albania	Information and Data Protection Commissioner	Commissioner	Commissioner	Commissioner and Courts	Parliament / Ministry of Justice
34.	Montenegro	Agency for Personal Data and Information	Agency	Agency	Agency and Courts	Ministry of the Interior
35.	North Macedonia	Personal Data Protection Agency	Agency	Agency	Agency and Courts	Ministry of Justice
36.	Bosnia and Herzegovina	Agency for Personal Data Protection (AZLP)	AZLP	AZLP	AZLP and Courts	Ministry of Civil Affairs
37.	Moldova	National Center for Personal Data Protection	Center	Center	Center and Courts	Ministry of Justice
38.	Ukraine	Parliamentary Commissioner for	Ombudsman	Ombudsman	Ombudsman and Courts	Ministry of Justice / Ministry of Digital Affairs

		Human Rights (Ombudsman)				
39.	Georgia	Personal Data Protection Service	Service	Service	Service and Courts	Ministry of Justice
40.	USA	Federal Trade Commission (FTC) / State Attorneys General	FTC	FTC / States	FTC and Federal Courts	Department of Commerce (DOC)
41.	Canada	Office of the Privacy Commissioner (OPC)	OPC	OPC	OPC and Courts	Ministry of Innovation, Science and Economic Development
42.	Mexico	National Institute for Transparency and Data Protection (INAI)	INAI	INAI	INAI and Courts	Ministry of Public Administration
43.	Brazil	National Data Protection Authority (ANPD)	ANPD	ANPD	ANPD and Courts	Ministry of Communications / Office of the President
44.	Argentina	Agency for Access to Public Information (AAIP)	AAIP	AAIP	AAIP and Courts	Cabinet of Ministers
45.	Colombia	Superintendency of Industry and Commerce (SIC)	SIC	SIC	SIC and Courts	Ministry of Commerce, Industry and Tourism
46.	Chile	Transparency Council (CPLT)	CPLT	CPLT	CPLT and Courts	Secretariat of the Presidency

47.	Peru	National Data Protection Authority (ANPD)	ANPD	ANPD	ANPD and Courts	Ministry of Justice and Human Rights
48.	Uruguay	Personal Data Control Regulatory Authority (URCDP)	URCDP	URCDP	URCDP and Courts	Agency for Electronic Government (AGESIC)
49.	Costa Rica	Personal Data Protection Agency (PRODHAB)	PRODHAB	PRODHAB	PRODHAB and Courts	Ministry of Justice and Peace
50.	Panama	National Authority for Transparency and Access to Information (ANTAI)	ANTAI	ANTAI	ANTAI and Courts	Ministry of the Presidency
51.	Ecuador	Superintendency of Data Protection	Superintendency	Superintendency	Superintendency and Courts	Ministry of Telecommunications
52.	Dominican Republic	Personal Data Protection Authority (under development)	Judicial System	Index and Audit Bodies	Courts	Ministry of Justice
53.	Jamaica	Office of the Information Commissioner (OIC)	OIC	OIC	OIC and Courts	Ministry of Science, Energy and Technology
54.	Bahamas	Office of the Data Protection Commissioner	Commissioner	Commissioner	Commissioner and Courts	Ministry of Finance
55.	Japan	Personal Information Protection Commission (PPC)	PPC	PPC	PPC and Courts	Cabinet of Ministers

56.	South Korea	Personal Information Protection Commission (PIPC)	PIPC	PIPC	PIPC and Courts	Ministry of Interior and Safety
57.	Singapore	Personal Data Protection Commission (PDPC)	PDPC	PDPC	PDPC and Courts	Ministry of Communications and Information
58.	Malaysia	Department of Personal Data Protection (PDP)	PDP	PDP	PDP and Courts	Ministry of Communications and Multimedia
59.	Philippines	National Privacy Commission (NPC)	NPC	NPC	NPC and Courts	Department of Information and Communications Technology
60.	Thailand	Personal Data Protection Committee (PDPC)	PDPC	PDPC	PDPC and Courts	Ministry of Digital Economy and Society
61.	Indonesia	Data Protection Authority (DPA - new)	DPA	DPA	DPA and Courts	Ministry of Communications and Information Technology
62.	India	Data Protection Board (DPB)	DPB	DPB	DPB and Courts	Ministry of Electronics and IT (MeitY)
63.	Pakistan	National Commission for Personal Data Protection (NCPDP)	NCPDP	NCPDP	NCPDP and Courts	Ministry of IT and Telecommunications
64.	Bangladesh	Digital Security Agency / DPA	Agency	Agency	Agency and Courts	Ministry of IT and Communication

