



# Comparing privacy laws: GDPR v. PDP Law



## About the authors

**OneTrust DataGuidance™** provides a suite of privacy solutions designed to help organisations monitor regulatory developments, mitigate risk and achieve global compliance.

The OneTrust DataGuidance™ platform includes focused guidance around core topics (i.e. GDPR, data transfers, breach notification, among others), Cross-Border Charts which allow you to compare PDP Law across multiple jurisdictions at a glance, a daily customised news service and expert analysis.

These tools, along with our in-house analyst service to help with your specific research questions, provide a cost-effective and efficient solution to design and support your privacy programme.

Image production credits:  
Cover/p.5/p.51: 221A / Signature collection / istockphoto.com | MicroStockHub / Signature collection / istockphoto.com  
Scale key p6-49: enisaksoy / Signature collection / istockphoto.com  
Icon p.33-40: AlexeyBlogoodf / Essentials collection / istockphoto.com  
Icon p.47-51: cnythzl / Signature collection / istockphoto.com | MicroStockHub / Signature collection / istockphoto.com

# Table of contents

<b>Introduction</b>	5
<b>1. Scope</b>	
1.1. Personal scope	7
1.2. Territorial scope	9
1.3. Material scope	10
<b>2. Key definitions</b>	
2.1. Personal data	12
2.2. Pseudonymisation	13
2.3. Controller and processors	14
2.4. Children	16
2.5. Research	17
<b>3. Legal basis</b>	19
<b>4. Controller and processor obligations</b>	
4.1. Data transfers	21
4.2. Data processing records	23
4.3. Data protection impact assessment	26
4.4. Data protection officer appointment	30
4.5. Data security and data breaches	32
4.6. Accountability	35
<b>5. Individuals' rights</b>	
5.1. Right to erasure	36
5.2. Right to be informed	40
5.3. Right to object	44
5.4. Right of access	48
5.5. Right not to be subject to discrimination	53
5.6. Right to data portability	54
<b>6. Enforcement</b>	
6.1. Monetary penalties	56
6.2. Supervisory authority	59
6.3. Civil remedies for individuals	65



## Introduction

The General Data Protection Regulation (Regulation (EU) 2016/679) ('GDPR') entered into effect on 25 May 2018, and governs the protection of personal data in European Union and European Economic Area ('EEA') Member States. The Law of 7 May 2021 No. 99-Z on Personal Data Protection ('the PDP Law'), entered into effect on 15 November 2021, and is the primary legislation governing the processing of personal information in Belarus. Further to this, the Presidential Edict No. 422 dated 28 October 2021 (only available in Russian [here](#)) established the National Data Protection Center ('NDPC') in Belarus as the national data protection authority and has provided it with corrective, advisory, and investigatory powers.

The PDP Law outlines basic terminology and has broad similarities to the GDPR. Both legislations address matters such as data subject rights, lawful grounds for data processing, as well as international data transfers, imposing restrictions on such transfers. In addition, the GDPR and PDP Law outline similar powers including tasks and the submission of an annual report. Nevertheless, the PDP Law and GDPR diverge in important areas. The PDP Law does not require data controllers to maintain data processing records, conduct Data Protection Impact Assessments ('DPIA'), and appoint of data protection officers ('DPO'). Furthermore, although the PDP Law does provide data subjects with rights, these are less detailed and have a smaller scope than the GDPR.

This overview organises provisions from the GDPR and the PDP Law into key topics and sets them alongside each other to enable analysis and comparison. Each section begins with a detailing of principal information and a general introduction, as well as a consistency rating.





## Structure and overview of the Guide

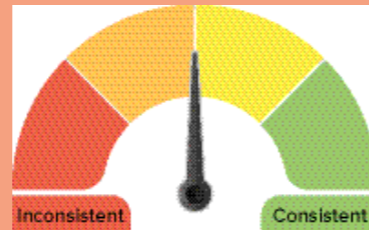
This Guide provides a comparison of the two legislative frameworks on the following key provisions:

1. Scope
2. Key definitions
3. Legal basis
4. Controller and processor obligations
5. Individuals' rights
6. Enforcement

Each topic includes relevant provisions from the two legislative legal frameworks, a summary of the comparison, and a detailed analysis of the similarities and differences between the GDPR and the PDP Law.

