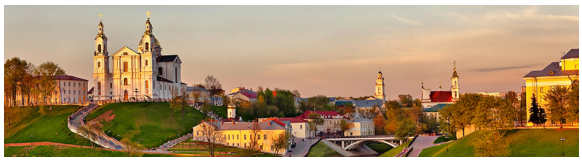
DATA PROTECTION LAWS OF THE WORLD

Belarus vs Latvia

DLA PIPER

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.

LATVIA

Last modified 11 January 2024

LAW

The General Data Protection Regulation (Regulation (EU) 2016/679) (**GDPR**) is a European Union law which entered into force in 2016 and, following a two-year transition period, became directly applicable law in all Member States of the European Union on May 25, 2018, without requiring implementation by the EU Member States through national law.

A Regulation (unlike the Directive which it replaced) is directly applicable and has consistent effect in all Member States. However, there remain more than 50 areas covered by GDPR where Member States are permitted to legislate differently in their own domestic data protection laws, and there continues to be room for different interpretation and enforcement practices among the Member States.

Territorial Scope

Primarily, the application of the GDPR turns on whether an organization is established in the EU. An 'establishment' may take a wide variety of forms, and is not necessarily a legal entity registered in an EU Member State.

However, the GDPR also has extra-territorial effect. An organization that it is not established within the EU will still be subject to the GDPR if it processes personal data of data subjects who are in the Union where the processing activities are related "*to the offering of goods or services*" (Article 3(2)(a)) (no payment is required) to such data subjects in the EU or "*the monitoring of their behaviour*" (Article 3(2)(b)) as far as their behaviour takes place within the EU.

The Personal Data Processing Law has been approved by the parliament and came into force on July 5, 2018. This law provides legal prerequisites for the implementation of the GDPR in Latvia and replaced the current Personal Data Protection Law.

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.

DEFINITIONS

Personal data is defined as "*any information relating to an identified or identifiable natural person*" (Article 4). A low bar is set for "identifiable" – if the natural person can be identified using “*all means reasonably likely to be used*” (Recital 26) the information is personal data. A name is not necessary either – any identifier will do, such as an identification number, phone number, location data or other factors which may identify that natural person.

Online identifiers are expressly called out in Recital 30, with IP addresses, cookies and RFID tags all listed as examples.

The GDPR creates more restrictive rules for the processing of **special categories** (Article 9) of personal data (including data relating to race, religion, sexual life, data pertaining to health, genetics and biometrics) and personal data relating to **criminal convictions and offences** (Article 10).

The GDPR is concerned with the **processing** of personal data. Processing has an extremely wide meaning, and includes any set of operations performed on data, including the mere storage, hosting, consultation or deletion of the data.

Personal data may be processed by either a **controller** or a **processor**. The controller is the decision maker, the person who "*alone or jointly with others, determines the purposes and means of the processing of personal data*" (Article 4). The processor "*processes personal data on behalf of the controller*", acting on the instructions of the controller. In contrast to the previous law, the GDPR imposes direct obligations on both the controller and the processor, although fewer obligations are imposed on the processor.

The "**data subject**" is a living, natural person whose personal data are processed by either a controller or a processor.

The Personal Data Processing Law reproduces the definitions of Article 4 of GDPR, and generally uses the same terminology as the GDPR.

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.

NATIONAL DATA PROTECTION AUTHORITY

Enforcement of the GDPR is the prerogative of data protection regulators, known as supervisory authorities (for example, the Cnil in France or the ICO in the UK). The European Data Protection Board (the replacement for the so-called Article 29 Working Party) is comprised of delegates from the supervisory authorities, and monitors the application of the GDPR across the EU, issuing guidelines to encourage consistent interpretation of the Regulation.

The GDPR creates the concept of **lead supervisory authority**. Where there is cross-border processing of personal data (*ie,* processing taking place in establishments of a controller or processor in multiple Member States, or taking place in a single establishment of a controller or processor but affecting data subjects in multiple Member States), then the starting point for enforcement is that controllers and processors are regulated by and answer to the supervisory authority for their main or single establishment, the so-called lead supervisory authority (Article 56(1)).

However, the lead supervisory authority is required to cooperate with all other concerned authorities, and a supervisory authority in another Member State may enforce where infringements occur on its territory or substantially affect data subjects only in its territory (Article 56(2)).

The concept of lead supervisory authority is therefore of somewhat limited help to multinationals.

