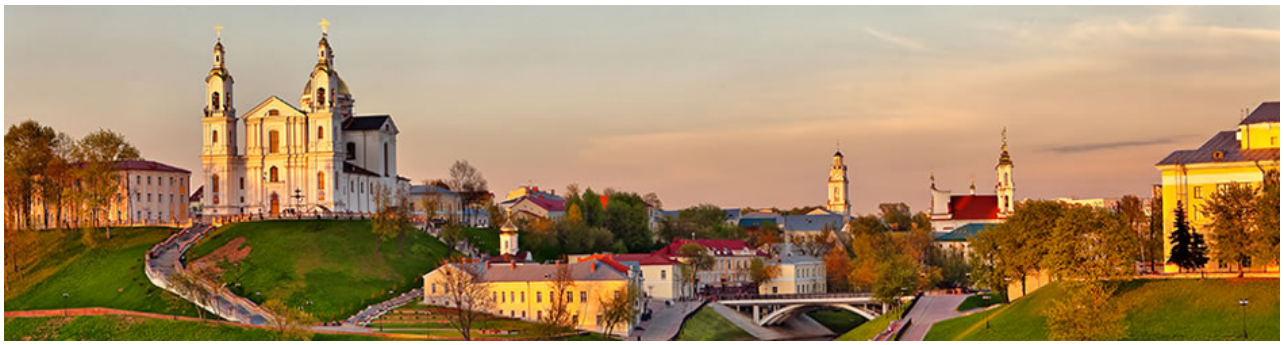
DATA PROTECTION LAWS OF THE WORLD

Belarus

BELARUS



Last modified 17 January 2024

LAW

The fundamental legal act regulating personal data protection in Belarus is the Law on Personal Data Protection of 7 May 2021 No. 99-Z which entered into force on 15 November 2021 (Data Protection Law). It is the first Belarusian legal act intended specifically for regulation of personal data protection issues.

It worth also to take into consideration the acts implemented within the framework of the Eurasian Economic Union (EEU), e.g. the Protocol on Information and Communication Technologies and Informational Interaction within the Eurasian Economic Union, Annex 3 to the Treaty on the Eurasian Economic Union of 29 May 2014. Following the Decision of the Supreme Eurasian Economic Council of 11 October 2017 the member states of EEU are planning to develop the initiative on conclusion of the Agreement on Data Circulation within the Union (including on personal data protection). The initiative is one of measures aimed at implementation of the Main Directions for Implementation of the Digital Agenda of the Eurasian Economic Union until 2025.

DEFINITIONS

Definition of personal data

Data Protection Law defines “personal data” as any information relating to an identified or identifiable natural person.

In its turn, “individual who can be identified” means an individual who can be directly or indirectly determined, in particular through the surname, proper name, patronymic, date of birth, identification number, or through one or more of characteristic features of her / his physical, psychological, mental, economic, cultural or social identity.

The Law also defines “special personal data”, “biometric personal data”, “genetic personal data” and “publicly available personal data”.

Definition of sensitive personal data

Data Protection Law defines “special personal data” which include information about race, nationality, political, religious and other convictions, health and sexual activity; criminal conviction records; biometric and genetic personal data.

“Biometric personal data” means information describing the physiological and biological characteristics of a person, which is used for her / his unique identification (fingerprints, palms, iris, characteristics of the face and its image, etc.), while “genetic personal data” is defined as information related to the inherited or acquired genetic characteristics of a

person, which contain unique data on her / his physiology or health and can be identified, in particular, during the study of her / his biological sample.

NATIONAL DATA PROTECTION AUTHORITY

The National Personal Data Protection Centre ("**NPDPC**") is the competent authority for the protection of personal data subjects' rights. The main tasks of the NPDPC are taking measures to protect the rights of personal data subjects in the processing of their personal data and organising training on personal data protection issues.