### Key for giving the consistency rate

-  **Consistent:** The GDPR and the PDP Law bear a high degree of similarity in the rationale, core, scope, and the application of the provision considered.
-  **Fairly consistent:** The GDPR and the PDP Law bear a high degree of similarity in the rationale, core, and the scope of the provision considered, however, the details governing its application differ.
-  **Fairly inconsistent:** The GDPR and the PDP Law bear several differences with regard to the scope and application of the provision considered, however, its rationale and core presents some similarities.
-  **Inconsistent:** The GDPR and the PDP Law bear a high degree of difference with regard to the rationale, core, scope, and application of the provision considered.



## Usage of the Guide

This Guide is general and informational in nature, and is not intended to provide, and should not be relied on as a source of, legal advice. The information and materials provided in the Guide may not be applicable in all (or any) situations and should not be PDP Lawed upon without specific legal advice based on particular circumstances.

# 1. Scope



Fairly consistent

## 1.1. Personal scope

Although the GDPR and the PDP Law both regulate the processing of personal information by private organisations as well as public bodies, there are notable differences between the two legislations. In particular, the PDP Law does not specify its applicability based on the nationality and place of residence of the data subject, nor does it clarify whether it is applicable to deceased persons.

GDPR	PDP Law
------	---------

Data controller	
-----------------	--

Article 4(7): 'controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

The PDP Law does not explicitly define a 'data controller'.  
  
However, Article 1 defines an 'operator' as a state body, a legal entity of the Republic of Belarus, another organisation, an individual, including an individual entrepreneur, independently or jointly with other specified persons organising and/ or carrying out the processing of personal data.

Data processor	
----------------	--

Article 4(8): 'processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

The PDP Law does not explicitly define a 'data processor'.  
  
However, Article 1 defines an 'authorised person' as state body, a legal entity of the Republic of Belarus, another organisation, an individual that, in accordance with an act of legislation, a state body decision or on the basis of an agreement with an operator, processes personal data on behalf of the operator or in the interests thereof.

Data subject	
--------------	--

Article 4(1): 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more fPDP Lawors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Article 1: 'personal data subject' as an individual in respect of whom processing of personal data is carried out.  
  
Article 1: 'natural person' a person who can be directly or indirectly determined, through their surname, first name, patronymic, date of birth, identification number or through one or several signs characteristic of their physical, psychological, mental, economic, cultural, or social identity.

Public bodies	
---------------	--

Article 4(7): 'controller' means the natural or legal person, public authority, agency or other body.

The PDP Law does not define a 'public bodies'.

## Public bodies (cont'd)

However, Article 1 defines an 'operator' as a state body, a legal entity of the Republic of Belarus, another organisation, an individual, including an individual entrepreneur, independently or jointly with other specified persons organising and (or) carrying out the processing of personal data.

In addition, Article 1 also defines an 'authorised person' as state body, a legal entity of the Republic of Belarus, another organisation, an individual that, in accordance with an act of legislation, a state body decision or on the basis of an agreement with an operator, processes personal data on behalf of the operator or in the interests thereof.

## Nationality of data subject

Recital 14: The protection afforded by this Regulation should apply to natural persons, whatever their nationality or place of residence, in relation to the processing of their personal data.

The PDP Law does not explicitly address the nationality of the data subject.

## Place of residence

See Recital 14, above.

The PDP Law does not explicitly address the data subjects' place of residence.

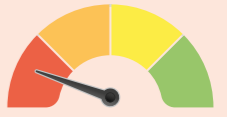
## Deceased individuals

Recital 27: This Regulation does not apply to the personal data of deceased persons. Member States may provide for rules regarding the processing of personal data of deceased persons.

The PDP Law does not explicitly address deceased individuals.

However, Article 5(9) of the PDP Law states that, in the event of the death of the subject of personal data, consent to the processing of their personal data is given by one of the heirs, close relatives, adoptive parents, adopted children or spouse of the subject of personal data, if such consent was not given by the data subject during their lifetime.

## 1.2. Territorial scope



Inconsistent

Unlike the GDPR, the PDP Law does not explicitly address its territorial scope. In particular, the GDPR specifies that it will apply to the processing of personal data in the context of the activities of an establishment in the Union, the offering of goods or services, and the monitoring from abroad in certain circumstances. Clarification from the Centre is expected on the territorial scope of the PDP Law.

## Establishment in jurisdiction

Article 3: This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.

The PDP Law does not explicitly address its territorial scope.

Recital 22: Establishment implies the effective and real exercise of PDP Law through stable arrangements.

## Extraterritorial

See Article 3, above.

The PDP Law does not explicitly address its territorial scope.