According to The Personal Data Processing Law the Data State Inspectorate (DSI) has become an independent institution, however, still supervised by the government.

In addition to the tasks provided by the GDPR, The Personal Data Processing Law provides for the DSI to perform the following tasks:

- Verifying the compliance of the processing of personal data with the requirements of regulatory enactments when the controller is prohibited by law from providing information to the data subject, after receiving a relevant application from the data subject
- Investigating administrative offenses

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

- Participating, in accordance with its competence, in the drafting of laws and policies, and giving an opinion on draft laws and policy planning documents prepared by other institutions
- Providing opinions on the compliance of the personal data processing systems created by state and local government institutions with the requirements of regulatory enactments
- Monitoring the circulation of information society services in relation to the personal data protection
- monitoring the operation of credit information offices
- Issuing a license to credit information offices
- Cooperating with the supervisory authorities of foreign personal data protection, information disclosure and access control, and the prohibition of sending commercial communications
- Providing the transferring of a data subject's request for information concerning themselves to Eurojust and Europol
- Representing Latvia in international organizations and activities in the field of data protection
- Carrying out studies, analyzing situations, making recommendations, opinions and informing the public about current issues in the areas of its competence
- Performing other tasks prescribed by regulatory enactments

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);

REGISTRATION

There are no EU-wide systems of registration or notification and Recital 89 of the GDPR seeks to prohibit indiscriminate general notification obligations. However, Member States may impose notification obligations for specific activities (eg, processing of personal data relating to criminal convictions and offences). The requirement to consult the supervisory authority in certain cases following a data protection impact assessment (Article 36) constitutes a notification requirement. In addition, each controller or processor must communicate the details of its data protection officer (where it is required to appoint one) to its supervisory authority (Article 37(7)).

- 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.

In many ways, external accountability to supervisory authorities via registration or notification is superseded in the GDPR by rigorous demands for internal accountability. In particular, controllers and processors are required to complete and maintain comprehensive records of their data processing activities (Article 30), which must contain specific details about personal data processing carried out within an organization and must be provided to supervisory authorities on request. This is a sizeable operational undertaking.

Given that the GDPR does not provide for the registration of processing personal data, registries and systems will no longer exist. Pre-recorded data will remain as archived information about past activities.

DATA PROTECTION OFFICERS

Each controller or processor is required to appoint a data protection officer if it satisfies one or more of the following tests:

- It is a public authority
- Its core activities consist of processing operations which, by virtue of their nature, scope or purposes, require regular and systemic monitoring of data subjects on a large scale, or
- Its core activities consist of processing sensitive

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.

personal data on a large scale.

Groups of undertakings are permitted to appoint a single data protection officer with responsibility for multiple legal entities (Article 37(2)), provided that the data protection officer is easily accessible from each establishment (meaning that larger corporate groups may find it difficult in practice to operate with a single data protection officer).

DPOs must have expert knowledge (Article 37(5)) of data protection law and practices, though it is possible to outsource the DPO role to a service provider (Article 37(6)).

Controllers and processors are required to ensure that the DPO is involved "*properly and in a timely manner in all issues which relate to the protection of personal data*" (Article 38(1)), and the DPO must directly report to the highest management level, must not be told what to do in the exercise of his or her tasks and must not be dismissed or penalized for performing those tasks (Article 38(3)).

The specific tasks of the DPO, set out in GDPR, include (Article 39):

- To inform and advise on compliance with GDPR and other Union and Member State data protection laws
- To monitor compliance with the law and with the internal policies of the organization including assigning responsibilities, awareness raising and training staff
- To advise and monitor data protection impact assessments where requested
- To cooperate and act as point of contact with the supervisory authority

This is a good example of an area of the GDPR where Member State gold plating laws are likely. For example, German domestic law has set the bar for the appointment of DPOs considerably lower than that set out in the GDPR.

The Personal Data Processing Law provides no derogation from the requirements of the GDPR regarding DPO. The Personal Data Processing Law provides the rules for examining an individual’s knowledge in data protection and obtaining the status of DPO. The Personal Data Processing Law allows data controllers and

processors to appoint as a DPO any person who has the qualifications under the requirements of the GDPR.

The October 6, 2020 Cabinet Regulation No 620 “Data Protection Specialist Qualification Regulation” (**Regulation No 620**) determines in detail the application procedure, the content and procedure of the qualification examination and payment procedures for organizing the qualification exam. However, the qualification examination is not mandatory.