65.	Sri Lanka	Data Protection Authority (DPA)	DPA	DPA	DPA and Courts	Ministry of Technology
66.	Nepal	National Information Commission	Commission	Commission	Commission and Courts	Ministry of Communications and IT
67.	Kazakhstan	Information Security Committee	Committee	Committee	Committee and Courts	Ministry of Digital Development (MCDO)
68.	Kyrgyzstan	State Agency for Personal Data Protection	Agency	Agency	Agency and Courts	Cabinet of Ministers
69.	Tajikistan	Agency for Information and Telecommunications	Agency	Agency	Agency and Courts	Ministry of Justice
70.	Turkmenistan	“Turkmenaragatnashyk” Agency / Ministry of Internal Affairs	Internal Affairs Bodies	Agency / Ministry of Internal Affairs	Courts	Ministry of Justice
71.	China	Cyberspace Administration of China (CAC)	CAC	CAC	CAC and People's Courts	Ministry of Industry and Information Technology (MIIT)
72.	Taiwan	National Development Council (NDC)	NDC / Sectoral Bodies	NDC	Sectoral Bodies and Courts	NDC and Ministries
73.	Macao (PRC)	Office for Personal Data Protection (GPDP)	GPDP	GPDP	GPDP and Courts	Government of Macao
74.	Hong Kong (PRC)	Office of the Privacy Commissioner (PCPD)	PCPD	PCPD	PCPD and Courts	Innovation and Technology Bureau

75.	UAE	UAE Data Office	Office	Office	Office and Courts	Cabinet of Ministers / TRA
76.	Saudi Arabia	Saudi Data and AI Authority (SDAIA) / NDMO	NDMO	NDMO	NDMO and Courts	SDAIA
77.	Qatar	National Cyber Security Agency (NCSA)	NCSA	NCSA	NCSA and Courts	Ministry of Transport and Communications
78.	Bahrain	Personal Data Protection Authority	Body	Body	Body and Courts	Ministry of Justice, Islamic Affairs and Waqfs
79.	Oman	Ministry of Transport, Communications and Information Technology (MTCIT)	MTCIT	MTCIT	MTCIT and Courts	MTCIT
80.	Israel	Privacy Protection Authority (PPA)	PPA	PPA	PPA and Courts	Ministry of Justice
81.	Turkey	Personal Data Protection Authority (KVKK)	KVKK	KVKK	KVKK and Courts	Ministry of Justice
82.	South Africa	Information Regulator	Regulator	Regulator	Regulator and Courts	Department of Justice and Constitutional Development
83.	Kenya	Office of the Data Protection Commissioner (ODPC)	ODPC	ODPC	ODPC and Courts	Ministry of IT and Communications

84.	Nigeria	Nigeria Data Protection Commission (NDPC)	NDPC	NDPC	NDPC and Courts	Ministry of Communications and Digital Economy
85.	Ghana	Data Protection Commission (DPC)	DPC	DPC	DPC and Courts	Ministry of Communications
86.	Senegal	Commission for Personal Data Protection (CDP)	CDP	CDP	CDP and Courts	Ministry of Digital Economy and Telecommunications
87.	Uganda	Personal Data Protection Office (PDPO)	PDPO	PDPO	PDPO and Courts	Ministry of Information and Communications Technology
88.	Rwanda	National Cyber Security Authority (NCSA)	NCSA	NCSA	NCSA and Courts	Ministry of ICT and Innovation
89.	Mauritius	Data Protection Office (DPO)	DPO	DPO	DPO and Courts	Ministry of Information Technology
90.	Morocco	National Commission for Personal Data Protection (CNDP)	CNDP	CNDP	CNDP and Courts	Office of the Head of Government
91.	Egypt	Data Protection Center (under development)	Center	Center	Center and Courts	Ministry of Communications and IT (MCIT)
92.	Tunisia	National Authority for Personal Data Protection (INPDP)	INPDP	INPDP	INPDP and Courts	Ministry of Justice