## Goods &amp; services from abroad

Recital 23: In order to ensure that natural persons are not deprived of the protection to which they are entitled under this Regulation, the processing of personal data of data subjects who are in the Union by a controller or a processor not established in the Union should be subject to this Regulation where the processing PDP Law activities are related to offering goods or services to such data subjects irrespective of whether connected to a payment.

The PDP Law does not explicitly address its territorial scope.

## Monitoring from abroad

Recital 24: The processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union should also be subject to this Regulation when it is related to the monitoring of the behaviour of such data subjects in so far as their behaviour takes place within the Union.

The PDP Law does not explicitly address its territorial scope.



Fairly consistent

## 1.3. Material scope

The PDP Law and the GDPR adopt similar concepts of personal data, data processing, as well as pseudonymisation, which is referred to as 'depersonalisation' in the PDP Law. In addition, both laws provide general exceptions for the processing of personal data for purely personal or household activities and specifically address special categories of data and sensitive data.

GDPR	PDP Law
------	---------

### Personal data/ personal information

Article 4(1): 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more fPDP Lawors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Article 1: 'personal data' any information related to an identified natural person, or natural person who can be identified.

### Data processing

Article 4(2): 'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Article 1: 'processing of personal data' as any type of action taken in relation to personal data including collection, systematisation, storage, modification, use, depersonalisation, blocking, distribution, provision, or erasure of personal data.

### Special categories of data

Article 9(1): Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.

Article 1: 'special personal data' as personal data concerning race or nationality, political views, membership of any trade unions, religious or other beliefs, health, or sexual life, administrative or criminal liability, as well as biometric and genetic personal data.

GDPR	PDP Law
------	---------

### Anonymised data

Recital 26: The principles of data protection should not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable.

The PDP Law does not explicitly define 'anonymised data'.

### Pseudonymised data

Article 4(5): 'pseudonymisation' means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.

Article 1: 'depersonalisation of personal data' - actions as a result of which it becomes impossible to determine the ownership of personal data by a specific subject of personal data without the use of additional information.

### Automated processing

Article 2(1): This Regulation applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.

Article 2(1): This Law governs relations related to the protection of personal data during their processing carried out: subject of personal data - an individual in respect of whom the processing of personal data is carried out; using automation tools; without the use of automation tools, if this provides for the search for personal data and (or) access to them according to certain criteria (file cabinets, lists, databases, magazines, etc.).

### General exemptions

Article 2(2): This Regulation does not apply to the processing of personal data:

- (a) in the course of an PDP Lawivity which falls outside the scope of Union law;
- (b) by the Member States when carrying out PDP Lawivities which fall within the scope of Chapter 2 of Title V of the Treaty on European Union; or
- (c) by a natural person in the course of a purely personal or household PDP Lawivity.

Article 2(2): This Law does not apply to relations relating to cases of personal data processing by individuals in the process of their exclusively personal, family, home and other similar use, not related to professional or entrepreneurial activities.

# 2. Key definitions



## 2.1. Personal data

The PDP Law contains similar definitions to the GDPR, including the types of personal information that are considered as sensitive/ special, definitions of operator/ data controller, and authorised persons/data processors respectively. Notably however, the GDPR provides a definition of online identifier when the PDP Law does not.

GDPR	PDP Law
------	---------

### Personal data/ personal information

Article 4(1): 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more fPDP Laws specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Article 1: 'personal data' as any information relating to an identified natural person or natural person who can be identified.

### Special categories of data

Article 9(1): Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.

Article 1: 'special personal data' as personal data related to race or nationality, political views, membership in trade unions, religious or other beliefs, health or sex life, administrative or criminal prosecution, as well as biometric and genetic personal data.

### Online identifiers

Recital 30: Natural persons may be associated with online identifiers provided by their devices, applications, tools and protocols, such as internet protocol addresses, cookie identifiers or other identifiers such as radio frequency identification tags. This may leave traces which, in particular when combined with unique identifiers and other information received by the servers, may be used to create profiles of the natural persons and identify them.

The PDP Law does not explicitly refer to online identifiers.

### Other

Not applicable.

Not applicable.



## 2.2. Pseudonymisation

The PDP Law and GDPR provide definitions for depersonalisation/ pseudonymisation of personal data, respectively. Further to this, both the PDP Law and GDPR require the implementation of technical and organisational measures to ensure that personal data is not attributable to a data subject, without the use of additional information. However, unlike the GDPR, the PDP Law does not refer to, or define, anonymised data.