The Regulation No 620 does not set mandatory education requirements. A person who wishes to take the qualification exam, applies the Data State Inspectorate and pays the examination fee. After the person has passed the qualification exam, they are included in the list of the qualified DPOs maintained by the Data State Inspectorate and published on its website.

Regulation No 620 also provides for the maintenance of professional qualifications for DPOs who already have been included in DPOs' list. To maintain their professional qualifications, the DPOs must participate in the training in personal data protection or another field related to the performance of the DPO's duties.

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;

COLLECTION & PROCESSING

Data Protection Principles

Controllers are responsible for compliance with a set of core principles which apply to all processing of personal data. Under these principles, personal data must be (Article 5):

- Processed lawfully, fairly and in a transparent manner (lawfulness, fairness and transparency principle)
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (purpose limitation principle)
- Adequate, relevant and limited to what is necessary in relation to the purpose(s) (data minimization principle)
- Accurate and where necessary kept up-to-date (accuracy principle)
- Kept in a form which permits identification of data

    - 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

subjects for no longer than is necessary for the purpose(s) for which the data are processed (storage limitation principle)
- Processed in a manner that ensures appropriate security of the personal data, using appropriate technical and organizational measures (integrity and confidentiality principle)

The controller is responsible for and must be able to demonstrate compliance with the above principles (accountability principle). Accountability is a core theme of the GDPR. Organizations must not only comply with the GDPR but also be able to *demonstrate* compliance perhaps years after a particular decision relating to processing personal data was taken. Record keeping, audit and appropriate governance will all form a key role in achieving accountability.

Legal Basis under Article 6

In addition, in order to satisfy the lawfulness principle, each use of personal data must be justified by reference to an appropriate basis for processing. The legal bases (also known lawful bases or lawful grounds) under which personal data may be processed are (Article 6(1)):

- With the consent of the data subject (where consent must be "*freely given, specific, informed and unambiguous,*" and must be capable of being withdrawn at any time)
- Where necessary for the performance of a contract to which the data subject is party, or to take steps at the request of the data subject prior to entering into a contract
- Where necessary to comply with a legal obligation (of the EU) to which the controller is subject
- Where necessary to protect the vital interests of the data subject or another person (generally recognized as being limited to 'life or death' scenarios, such as medical emergencies)
- Where necessary for the performance of a task carried out in the public interest, or in the exercise of official authority vested in the controller
- Where necessary for the purposes of the legitimate interests of the controller or a third party (which is subject to a balancing test, in which the interests of the controller must not override the interests or fundamental rights and freedoms of the data subject. Note also that this basis cannot be relied upon by a public authority in the performance of its tasks)

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.

Special Category Data

Processing of special category data is prohibited (Article 9), except where one of the following exemptions applies (which, in effect, operate as secondary bases which must be established for the lawful processing of special category data, in addition to an Article 6 basis):

- With the explicit consent of the data subject
- Where necessary for the purposes of carrying out obligations and exercising rights under employment, social security and social protection law or a collective agreement
- Where necessary to protect the vital interests of the data subject or another natural person who is physically or legally incapable of giving consent
- In limited circumstances by certain not-for-profit bodies
- Where processing relates to the personal data which are manifestly made public by the data subject
- Where processing is necessary for the establishment, exercise or defense of legal claims or where courts are acting in their legal capacity
- Where necessary for reasons of substantial public interest on the basis of Union or Member State law, proportionate to the aim pursued and with appropriate safeguards
- Where necessary for preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, provision of health or social care or treatment of the management of health or social care systems and services
- Where necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of health care and of medical products and devices
- Where necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with restrictions set out in Article 89(1)

Member States are permitted to introduce domestic laws including further conditions and limitations for processing with regard to processing genetic data, biometric data and health data.

Criminal Convictions and Offences data

Processing of personal data relating to criminal convictions and offences is prohibited unless carried out under the control of an official public authority, or specifically

authorized by Member State domestic law (Article 10).