93.	Australia	Office of the Australian Information Commissioner (OAIC)	OAIC	OAIC	OAIC and Courts	Attorney General's Department
94.	New Zealand	Office of the Privacy Commissioner (OPC)	OPC	OPC	OPC and Courts	Ministry of Justice
95.	Fiji	Information and Communication Technologies Commission	Commission	Commission	Commission and Courts	Ministry of Communications
96.	Maldives	Office of the Information Commissioner (ICOM)	ICOM	ICOM	ICOM and Courts	Ministry of Communications, Science and Technology
97.	Barbados	Data Protection Commissioner	Commissioner	Commissioner	Commissioner and Courts	Ministry of Innovation and Smart Technologies
98.	Trinidad and Tobago	Office of the Information Commissioner	Office	Office	Office and Courts	Ministry of Public Administration and Communications
99.	Bermuda	Information Commissioner's Office (ICO)	ICO	ICO	ICO and Courts	Ministry of Justice
100	Cayman Islands	Office of the Ombudsman	Ombudsman	Ombudsman	Ombudsman and Courts	Ministry of Finance and Economic Development

101	Azerbaijan	Ministry of Digital Development and Transport	Ministry	Ministry	Ministry and Courts	Cabinet of Ministers
102	Armenia	Personal Data Protection Agency (PDPA)	PDPA	PDPA	PDPA and Courts	Ministry of Justice
103	Belarus	National Center for Personal Data Protection (NCPDP)	NCPDP	NCPDP	NCPDP and Courts	Administration of the President
104	Andorra	Data Protection Agency (APDA)	APDA	APDA	APDA and Courts	Government of Andorra
105	Monaco	Commission for the Control of Personal Data (CCIN)	CCIN	CCIN	CCIN and Courts	Ministry of State
106	San Marino	Data Protection Authority (Garante)	Garante	Garante	Garante and Courts	Secretariat of State
107	Kosovo	Information and Privacy Agency (AIP)	AIP	AIP	AIP and Courts	Parliament / Ministry of Justice
108	Jersey (UK)	Office of the Information Commissioner (JOIC)	JOIC	JOIC	JOIC and Courts	Government of Jersey
109	Guernsey (UK)	Office of the Data Protection Authority (ODPA)	ODPA	ODPA	ODPA and Courts	Local Government
110	Isle of Man (UK)	Information Commissioner (IOMICO)	IOMICO	IOMICO	IOMICO and Courts	Government of the Island
111	Gibraltar (UK)	Regulatory Authority (GRA)	GRA	GRA	GRA and Courts	Ministry of Digital Services

112	El Salvador	Institute for Transparency and Access to Information (IAIP)	IAIP	IAIP	IAIP and Courts	Public Administration
113	Guatemala	Human Rights Ombudsman	Ombudsman	Ombudsman	Courts	Ministry of Justice
114	Honduras	Institute for Transparency and Access to Information (IAIP)	IAIP	IAIP	IAIP and Courts	Office of the President
115	Nicaragua	Data Protection Directorate (DIPRODAP)	DIPRODAP	DIPRODAP	DIPRODAP and Courts	Judicial System
116	Belize	Telecommunications Regulatory Authority	Body	Body	Body and Courts	Ministry of Justice
117	Cuba	Ministry of Communications (MINCOM)	MINCOM	MINCOM	MINCOM and Courts	Council of Ministers
118	Haiti	National Council of Telecommunications (CONATEL)	CONATEL	CONATEL	CONATEL and Courts	Ministry of Communications
119	Antigua and Barbuda	Office of the Information Commissioner	Commissioner	Commissioner	Commissioner and Courts	Ministry of Justice
120	Saint Kitts and Nevis	Ministry of Justice and Legal Affairs	Ministry	Ministry	Courts	Ministry of Justice
121	Saint Lucia	Ministry of Justice	Ministry	Ministry	Courts	Ministry of Justice
122	Saint Vincent and	Ministry of Information and	Ministry	Ministry	Courts	Ministry of Finance and ICT

	the Grenadines	Communication Technologies				
123	Grenada	Common Law and Judicial System	Prosecutor's Office	Ministry of Internal Affairs	Courts	Ministry of Justice
124	Guyana	Ministry of Communications and ICT	Ministry	Ministry	Courts	Ministry of Communications
125	Suriname	Telecommunications Authority (TAS)	TAS	TAS	TAS and Courts	Ministry of Transport and Communications
126	Bolivia	Telecommunications Regulatory Authority (ATT)	ATT	ATT	ATT and Courts	Ministry of Public Works
127	Paraguay	Directorate of Personal Data (in formation)	Ministry	Agency	Courts	Ministry of ICT (MITIC)
128	Venezuela	Ministry of Science and Technology	Ministry	Ministry	Ministry and Courts	Presidency
129	Puerto Rico (USA)	Department of Consumer Affairs (DACO)	DACO	DACO	DACO and Courts	Territorial Administration
130	Virgin Islands (UK)	Information Commissioner (planned)	Commissioner	Commissioner	Courts	Office of the Governor
131	Kuwait	Communications and IT Regulatory Authority (CITRA)	CITRA	CITRA	CITRA and Courts	Cabinet of Ministers
132	Iraq	Communications and Media Commission (CMC)	CMC	CMC	CMC and Courts	Ministry of Communications