GDPR	PDP Law
------	---------

### Anonymisation

Recital 26: 'anonymous information' is information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable.

The PDP Law does not refer to anonymised data.

### Pseudonymisation

Article 4(5): 'pseudonymisation' means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.

Article 1: 'depersonalisation of personal data' - actions as a result of which it becomes impossible to determine the ownership of personal data by a specific subject of personal data without the use of additional information.





## 2.3. Controllers and processors

While the PDP Law and GDPR do not use the same terminology for data controllers and processors, the scope of the terms are relatively similar. In addition, in line with the GDPR, the PDP Law requires vendor management contracts be in place between parties, and stipulates the appointment of a relevant persons responsible for internal controls related to personal data processing. However, unlike the GDPR, the PDP Law does not explicitly provide for the conducting of DPIAs.

GDPR	PDP Law
------	---------

Data controller	
-----------------	--

Article 4(7): 'controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

Article 1: 'operator' as a state body, a legal entity of the Republic of Belarus, another organisation, an individual, including an individual entrepreneur, independently or jointly with other specified persons organising and (or) carrying out the processing of personal data.

Data processor	
----------------	--

Article 4(8): 'processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

Article 1: 'authorised person' as state body, a legal entity of the Republic of Belarus, another organisation, an individual that, in accordance with an act of legislation, a state body decision or on the basis of an agreement with an operator, processes personal data on behalf of the operator or in the interests thereof.

Controller and processor contracts	
------------------------------------	--

Article 28(3): Processing by a processor shall be governed by a contract under PDP Law or other legal PDP Law under Union or Member State law, that is binding on the processor with regard to the controller and that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller. [Article 28 goes on to stipulate necessary information to be included in such a contract.]

Article 7(1): states that in an agreement between the operator and an authorised person, an act of legislation, or the decision of the state body must be determined:

- the purposes of personal data processing;
- a list of actions that will be performed with personal data an authorised person;
- obligations to maintain the confidentiality of personal data; and
- measures to ensure the protection of personal data in accordance with Article 17 of the PDP Law.

Further to this, Article 29 of the Law of 10 November 2008 No. 455-Z on Information, Informatization and Protection of Information ('the Law on Information') provides the following requirements:

GDPR	PDP Law
------	---------

Controller and processor contracts	
------------------------------------	--

- legal measures for protection of information shall include agreements between the holder of information and the user of information, which establish the terms and conditions of information use, as well as the liability of parties to the agreement for breach of these terms and conditions;
- organisational measures for protection of information shall include special security arrangements for access to the territory (premises) where information (material carriers) can be accessed, as well as differentiating access privileges by the circle of persons and the nature of the information;
- technical measures for protection of information shall include measures for the use of technical and cryptographic means for protection of information, as well as measures for controlling the security of information; and
- state bodies and legal entities that process information dissemination and (or) provision of which is restricted shall identify relevant units or designated persons responsible for protection of information.

Data Protection Impact Assessment ('DPIA')	
--	--

DPIA is not specifically defined, however Article 35 sets out requirements for DPIAs (see section 5.3. for further information).

The PDP Law does not explicitly refer to DPIAs.

Data Protection Officer ('DPO')	
---------------------------------	--

DPO is not specifically defined, however Article 37 sets out requirements related to DPOs (see section 5.4. for further information).

Article 17(3): Authorised persons are required to appointment relevant department or persons responsible for internal controls on the processing of personal data.

However, while the PDP Law specifies the above appointment, it does not specify any additional requirements for such a unit/person.





## 2.4. Children

Both the GDPR and the PDP Law refer to children/minors. According to the PDP Law, the general age at which a person may give consent for operations with their personal data is 16 years, but legislative acts may provide for a different age. In this regard, it is consistent with the GDPR as the age of consent in Member States can be as low as 13 years, but the GDPR itself states that the processing of the personal data of a child shall be lawful where the child is at least 16 years old. However, unlike the GDPR, the PDP Law does not provide requirements for the language of privacy notices specific to children.

GDPR	PDP Law
------	---------

### Children's definition

The GDPR does not specifically define 'child'. However, Article 8(1) provides: Where point (a) of Article 6(1) applies, in relation to the offer of information society services directly to a child, the processing of the personal data of a child shall be lawful where the child is at least 16 years old. Where the child is below the age of 16 years, such processing shall be lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility over the child. Member States may provide by law for a lower age for those purposes provided that such lower age is not below 13 years.