In accordance with these tasks NPDPC performs the following functions:

- controls the processing of personal data by operators (authorised persons);
- considers complaints of personal data subjects regarding the processing of personal data;
- determines the list of foreign countries having proper level of data subjects’ rights protection;
- issues permits for cross-border transfer of personal data, if the level of protection of personal data subjects' rights in a foreign country is not adequate, as well as establishes the procedure for issuing such permits;
- makes proposals on the improvement of the personal data legislation, participates in the drafting of legal acts on personal data;
- provides explanations on the application of personal data legislation, carries out other explanatory work on personal data legislation;
- determines the cases in which it is not necessary to notify NPDPC of the breach of personal data protection systems;
- establishes the classification of information resources (systems) containing personal data in order to determine the technical and cryptographic protection requirements for personal data;
- participates in the work of international organisations on personal data protection issues;
- cooperates with authorities (organisations) for protection of rights of personal data subjects in foreign countries;
- publishes annually by 15 March, the report in mass media on its activities;
- implements educational programs of additional education for adults in accordance with the legislation on education;
- exercises other authority established by the personal data legislation.

NPDPC constantly develops legislation in a field of personal data protection. Data protection authority publishes its recommendations and clarifications on application of Data Protection Law provisions and specifics of personal data protection on various matters (*inter alia*, on the content of privacy policy, on personal data processing in employment and pre-employment relations, in educational sphere, on relations between operators and authorised persons in terms of personal data processing).

Contact information of NPDPC

Build. 24-3
K.Zetkin str.
Minsk, 220036

T: + 375 17 367 07 90

e-mail: info@cpd.by

REGISTRATION

Since 1 January 2024 operators are obliged to add information about information resources (systems) containing personal data into Register of Personal Data Operators and ensure that the relevant information is kept up-to-date. Information shall be added regarding information resources (systems) that involve:

- cross–border transfer of special personal data, to a foreign state with “inappropriate” level of data subjects’ rights protection (special except for certain cases provided by Data Protection Law);
- processing of biometric and (or) genetic personal data;
- personal data processing of more than 100 thousand individuals; and
- personal data processing of more than 10 thousand individuals under the age of sixteen.

Order of the Operational and Analytical Centre under the President of the Republic of Belarus (OAC) No. 94 of 1 June 2022 establishes the list of data that shall be added into the Register of Personal Data Operators.

State information systems shall be registered under the separate procedure regardless whether any personal data are processed in it or not. According to Belarusian legislation state information systems are information systems created and / or acquired at the expense of state or local budgets, state off-budget funds, or by state legal entities. Registration is performed by specially authorised by the Ministry organisation – SERUE “Institute of Application Software Systems”. One of the conditions for state registration of an information system is registration of all information resources included in such an information system. Described registration can be performed for private owned information systems voluntarily.

According to the Edict of the President of the Republic of Belarus of 16 April 2013 No. 196 On Certain Measures for Improvement of the Information (Information Protection Edict) organisations owning information systems intended for processing of personal data are obliged to notify the OAC on the conditions of technical information protection of such systems.

DATA PROTECTION OFFICERS

Data Protection Law obliges operators to designate a structural unit or person responsible for the internal control of personal data processing. This shall be an internal unit or employees of the organisation, i.e. it is not possible to outsource the control functions. The legislation establishing obligations of different positions stipulates that the specialist of internal control over personal data processing shall have higher education, while no requirements for work experience are established.

Persons responsible for the internal control of personal data processing shall complete training on issues related to personal data protection at least once every five years. Depending on the type of organisation, the training may be organised at NPDPC or other educational organisations. In addition, the operators shall annually by 15 November provide NPDPC with information on the number of persons who shall complete training at NPDPC.

Moreover, a legal entity, including state body, processing personal data shall create information protection systems to secure information in their information systems used for processing of such data. As a part of creation of such system the entity should establish special department or appoint employee responsible to take required technical and cryptography information protection measures. According to the Information Protection Edict, the employees of such department (responsible employee) are required to have higher education in the sphere of information protection security or other higher or specialised secondary or professional - technical education and undergo training on the issues of technical and cryptographic information protection.

If for some reasons respective departments / employees cannot take such measures themselves, a special organisation licensed to perform activities on technical and / or cryptography information protection may be involved.