133	Iran	Supreme Council of Cyberspace	Council	Council	Council and Courts	Ministry of ICT
134	Syria	National Network Security Agency	Agency	Agency	Agency and Courts	Ministry of Communications and Technology
135	Lebanon	Ministry of Economy and Trade	Ministry	Ministry	Courts	Ministry of Communications
136	Jordan	Personal Data Protection Council	Council	Council	Council and Courts	Ministry of Digital Economy
137	Yemen	Ministry of Communication and Information Technology	Ministry	Ministry	Courts	Ministry of Communications
138	Palestine	Ministry of Telecommunications and Information Technology (MTIT)	MTIT	MTIT	MTIT and Courts	Ministry of the Interior
139	Afghanistan	Ministry of Communications and Information Technology (MCIT)	MCIT	MCIT	Courts	MCIT
140	Bhutan	Ministry of Information and Communications (MoIC)	MoIC	MoIC	MoIC and Courts	Ministry of Information and Communications
141	Myanmar	Ministry of Transport and Communications	Ministry	Ministry	Ministry and Courts	Ministry of the Interior

142	Cambodia	Ministry of Posts and Telecommunications (MPTC)	MPTC	MPTC	MPTC and Courts	Ministry of the Interior
143	Laos	Ministry of Technology and Communications	Ministry	Ministry	Ministry and Courts	Ministry of Technology
144	Vietnam	Ministry of Information and Communications (MIC) / Ministry of Internal Affairs	MIC and Ministry of Internal Affairs	Ministry of Internal Affairs	Ministry of Internal Affairs and Courts	Ministry of Information and Communications
145	Brunei	Cybersecurity Agency (CSB) / AITI	AITI	CSB	AITI and Courts	Ministry of Transport and Infocommunications
146	Mongolia	National Human Rights Commission / MDD	Commission	MDD	Commission and Courts	Ministry of Digital Development
147	North Korea	Ministry of State Security	Ministry	Ministry	Ministry and Courts	State Council
148	East Timor	Ministry of Transport and Communications	Ministry	Ministry	Courts	Ministry of Transport
149	Algeria	National Personal Data Authority (ANPDP)	ANPDP	ANPDP	ANPDP and Courts	Ministry of Posts and Telecommunications
150	Libya	National Authority of Telecommunications and IT	Body	Body	Body and Courts	Ministry of Communications

151	Sudan	Telecommunications Regulatory Authority (TPRA)	TPRA	TPRA	TPRA and Courts	Ministry of Communications
152	South Sudan	Ministry of Information, Communication and Technology	Ministry	Ministry	Courts	Ministry of Information
153	Ethiopia	Information Network Security Agency (INSA)	INSA	INSA	INSA and Courts	Ministry of Innovation and Technology
154	Eritrea	Ministry of Information	Ministry	Ministry	Courts	Ministry of Information
155	Djibouti	Ministry of Information and Communication	Ministry	Ministry	Ministry and Courts	Ministry of Communications
156	Somalia	National Communications Authority (NCA)	NCA	NCA	NCA and Courts	Ministry of Communications and Technology
157	Tanzania	Personal Data Protection Commission (PDPC)	PDPC	PDPC	PDPC and Courts	Ministry of Information and ICT
158	Burundi	Regulatory Authority for Telecommunications (ARCT)	ARCT	ARCT	ARCT and Courts	Ministry of Communications
159	DR Congo	Posts and Telecommunications Regulatory Authority (ARPTC)	ARPTC	ARPTC	ARPTC and Courts	Ministry of Posts and Telecommunications