The PDP Law does not specifically define 'child.' However, Article 5(9) states that: [...] before he reaches the age of 16, with the exception of marriage before reaching the age of 16, consent to the processing of their personal data is given by one of their legal representatives. Legislative acts may provide for a different age of a minor, before reaching which consent to the processing of their personal data is given by one of their legal representatives.

### Consent for processing children's data

Article 8(2): The controller shall make reasonable efforts to verify in such cases that consent is given or authorised by the holder of parental responsibility over the child, taking into consideration available technology.

Article 5(9): [...] before he reaches the age of 16, with the exception of marriage before reaching the age of 16, consent to the processing of their personal data is given by one of their legal representatives.

### Privacy notice (children)

Recital 58: Given that children merit specific protection, any information and communication, where processing is addressed to a child, should be in such a clear and plain language that the child can easily understand.

The PDP Law does not explicitly address privacy notices targeted at children.



## 2.5. Research

Both the GDPR and PDP Law provide exceptions to data processing requirements when processed for scientific or other research purposes. Notably, however, the PDP Law provides little detail on this matter, while the GDPR sets out specific requirements and exceptions in regard to research. In addition, the PDP Law does not address compatibility with original purpose of collection or data subject rights in the context of research, while the GDPR does.

GDPR	PDP Law
------	---------

### Scientific/ historical research definition

Recital 159: Where personal data are processed for scientific research purposes, this Regulation should also apply to that processing. For the purposes of this Regulation, the processing of personal data for scientific research purposes should be interpreted in a broad manner including for example technological development and demonstration, fundamental research, applied research and privately funded research.

The PDP Law does not explicitly address or define processing of personal data for scientific or historical purposes.

However, Article 6 states that consent is not required where the personal data is being used for scientific or other research purposes, subject to the mandatory pseudonymisation of personal data, with an exception for needing consent with regard to special personal data.

Recital 160: Where personal data are processed for historical research purposes, this Regulation should also apply to that processing. This should also include historical research and research for genealogical purposes, bearing in mind that this Regulation should not apply to deceased persons.

### Compatibility with original purpose of collection

Article 5(1)(b): Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation').

The PDP Law does not explicitly address processing for compatible purposes.

### Appropriate safeguards

Article 89(1): Processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, shall be subject to appropriate safeguards, in accordance with this Regulation, for the rights and freedoms of

The PDP Law does not explicitly address appropriate safeguards in this context.

However, Article 6 provides that the consent of the data subject is not required for scientific or other research purposes, subject to mandatory depersonalisation of personal data.

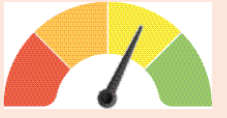
## Data subject rights (research)

Under Article 17(3), the right to erasure may not apply in cases of scientific or historical research. Article 21(6), however, provides that data subjects may exercise the right to object to data processing for scientific or historical research purposes. In addition, Article 89 provides that Member States may derogate from the GDPR in regard to data subject rights and data processing for research purposes.

The PDP Law does not explicitly address this point. However, Article 11(3) states that [...] information specified in the first Article 11(1), may not be provided if the processing of personal data is carried out in accordance with the legislation on state statistics.



## 3. Legal basis



Fairly consistent

While the GDPR sets out an exhaustive list of legal grounds for the processing of personal data, the PDP Law provides consent as its main lawful basis outlining exceptions to the same. Nevertheless, we do see similarities including, for example, processing based on vital interest, legal obligations, and legitimate purposes. In addition, the PDP Law, like the GDPR, sets out conditions for the processing of sensitive data and conditions for consent, albeit not as detailed as provided for in the GDPR.

## GDPR

## PDP Law

## Legal grounds

Article 6(1): Processing shall be lawful only if and to the extent that at least one of the following applies:

- (a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;
- (b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
- (c) processing is necessary for compliance with a legal obligation to which the controller is subject;
- (d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;
- (e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; or
- (f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

Article 4(1): The processing of personal data is carried out in accordance with this Law and other acts of legislation.