COLLECTION & PROCESSING

Data Protection Law contains a wide range of legal bases for personal data processing:

- data subject’s consent;
- if the processing is required for:
    - administrative or criminal proceedings, operational-search activities;
    - administration of justice and the enforcement of court orders and other enforcement documents;
    - performing monitoring activities (supervision) in accordance with the legislation;
    - implementation of legislation on national security, on combating corruption, on preventing money laundering,

financing of terrorist activities and financing weapons of mass destruction proliferation;
    - the implementation of legislation on elections and referendum;
    - state social insurance purposes;
    - formalising employment relationships, in the process of employment activities;
    - notarial activities;
    - Belarusian citizenship issues;
    - assignment and payment of pensions, benefits;
    - the organisation and carrying out of national statistical observations;
    - scientific and other research purposes, on condition that the personal data are depersonalised;
    - accounting, calculation, charging of fees for housing and utility services, other services, taxes;
- processing is based on a contract, that is concluded (being concluded) with data subject, and for the purpose of performing actions stipulated by this contract;
- if personal data are specified in a document addressed to the operator and signed by the data subject;
- processing is essential for the performance of certain journalist’s activities;
- processing is required to protect the subject's life, health or other interests if obtaining of consent is not possible;
- if personal data were previously disseminated;
- in order to fulfil the duties / powers stipulated in legislation;
- in other cases expressly provided in legislation.

Data Protection Law has different list of legal bases for processing of special personal data and for cross-border transfer of personal data to the territories of states that do not ensure proper protection of data subjects rights.

The consent of the data subject can be obtained in writing, in the form of an electronic document or in another electronic form (e.g. via tick-box at the website or SMS / email verification). Operator shall provide proof, if be required, that it has collected proper consent for personal data processing.

Before obtaining consent, the operator shall provide the subject of personal data with the following information:

- name (full name) and location (address of residence) of the operator;
- purpose of personal data processing;
- list of personal data to be processed;
- consent validity term;
- information about the persons authorised by operator to process personal data (if those are engaged);
- what actions be done with personal data;
- a general description of the processing methods;
- other relevant information.

In addition, apart from other necessary information, the subject shall be informed of his/her rights, the mechanism for exercising them, the consequences of giving and withdrawing consent.

Operator may collect surname, first name, middle name of data subject, date of birth, identification number (if not, the number of the ID document) only if it is required for the purposes of processing. Such information shall be provided by data subject when at the time he/she provides the consent.

Collection and processing of personal data shall be performed having implemented certain legal, organisational and technical measures for personal data protection. The organisational measures may include establishing a special entrance regime to the premises used for collection and processing, designation of employees who can have an access to such premises and data, and differentiation of access levels to respective information. The technical measures may include using cryptography, technical means and other possible measures of control over information protection.

TRANSFER

The general rule is that cross-border transfer is prohibited, unless a foreign state provides an appropriate level of protection of the personal data subjects’ rights. NPDPC has established that the list of foreign states, which ensure appropriate level of protection. The list includes foreign states that are parties to the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, adopted in Strasbourg on 28 January 1981 as well as foreign states that are members of the Eurasian Economic Union. There are certain plans to broaden the list of foreign states that provide appropriate level of protection of the personal data subjects’ rights.

However there are certain exceptions, when transfer to the jurisdictions with inappropriate level of protection will be allowed. For example, upon respective consent of the personal data subject and informing of the possible risks or under the individual permit for cross-border transfer issued by NPDPC.

SECURITY

The owners of the information systems should take appropriate technical, legal and organisational measures to secure personal data processed in their information systems. The key technical measure is creation of the information protection system to secure the information system of an entity intended for processing of personal data. The information protection system shall be attested according to the procedure established by the OAC. The rules also suggest simplified attestation procedure for subjects using information system of other organisations who have already passed attestation procedure for their systems.

BREACH NOTIFICATION

Data Protection Law establishes an obligation to notify NPDPC on breach of systems used for personal data protection immediately, but not later than within three business days of discovery, in writing or in the form of an electronic document. Exceptions to this requirement are cases where a breach of security systems has not resulted in the unlawful dissemination, provision of personal data; modification, blocking or deletion of personal data without the possibility of restoring access to it.

Certain additional requirements on the notification of the OAC are set for specific cases of information protection system breaches or periodical reporting as required by Belarus law. The respective requirements are set forth in the Regulations on the procedure for submitting information about information security events, the state of technical and cryptographic protection of information to the OAC, as approved by the Order of the OAC of 2 February 2020 No. 66.