160	Republic of the Congo	Commission for Personal Data Protection (CPDP)	CPDP	CPDP	CPDP and Courts	Ministry of Posts and Telecommunications
161	Central African Republic	Telecommunications Regulatory Authority (ART)	ART	ART	ART and Courts	Ministry of Digital Economy
162	Chad	Electronic Communications Regulatory Authority (ARCEP)	ARCEP	ARCEP	ARCEP and Courts	Ministry of Posts and Digital Economy
163	Cameroon	Telecommunications Regulatory Agency (ART)	ART	ART	ART and Courts	Ministry of Posts and Telecommunications
164	Equatorial Guinea	Regulatory Authority for Telecommunications (ORTEL)	ORTEL	ORTEL	ORTEL and Courts	Ministry of Transport and Posts
165	Gabon	National Commission for Personal Data Protection (CNPDCP)	CNPDCP	CNPDCP	CNPDCP and Courts	Ministry of Digital Economy
166	Sao Tome and Principe	General Regulatory Authority (AGER)	AGER	AGER	AGER and Courts	Ministry of Infrastructure and Natural Resources
167	Angola	Data Protection Agency (APD)	APD	APD	APD and Courts	Ministry of Telecommunications and IT

168	Namibia	Ministry of Information and Communications Technology	Ministry	Ministry	Courts	Ministry of Information
169	Botswana	Data Protection Commission	Commission	Commission	Commission and Courts	Ministry of Transport and Communications
170	Zimbabwe	Postal and Telecommunications Regulatory Authority (POTRAZ)	POTRAZ	POTRAZ	POTRAZ and Courts	Ministry of ICT and Cybersecurity
171	Zambia	Office of the Data Protection Commissioner	Commissioner	Commissioner	Commissioner and Courts	Ministry of Technology and Science
172	Malawi	Communications Regulatory Authority (MACRA)	MACRA	MACRA	MACRA and Courts	Ministry of Information and Digitalization
173	Mozambique	National Institute of Information and ICT (INTIC)	INTIC	INTIC	INTIC and Courts	Ministry of Science and Technology
174	Eswatini	Eswatini Communications Commission (ESCCOM)	ESCCOM	ESCCOM	ESCCOM and Courts	Ministry of ICT
175	Lesotho	Data Protection Commission (draft)	Commission	Commission	Courts	Ministry of Communications, Science and Technology

176	Madagascar	Regulatory Authority for Telecommunications (ARTEC)	ARTEC	ARTEC	ARTEC and Courts	Ministry of Digital Development
177	Seychelles	Information Commissioner	Commissioner	Commissioner	Commissioner and Courts	Department of Information Technology
178	Comoros	National Agency of Information and Communication (ANRTIC)	ANRTIC	ANRTIC	ANRTIC and Courts	Ministry of Telecommunications
179	Mali	Personal Data Protection Authority (APDP)	APDP	APDP	APDP and Courts	Ministry of Digital Economy
180	Niger	High Authority for Data Protection (HAPDP)	HAPDP	HAPDP	HAPDP and Courts	Ministry of Posts and IT
181	Burkina Faso	Commission for Information and Liberty (CIL)	CIL	CIL	CIL and Courts	Ministry of Digital Transition
182	Côte d'Ivoire	Telecommunications and ICT Authority (ARTCI)	ARTCI	ARTCI	ARTCI and Courts	Ministry of Digital Economy
183	Liberia	Liberia Telecommunications Authority (LTA)	LTA	LTA	LTA and Courts	Ministry of Posts and Telecommunications

184	Sierra Leone	National Telecommunications Commission (NATCOM)	NATCOM	NATCOM	NATCOM and Courts	Ministry of Information and Communications
185	Guinea	Regulatory Authority for Post and Telecommunications (ARPT)	ARPT	ARPT	ARPT and Courts	Ministry of Posts and Telecommunications
186	Guinea-Bissau	National Communications Authority (ARN)	ARN	ARN	ARN and Courts	Ministry of Transport and Communications
187	Gambia	Ministry of Communications and ICT	Ministry	Ministry	Courts	Ministry of ICT
188	Mauritania	Personal Data Authority (under development)	Body	Body	Courts	Ministry of Digital Transition
189	Cape Verde	National Data Protection Commission (CNPD)	CNPD	CNPD	CNPD and Courts	Ministry of Digital Economy
190	Togo	Personal Data Protection Authority (IPD)	IPD	IPD	IPD and Courts	Ministry of Digital Economy
191	Benin	Personal Data Protection Authority (APDP)	APDP	APDP	APDP and Courts	Ministry of Digitalization
192	Papua New Guinea	National Information and Communications	NICTA	NICTA	NICTA and Courts	Ministry of Communications and IT