Processing for a Secondary Purpose

Increasingly, organizations wish to re-purpose personal data – *ie,* use data collected for one purpose for a new purpose which was not disclosed to the data subject at the time the data were first collected. This is potentially in conflict with the core principle of purpose limitation; to ensure that the rights of data subjects are protected. The GDPR sets out a series of factors that the controller must consider to ascertain whether the new process is compatible with the purposes for which the personal data were initially collected (Article 6(4)). These include:

- Any link between the original purpose and the new purpose
- The context in which the data have been collected
- The nature of the personal data, in particular whether special categories of data or data relating to criminal convictions are processed (with the inference being that if they are it will be much harder to form the view that a new purpose is compatible)
- The possible consequences of the new processing for the data subjects
- The existence of appropriate safeguards, which may include encryption or pseudonymization

If the controller concludes that the new purpose is incompatible with the original purpose, then the only bases to justify the new purpose are consent or a legal obligation (more specifically an EU or Member State law which constitutes a necessary and proportionate measure in a democratic society).

Transparency (Privacy Notices)

The GDPR places considerable emphasis on transparency, *ie,* the right for a data subject to understand how and why his or her data are used, and what other rights are available to data subjects to control processing. The presentation of granular, yet easily accessible, privacy notices should, therefore, be seen as a cornerstone of GDPR compliance.

Various information must be provided by controllers to data subjects in a concise, transparent and easily accessible form, using clear and plain language (Article 12(1)).

The following information must be provided (Article 13) at the time the data are obtained:

- The identity and contact details of the controller

- The data protection officer's contact details (if there is one)
- Both the purpose for which data will be processed and the legal basis for processing, including, if relevant, the legitimate interests for processing
- The recipients or categories of recipients of the personal data
- Details of international transfers
- The period for which personal data will be stored or, if that is not possible, the criteria used to determine this
- The existence of rights of the data subject including the right to access, rectify, require erasure, restrict processing, object to processing and data portability
- Where applicable, the right to withdraw consent, and the right to complain to supervisory authorities
- The consequences of failing to provide data necessary to enter into a contract
- The existence of any automated decision making and profiling and the consequences for the data subject
- In addition, where a controller wishes to process existing data for a new purpose, they must inform data subjects of that further processing, providing the above information

Somewhat different requirements apply (Article 14) where information has not been obtained from the data subject.

Rights of the Data Subject

Data subjects enjoy a range of rights to control the processing of their personal data, some of which are very broadly applicable, while others only apply in quite limited circumstances. Controllers must provide information on action taken in response to requests within one calendar month as a default, with a limited right for the controller to extend this period thereby a further two months where the request is onerous.

Right of access (Article 15)

A data subject is entitled to request access to and obtain a copy of his or her personal data, together with prescribed information about the how the data have been used by the controller.

Right to rectify (Article 16)

Data subjects may require inaccurate or incomplete personal data to be corrected or completed without undue delay.

Right to erasure ('right to be forgotten') (Article 17)

Data subjects may request erasure of their personal data. The forerunner of this right made headlines in 2014 when Europe’s highest court ruled against Google (Judgment of the CJEU in Case C-131/12), in effect requiring Google to remove search results relating to historic proceedings against a Spanish national for an unpaid debt on the basis that Google as a data controller of the search results had no legal basis to process that information.

The right is not absolute; it only arises in quite a narrow set of circumstances, notably where the controller no longer needs the data for the purposes for which they were collected or otherwise lawfully processed, or as a corollary of the successful exercise of the objection right, or of the withdrawal of consent.

Right to restriction of processing (Article 18)

Data subjects enjoy a right to restrict processing of their personal data in defined circumstances. These include where the accuracy of the data is contested; where the processing is unlawful; where the data are no longer needed save for legal claims of the data subject, or where the legitimate grounds for processing by the controller are contested.

Right to data portability (Article 20)

Where the processing of personal data is justified either on the basis that the data subject has given his or her consent to processing or where processing is necessary for the performance of a contract, then the data subject has the right to receive or have transmitted to another controller all personal data concerning him or her in a structured, commonly used and machine-readable format (*eg,* commonly used file formats recognized by mainstream software applications, such as .xsl).

Right to object (Article 21)

Data subjects have the right to object to processing on the legal basis of the legitimate interests of the data controller or where processing is in the public interest. Controllers will then have to suspend processing of the data until such time as they demonstrate “compelling legitimate grounds” for processing which override the rights of the data subject.

In addition, data subjects enjoy an unconditional right to object to the processing of personal data for direct

marketing purposes at any time.