ENFORCEMENT

According to Data Protection Law, NPDPC supervises the processing of personal data by operators and authorised persons. In the case of a breach of personal data legislation, NPDPC has the right to issue a demand to eliminate the detected violations and / or to terminate personal data processing in the information resource (system). Term for elimination and / or termination is set by the NPDPC, but shall not be longer than six months.

Violation of personal data protection legislation may result in civil, criminal and administrative liability. If the violation has led to moral damages, the violator may be required by the court to reimburse such damages.

Administrative Offences Code of Republic of Belarus stipulates specific sanctions for personal data processing violations, including:

- intentional illegal collection, processing, storage or transfer of personal data of an individual or violation of his / her rights related to the processing of personal data may cause a fine up to 50 base units; intentional distribution – up to 200 base units (since 1 January 2023 one base unit equals BYN 37, approx. EUR 11);
- **non-compliance with requirements on data protection** measures implementation may cause a fine ranging from 20 to 50 base units for legal entities.

The Criminal Code of Republic of Belarus envisages criminal liability for the following breaches:

- unlawful collection or provision of information relating to the private life and (or) personal data of another person without his / her consent (depending on the circumstances like volume on gravity) causing substantial harm to the rights, freedoms and legitimate interests of a citizen a person could be sentenced to community work, a criminal fine, arrest, or the restriction or deprivation of liberty for up to two years. For the unlawful distribution – restriction or deprivation

of liberty for up to three years with the criminal fine. Higher liability may apply if offence relates to the victims performing public functions; failure to comply with measures to ensure the protection of personal data by a person who processes personal data, which has inadvertently resulted in their dissemination and causing serious consequences a person could be sentenced to a criminal fine, deprivation of the right to occupy certain job positions or perform certain activities, corrective work for up to one year, arrest, or the restriction of liberty for up to two years or deprivation of liberty for up to one year.

ELECTRONIC MARKETING

Electronic marketing is subject to the rules established by the Law on Advertising of 10 May 2007 No. 225-Z (Advertising Law) and the Law on Mass Media of 17 July 2008 No. 427-Z (Mass Media Law).

According to the general rule of the Advertising Law it is not allowed to use in advertising names, pseudonyms, images or statements of citizens of the Republic of Belarus without their consent or the consent of their legal representatives.

Distribution of advertisements by telecommunication means (e.g. telephone, telex, facsimile, mobile telephone communications, email) can be performed only with the consent of respective subscriber or addressee. Such consent can be made as a text document, including document in electronic form. The consent also can be a part of an agreement for telecom services. In this case subscriber or addressee must be informed about her / his right to demand stopping placing (distributing) advertisement to her / him, which shall be specifically confirmed by the subscriber (addressee).

The advertisement distributor is obliged to immediately stop advertising to subscriber or addressee upon his / her demand within one work day from receiving the demand.

Individuals whose rights have been violated as a result of creation and / or distribution of an advertisement are entitled to protect their rights in court proceedings.

According to the Mass Media Law, information about person’s personal life or audio, video records and photos of a person can be distributed in mass media as a general rule only with consent of such person or his/her authorised representative. As an exception, distribution in the media of information messages and (or) materials prepared using audio or video recording, filming or photo of an individual without her / his consent is allowed only if measures are taken against the possible identification of this individual by unauthorized persons, and also provided that the dissemination of these information messages or materials does not violate the constitutional rights and freedoms of the individual and is necessary to protect public interests (except to criminal investigations or court proceedings).

ONLINE PRIVACY

Belarus law does not specifically regulate online privacy. General requirements on personal data protection apply.

Certain specific online privacy requirements can be established under the legislation. For example, personal data of a person, who is a domain name administrator, can be disclosed in online WHOIS service of Belarusian domain zone only with consent of such person. However, consent is not required if the domain name was registered in the name of an individual entrepreneur.

KEY CONTACTS

Sorainen

www.sorainen.com/

Kirill Laptev
Partner
Sorainen
T +375 17 391 2061
kirill.laptev@sorainen.com

Veranika Amelyanchuk
Associate
Sorainen
T +375 17 391 2061
veranika.amelyanchuk@sorainen.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.