		Technology Authority (NICTA)				
193	Solomon Islands	Telecommunications Commission (TCSI)	TCSI	TCSI	TCSI and Courts	Ministry of Communication and Aviation
194	Vanuatu	Telecommunications and Radiocommunications Regulator (TRBR)	TRBR	TRBR	TRBR and Courts	Ministry of Infrastructure and Public Works
195	New Caledonia	Representation of CNIL (France)	CNIL	CNIL	CNIL and Courts	Local Government
196	French Polynesia	Representation of CNIL (France)	CNIL	CNIL	CNIL and Courts	Local Government
197	Samoa	Ministry of Communications and Information Technology (MCIT)	MCIT	MCIT	MCIT and Courts	Ministry of Communications and IT
198	Tonga	Department of Information and Communications	Department	Department	Courts	Ministry of Communications
199	Micronesia	Department of Transportation, Communications and Infrastructure	Department	Department	Courts	Department of Transport and Communications
200	Nauru	National Telecommunications Regulatory Commission (NTRC)	Commission (NTRC)	Commission (NTRC)	Commission and Judicial System	Ministry of Communications and Information Technology

Annex 3

Definitions of General Concepts Related to Personal Data Processing

1) **blocking (restriction) of personal data** – temporary suspension of personal data processing;

2) **use of personal data** – actions with personal data aimed at achieving the operational goals of the owner, operator, and third parties;

3) **alteration and (or) supplementation of personal data** – changing and (or) supplementing the values of personal data contained in a personal data database;

4) **cross-border transfer of personal data** – transfer of personal data by the owner and (or) operator outside the territory of the Republic of Uzbekistan;

5) **depersonalization (anonymization) of personal data** – actions as a result of which it becomes impossible to determine the attribution of personal data to a specific data subject;

6) **destruction of personal data** – actions as a result of which it becomes impossible to restore personal data;

7) **collection of personal data** – actions related to obtaining personal data;

8) **systematization of personal data** – an action aimed at combining personal data into a structured system;

9) **storage of personal data** – actions to ensure the integrity, confidentiality, and availability of personal data;

10) **dissemination of personal data** – actions aimed at disclosing personal data to an indefinite circle of persons, including making personal data publicly known through mass media, publishing on the World Wide Web (Internet), or providing access to personal data in any other manner;

11) **provision of personal data** – actions aimed at disclosing personal data to a specific person;

12) **pseudonymization** – a technique for processing personal data in such a manner that the data can no longer be directly attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and subject to technical and organizational measures to ensure its security;

13) **profiling (automated analysis and forecasting)** – processing carried out for the purpose of automatically evaluating a physical person’s preferences, interests, financial situation, behavior, location, and health, as well as modeling future behavior; it also encompasses analyzing or forecasting a person’s work performance, reliability, interests, personal preferences, behavior, movement, and other personal aspects;

14) **contextual enrichment (Data Enrichment)** – forming a comprehensive digital profile of a subject by combining existing data relating to that subject with information obtained from external sources, public registries, or other databases;

15) **right to data portability (Data Portability)** – a legal and technological mechanism that provides the subject, in cases provided for by legislation, with the

ability to receive personal data concerning them in a structured, commonly used, and machine-readable format and to transmit that data to another operator;

16) **de-indexing (delisting from search engines)** – removing or blocking links and index indicators associated with a subject's name or digital identifier in global search engines and databases;

17) **logging and audit (Logging)** – automatically recording who accessed personal data, when, for what purpose, and what action was performed in an immutable electronic ledger;

18) **recovery (restoration from backup)** – restoring damaged or lost personal data to its original state using backup copies following technical accidents, cyberattacks, or system disruptions;

19) **depositary archiving** – placing personal data into long-term storage under a special protection regime after the expiration of the relevant retention period for reasons of public interest, historical, scientific, or statistical research;

20) **homomorphic (encrypted) processing** – performing mathematical, algorithmic, and logical operations directly on personal data without first decrypting (opening) it;

21) **zero-knowledge proof (Zero-Knowledge Proof – ZKP)** – verifying the accuracy of personal data through cryptographic proof without disclosing the data itself to the operator (for example, proving an age is over 18 without showing the date of birth);

22) **differential privacy** – a technique for conducting statistical analysis while mathematically limiting the risk of re-identifying information about an individual subject by introducing statistical noise into the dataset;