The right not to be subject to automated decision making, including profiling (Article 22)

Automated decision making (including profiling) "*which produces legal effects concerning [the data subject] … or similarly significantly affects him or her*" is only permitted where:

a. Necessary for entering into or performing a contract
b. Authorized by EU or Member State law
c. The data subject has given their explicit (*ie,* opt-in) consent

Further, where significant automated decisions are taken on the basis of grounds (a) or (c), the data subject has the right to obtain human intervention, to contest the decision, and to express his or her point of view.

The Personal Data Processing Law contains provisions on specific treatment related to the exercise of other fundamental rights of the individual, providing derogations relating to the data processing for archiving purposes, scientific or historical research purposes, statistical purposes, and the processing of national classified data.

The Personal Data Processing Law provides specific rules and exceptions regarding the journalistic, academic, artistic and literary processing of personal data. When processing data for these purposes, it is necessary to assess the balance between the right to privacy and freedom of expression.

The Personal Data Processing Law also provides for specific rules regarding the processing of data in the official publication. It states that the data published in the official publication is deleted by the publisher on the basis of a decision of the DSI or a decision confirming that such publication does not comply with the provisions of the GDPR.

The consent of a child for the use of information society services is deemed lawful where the child is at least 13 years old, meaning that Latvia has chosen the lowest threshold regarding the age of the child. Where the child is below the age of 13 years, such consent will be lawful only if and to

the extent that consent is given or authorized by the holder of parental responsibility over the child.

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.

TRANSFER

Transfers of personal data by a controller or a processor to third countries outside of the EU (and Norway, Liechtenstein and Iceland) are only permitted where the conditions laid down in the GDPR are met (Article 44).

The European Commission has the power to make an adequacy decision in respect of a third country, determining that it provides for an adequate level of data protection, and therefore personal data may be freely transferred to that country (Article 45(1)). Currently, the following countries or territories enjoy adequacy decisions: Andorra, Argentina, Canada (with some exceptions), Switzerland, Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, Eastern Republic of Uruguay and New Zealand.

Transfers to third countries are also permitted where appropriate safeguards have been provided by the controller or processor and on condition that enforceable data subject rights and effective legal remedies for the data subject are available. The list of appropriate safeguards includes amongst others binding corporate rules and standard contractual clauses. The GDPR has removed the need which existed in some Member States under the previous law to notify and in some cases seek prior approval of standard contractual clauses from supervisory authorities.

The GDPR also includes a list of context specific derogations, permitting transfers to third countries where:

a. Explicit informed consent has been obtained
b. The transfer is necessary for the performance of a contract or the implementation of pre-contractual measures
c. The transfer is necessary for the conclusion or performance of a contract concluded in the interests of the data subject between the controller and another natural or legal person
d. The transfer is necessary for important reasons of public interest
e. The transfer is necessary for the establishment, exercise or defense of legal claims
f. The transfer is necessary in order to protect the vital interests of the data subject where consent

cannot be obtained

g. The transfer is made from a register which according to EU or Member State law is intended to provide information to the public, subject to certain conditions

There is also a very limited derogation to transfer where no other mechanism is available and the transfer is necessary for the purposes of compelling legitimate interests of the controller which are not overridden by the interests and rights of the data subject; notification to the supervisory authority and the data subject is required if relying on this derogation.

Transfers demanded by courts, tribunals or administrative authorities of countries outside the EU (Article 48) are only recognized or enforceable (within the EU) where they are based on an international agreement such as a mutual legal assistance treaty in force between the requesting third country and the EU or Member State; a transfer in response to such requests where there is no other legal basis for transfer will infringe the GDPR.

The Personal Data Processing Law imposes a limitation period with respect to a data subject’s rights to information on the recipients or categories of recipients to whom the data have been transferred: the data subject has the right to receive information about transfers within the last 2 years. The Personal Data Processing Law does not provide any other derogations or additional requirements to the GDPR regarding the transferring of the data.

For more information, please visit our Transfer - global data transfer methodology website.

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

SECURITY

Security

The GDPR is not prescriptive about specific technical standards or measures. Rather, the GDPR adopts a proportionate, context-specific approach to security. Article 32 states that controllers and processors shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk of the processing. In so doing, they must take account of the state of the art, the costs of implementation, and the nature, scope, context and purposes of processing. A

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.

'one size fits all' approach is therefore the antithesis of this requirement.

However the GDPR does require controllers and processors to consider the following when assessing what might constitute adequate security:

a. The pseudonymization and encryption of personal data
b. The ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services
c. The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident
d. A process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing

The Personal Data Processing Law does not provide any derogations or additional requirements to the GDPR regarding security.