23) **hash-fixation to a distributed ledger** – a method of recording cryptographic hash values that confirm the integrity, existence, or execution of a specific legal action regarding personal data without placing the personal data itself on a distributed ledger;

24) **synthetic data generation** – creating entirely new (artificial) datasets for training artificial intelligence models while preserving the statistical properties of real personal data;

25) **ingestion into artificial intelligence models (AI Model Training Ingestion)** – converting personal data into non-reversible weight coefficients (weights) during the training process of neural networks;

26) **digital twin synchronization (Digital Twin Processing)** – continuously transmitting and adapting a person's real-time biological, behavioral, and cognitive parameters to their virtual meta-model (digital twin);

27) **digitization of neuro-cognitive and bio-signals** – converting and processing personal data obtained from brain impulses, DNA sequences, and neural connections into digital information formats;

28) **post-mortem (post-death) digital estate processing (Digital Afterlife Governance)** – processing or closing the digital footprints, profiles, and data of a deceased subject based on their legal heirs' requests or a will;

29) **localization** – the requirement to ensure the primary placement and processing of personal data databases and the data contained therein on physical servers located within the territory of a specific sovereign state;

30) **Legal Hold (legal retention regime)** – an organizational and legal measure aimed at temporarily suspending the scheduled destruction or alteration of data due to litigation, investigation, dispute resolution, or other legal proceedings, protecting such data while preserving its evidentiary value;

31) **consent withdrawal management** – the process of recording a subject's decision to withdraw consent to personal data processing in relevant information systems, reassessing processing operations based on legal grounds, and taking measures to cease processing or delete the data where necessary;

32) **Escrow (key escrow)** – placing the keys for anonymized or encrypted data into temporary or conditional custody with an impartial and independent third party (escrow agent);

33) **segregation (isolation)** – storing databases collected for different purposes, categories of subjects, or legal sources separately from one another from a technical, logical, and physical standpoint;

34) **replication and cloning** – synchronously or asynchronously copying identical replicas of data to servers across different geographical zones to ensure high system availability (High Availability) and for emergency recovery;

35) **partitioning (logical splitting)** – dividing massive datasets (Big Data) into smaller, independent, and manageable sectors to increase processing efficiency and reduce risk;

36) **dynamic caching (temporary memory storage)** – temporarily placing frequently accessed data in a fast memory (RAM/Cache) layer to increase processing speed and automatically purging it upon expiration;

37) **aggregation (data summarization)** – transforming individual personal data into aggregate form, average indicators, or a general statistical array to reduce the likelihood of directly identifying an individual subject while deriving analytical insights;

38) **scoring (credit and risk assessment)** – processing a subject's behavior, history, and indicators into rating scores using mathematical models and algorithms;

39) **clustering (grouping)** – grouping subjects into mathematical clusters based on previously undefined, hidden similarity attributes using artificial intelligence and machine learning algorithms;

40) **anomaly detection (Behavioral Anomaly Detection)** – assessing fraud or security threats by detecting deviations from a subject's customary behavior pattern;

41) **tokenization** – a method of reducing the risk of data exposure by replacing data that requires protection with surrogate identifiers that do not directly reflect its original value;

42) **obfuscation (crypto-blurring)** – scrambling data code and structure in such a way that it becomes incomprehensible to an external observer while preserving the functionality of the information;

43) **Data Masking (dynamic masking)** – displaying data with specific parts hidden in real time (for example, 1234) based on the user's or operator's access authorization level;

44) **DLP (Data Loss Prevention) control** – filtering data flows through deep packet inspection (DPI) to prevent unlawful leakage, unauthorized copying, or transmission of data; it also encompasses mechanisms to control data leakage via email, USB, cloud, files, endpoints, network traffic, and corporate information systems;

45) **genomic data analysis (Genomic Data Processing/Analysis)** – digitizing a person's complete DNA and hereditary genome sequence, and processing it for genetic disease and phenotype predictions;

46) **ambient/passive collection (Ambient Passive Ingestion)** – continuously capturing a person's subconscious and passive bio-behavioral indicators through environmental "smart" sensors and cyber-physical systems;

47) **post-quantum cryptography (Post-Quantum Cryptography, PQC)** – processing data under cryptographic lattice-based algorithms that are resilient against the threat of data decryption by quantum computers;

48) **quantum-shielding against de-anonymization** – the practice of introducing continuous quantum "noise" to counteract the risk of re-identifying anonymized data using artificial intelligence and quantum computing;