BREACH NOTIFICATION

The GDPR contains a general requirement for a personal data breach to be notified by the controller to its supervisory authority, and for more serious breaches to also be notified to affected data subjects. A personal data breach is a wide concept, defined as any "*breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed*" (Article 4).

The controller must notify a breach to the supervisory authority without undue delay, and where feasible, not later than 72 hours after having become aware of it, unless the controller determines that the breach is unlikely to result in a risk to the rights and freedoms of natural persons. When the personal data breach is likely to result in a high risk to natural persons, the controller is also required to notify the affected data subjects without undue delay (Article 34).

Where the breach occurs at the level of the processor, it is required to notify the controller without undue delay upon becoming aware of the breach (Article 33(2)).

The notification to the supervisory authority must include where possible the categories and approximate numbers

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

of individuals and records concerned, the name of the organization’s data protection officer or other contact, the likely consequences of the breach and the measures taken to mitigate harm (Article 33(3)).

Controllers are also required to keep a record of all data breaches (Article 33(5)) (whether or not notified to the supervisory authority) and permit audits of the record by the supervisory authority.

The Personal Data Processing Law does not provide any derogations or additional requirements to the GDPR regarding breach notification duties. The Data State Inspectorate has created a template for the data breach notification available on its webpage (only in Latvian).

ENFORCEMENT

Fines

The GDPR empowers supervisory authorities to impose fines of up to 4% of annual worldwide turnover, or EUR 20 million (whichever is higher).

It is the intention of the European Commission that fines should, where appropriate, be imposed by reference to the revenue of an economic undertaking rather than the revenues of the relevant controller or processor. Recital 150 of the GDPR states that 'undertaking' should be understood in accordance with Articles 101 and 102 of the Treaty on the Functioning of the European Union, which prohibit anti-competitive agreements between undertakings and abuse of a dominant position. Unhelpfully, the Treaty does not define undertaking and the extensive case-law is not entirely straightforward, with decisions often turning on the specific facts of each case. However, in many competition cases, group companies have been regarded as part of the same undertaking. The assessment will turn on the facts of each case, and the first test cases under the GDPR will need to be scrutinized carefully to understand the interpretation of undertaking. Under EU competition law case-law, there is also precedent for regulators to impose joint and several liability on parent companies for fines imposed on those subsidiaries in some circumstances (broadly where there is participation or control), so-called look through liability. Again, it remains to be seen whether there will be a direct read-across of this principle into GDPR enforcement.

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.

Fines are split into two broad categories.
The highest fines (Article 83(5)) of up to EUR 20 million or, in the case of an undertaking, up to 4% of total worldwide turnover of the preceding year, whichever is higher, apply to infringement of:

- The basic principles for processing including conditions for consent
- data subjects’ rights
- International transfer restrictions
- Any obligations imposed by Member State law for special cases such as processing employee data
- Certain orders of a supervisory authority

The lower category of fines (Article 83(4)) of up to EUR 10 million or, in the case of an undertaking, up to 2% of total worldwide turnover of the preceding year, whichever is the higher, apply to infringement of:

- Obligations of controllers and processors, including security and data breach notification obligations
- Obligations of certification bodies
- Obligations of a monitoring body

Supervisory authorities are not required to impose fines but must ensure in each case that the sanctions imposed are effective, proportionate and dissuasive (Article 83(1)).

Fines can be imposed in combination with other sanctions.

Investigative and corrective powers

Supervisory authorities also enjoy wide investigative and corrective powers (Article 58) including the power to undertake on-site data protection audits and the power to issue public warnings, reprimands and orders to carry out specific remediation activities.

Right to claim compensation

The GDPR makes specific provision for individuals to bring private claims against controllers and processors:

- Any person who has suffered material or non-material damage as a result of a breach of the GDPR has the right to receive compensation (Article 82(1)) from the controller or processor. The inclusion of non-material damage means that individuals will be able to claim compensation for distress even where they are not able to prove financial loss.
- Data subjects have the right to mandate a consumer protection body to exercise rights and bring claims on their behalf (Article 80).

Individuals also enjoy the right to lodge a complaint with a supervisory authority (Article 77).

All natural and legal persons, including individuals, controllers and processors, have the right to an effective judicial remedy against a decision of a supervisory authority concerning them or for failing to make a decision (Article 78).

Data subjects enjoy the right to an effective legal remedy against a controller or processor (Article 79).

Enforcing the decisions provided for in Article 58 of the GDPR in relation to the imposition of a legal obligation, DSI will apply the Administrative Procedure Law. Under the Personal Data Processing Law, DSI is entitled to impose administrative sanctions to the legal entity governed by public law, e.g. state institutions. The liable official for unlawful activities with personal data and failure to comply with the obligations of the controller or processor may be punished up to EUR 1000.

The Personal Data Processing Law imposes a limitation period of 5 years for civil claims on the reimbursement of losses caused by the violations of the GDPR.

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

ELECTRONIC MARKETING

The GDPR will apply to most electronic marketing activities, as these will involve some use of personal data (eg, an email address which includes the recipient's name). The most plausible legal bases for electronic marketing will be consent, or the legitimate interests of the controller (which is expressly referenced as an appropriate basis by Recital 47). Where consent is relied upon, the strict standards for consent under the GDPR are to be noted, and marketing consent forms will invariably need to incorporate clearly worded opt-in mechanisms (such as the ticking of an unticked consent box, or the signing of a statement, and not merely the acceptance of terms and conditions, or consent implied from conduct, such as visiting a website).

Data subjects have an unconditional right to object to (and therefore prevent) any form of direct marketing (including electronic marketing) at any time (Article 21(3)).

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).

Specific rules on electronic marketing (including circumstances in which consent must be obtained) are to be found in Directive 2002/58/EC (ePrivacy Directive), as transposed into the local laws of each Member State. The ePrivacy Directive is to be replaced by a Regulation. However, it is currently uncertain when this is going to happen, as the European Commission has discarded its draft of the ePrivacy Regulation after disagreements by the Member States in the Council of the European Union. In the meantime, GDPR Article 94 makes it clear that references to the repealed Directive 95/46/EC will be replaced with references to the GDPR. As such, references to the Directive 95/46/EC standard for consent in the ePrivacy Directive will be replaced with the GDPR standard for consent.

The Personal Data Protection Law does not specifically address (electronic) marketing. However the use of personal data for marketing purposes falls within the scope of the law. The provisions on electronic marketing are also included in the Law on Information Society Services, which requires prior express consent of the person before using his or her contact information (e.g. email address, phone number) for electronic marketing purposes. This is also stressed in the guidelines provided by DSI.

According to the provisions of the Law on Information Society Services no consent is required if the data has been obtained in the course of the sale of goods or provision of services, occurs for the same or similar goods or services, the recipient is able to decline easily and with no costs for the use of his or her personal data and the recipient has not previously declared that he or she does not want to be contacted.

The Electronic Communications Law contains procedures for submitting and reviewing complaints which states that the end user has the right to submit any complaints regarding the provision of the electronic communications services (thus also possibly any data protection issues), firstly, to the relevant electronic communications merchant and afterwards to the Public Utilities Commission (Article 44 of the Electronic Communications Law.

The Personal Data Processing Law does not provide any derogations or additional requirements to the GDPR regarding electronic marketing.

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.

ONLINE PRIVACY

Specific issues of online privacy are regulated in the Electronic Communications Law and the Law on Information Society Services.

The Law on Information Society Services states that the storage of information received, including cookies or similar technologies, is permitted, provided that the consent of the person has been received after he or she has received clear and comprehensive information regarding the purpose of intended storage and data processing. Therefore, with regard to cookies Latvian law supports an opt in approach.

As to location data, the Electronic Communications Law permits the processing of location data only to ensure the provision of electronic communications services or if the express prior consent is obtained. The person whose location data is being processed has the right to revoke his or her consent or to suspend it at any time, notifying the relevant electronic communications merchant of this revocation or requested suspension.

The processing of location data for other purposes without the consent of a user or subscriber is permitted only if it is not possible to identify the person utilizing such location data or if the processing of location data is necessary for emergency services.

The Personal Data Processing Law does not provide any derogations or additional requirements to the GDPR regarding online privacy.

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@sorainer

DATA PRIVACY TOOL

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

KEY CONTACTS

Sorainen
www.sorainen.com/

Ieva Andersone
Senior Associate, Head of Commercial & Regulatory Practice Group in Latvia
Sorainen
T +371 67 365 000
ieva.andersone@sorainen.com

Andis Burkevics
Senior Associate
Sorainen
T +371 67 365 007
andis.burkevics@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.