49) **neuro-synchronization and cognitive footprints** – converting and storing a person's thought impulses and memory circuits into a digital data array via brain-computer interfaces (BCI);

50) **association and tracing (Lineage Tracking)** – determining the complete movement trajectory and source hierarchy of data from its initial point of origin to its final processing point;

51) **quarantining (Data Quarantine)** – temporarily storing and verifying corrupted data, data of questionable accuracy, data under cyber threat, or data with an uncertain legal status in a separate, isolated environment;

52) **federated learning processing (Federated Learning Processing)** – processing personal data directly on a local device without transmitting it to a central server, and updating only the algorithm's mathematical weight parameters to the center;

53) **secure-enclave level processing (TEE Enclaving)** – processing data in a hardware-isolated, fully separated execution environment zone (Trusted Execution Environment) at the processor level;

54) **federation (Federated Identity Mapping)** – linking subject identifiers across various independent information systems and platforms without creating a separate centralized database;

55) **quantification and monetization (Data Valuation)** – determining the financial or intangible value of data and processing it as a property asset;

56) **automated filtering (Data Sanitization)** – systematically and automatically purging errors, duplicates, and sensitive elements from datasets;

57) **dynamic micro-consent processing (Dynamic Granular Consent Processing)** – algorithmic management that allows a subject to grant and revoke separate consent in real-time for each micro-operation involving their data;

58) **synthetic avatarization (Synthetic Identity Representation)** – creating and processing a legally significant digital avatar linked to a specific person in place of their real biometric and personal indicators for use in legal relations;

59) **bio-adaptive regenerative processing** – automatically processing information at the DNA and cellular level in real-time via bio-sensors and nano-robots for medical and genetic correction;

60) **sub-atomic quantum state recording (Quantum State Telemetry)** – instantaneously transmitting and processing a person's physical and biological state to interconnected memory platforms via quantum-entangled particles;

61) **cognitive substrate transfer (Consciousness Substrate Transfer)** – transferring and activating memory, character, and consciousness parameters from a person's neural networks to non-biological substrates after the termination of the biological body;

62) **recording of personal data** – the process of capturing personal data in a specified form within an information system, register, or other data carrier;

63) **retrieval of personal data** – the process of finding and extracting personal data stored in an information and communication system based on specified criteria;

64) **consultation of personal data** – the process of viewing or studying personal data for the purpose of determining its content, evaluating it, or making a decision;

65) **combination/alignment of personal data** – the process of coordinating personal data existing in various sources and integrating it into a single data array;

66) **automated decision-making (Automated Decision-Making)** – the process of making a decision that produces legal effects concerning a person or significantly affects them without human involvement or with significantly limited human involvement, as a result of processing personal data through automated algorithms, artificial intelligence, or other software tools;

67) **data protection impact assessment (Data Protection Impact Assessment – DPIA)** – the process of identifying and assessing in advance the potential impact of personal data processing on the rights and freedoms of an individual, existing risks, and legal, organizational, and technical measures aimed at mitigating these risks;

68) **purpose limitation (Purpose Limitation)** – the principle of collecting personal data for specified, explicit, and legitimate purposes, and preventing its further use in a manner incompatible with those purposes;

69) **data minimization (Data Minimisation)** – the principle of collecting and processing personal data only to the extent necessary and sufficient to achieve the processing purpose;

70) **privacy by design (Privacy by Design)** – the principle of systematically integrating personal data protection requirements starting from the

design, development, and implementation stages of information and communication systems, software products, and data processing operations;

71) **privacy by default (Privacy by Default)** – the principle that default configurations of information and communication systems are set to ensure minimal collection, use, and disclosure of personal data;

72) **personal data breach (Personal Data Breach)** – a security incident that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data;

73) **data provenance tracking (Data Provenance)** – a mechanism for documenting and tracking the original source, time of creation, modifications made, processing stages, and movement directions of personal data;

74) **role-based access control (Role-Based Access Control – RBAC)** – a mechanism for defining and technically restricting user access rights to personal data in accordance with their position, duties, and authorities;

75) **principle of least privilege (Principle of Least Privilege)** – the principle of granting every user, application, or information system component the minimum level of access rights necessary to perform their functions;

76) **data retention management (Data Retention Management)** – the process of establishing and monitoring the storage period for personal data based on processing purposes and legal requirements, and deleting, anonymizing, or archiving the data upon expiration of that period.