Article 6: [...] consent of the subject of personal data to the processing of personal data, with the exception of special personal data, the processing procedure for which is established by Article 8 of this Law, is not required:

- for the administration of justice, the execution of court decisions and other executive documents;
- for the purpose of exercising control (supervision) in accordance with legislative acts;
- when implementing the norms of legislation in the field of national security, on the fight against corruption, on the prevention of legalisation of proceeds from crime, the financing of terrorist activities and the financing of the proliferation of weapons of mass destruction;
- when implementing the norms of the legislation on elections, referendum, on the recall of a deputy of the House of Representatives, a member of the Council of the Republic of the National Assembly of the Republic of Belarus, a deputy of the local Council of Deputies;
- to maintain individual (personalised) records of information about insured persons for the purposes of state social insurance, including professional pension insurance;
- when registering labour (service) relations, as well as in the process of labour (service) activities of the subject of personal data in cases provided for by law;
- for the implementation of notarial activities;
- when considering issues related to citizenship of the Republic of Belarus, granting refugee status, subsidiary protection, asylum and temporary protection in the Republic of Belarus;
- for the purpose of assigning and paying pensions, benefits;
- for the organisation and conduct of state statistical observations, the formation of official statistical information; and

## Legal grounds (cont'd)

- for scientific or other research purposes, subject to mandatory depersonalisation of personal data.

## Sensitive data (legal basis)

There are specific requirements for processing special categories of data, see Article 9 of the GDPR for further information.

There are specific requirements for processing special categories of data, see Article 8 of the PDP Law for further information.

## Conditions for consent

Article 7(3): The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent.

Article 4: (11) 'consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative PDP Lawion, signifies agreement to the processing of personal data relating to him or her.

Article 10(1): The subject of personal data has the right to withdraw their consent at any time without giving reasons by submitting an application to the operator in the manner prescribed by Article 14 of this Law, or in the form through which their consent was obtained.

Article 10(4): The withdrawal of the consent of the subject of personal data has no retroactive effect, that is, the processing of personal data until it is terminated in accordance with Article 10(2) of this article is not illegal. Printed publications, audio or video recordings of programs, radio, television programs, newsreel programs, other information products containing personal data released before the withdrawal of the consent of the subject of personal data are not subject to withdrawal from civil circulation.

Article 5(1): The consent of the subject of personal data is a free, unambiguous, informed expression of their will, through which they authorises the processing of their personal data.

## Journalism/artistic purposes

Article 85(1): Member States shall by law reconcile the right to the protection of personal data pursuant to this Regulation with the right to freedom of expression and information, including processing for journalistic purposes and the purposes of academic, artistic or literary expression.

Article 6: The consent of the subject of personal data to the processing of personal data, with the exception of special personal data, is not required: [...] for the purpose of carrying out the legitimate professional activities of a journalist and/or the activities of a mass media organisation engaged in publishing activities aimed at protecting the public interest, which is the need of society to detect and disclose information about threats to national security, public order, public health and the environment, information affecting the performance of their duties by public officials in a responsible position, public figures, with the exception of cases provided for by civil procedural, economic procedural, criminal procedural legislation, legislation determining the procedure for an administrative process [...]

## 4. Controller and processor obligations



Fairly consistent

### 4.1. Data transfers

Both the GDPR and PDP Law prohibit the transfer of personal data to third countries that do not have an adequate level of protection. In addition, the PDP Law and GDPR provide for the transfer of personal data to jurisdictions that do not provide an adequate level of data protection. For example, such cases include the consent of the data subject with due notification on the relevant risks. Notably, the PDP Law does not provide alternative mechanisms for data transfers as found in the GDPR including SCCs and BCRs.

## GDPR

## PDP Law

## Adequate protection

Article 45(1): A transfer of personal data to a third country or an international organisation may take place where the Commission has decided that the third country, a territory or one or more specified sectors within that third country, or the international organisation in question ensures an adequate level of protection. Such a transfer shall not require any specific authorisation.

Article 9 (1): Cross-border transfers of personal data are prohibited if an adequate level of protection of the rights of personal data subjects is not ensured in the territory of a foreign state [...]

Article 9(2): The authorised body for the protection of the rights of subjects of personal data determines the list of foreign states on the territory of which an appropriate level of protection of the rights of subjects of personal data is ensured.

## Other mechanisms for data transfers

Article 46(1): In the absence of a decision pursuant to Article 45(3), a controller or processor may transfer personal data to a third country or an international organisation only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available.

(2) The appropriate safeguards referred to in paragraph 1 may be provided for, without requiring any specific authorisation from a supervisory authority, by:

- (a) a legally binding and enforceable instrument between public authorities or bodies;
- (b) binding corporate rules in accordance with Article 47;
- (c) standard data protection clauses adopted by the Commission in accordance with the examination procedure referred to in Article 93(2);
- (d) standard data protection clauses adopted by a supervisory authority and approved by the Commission pursuant to the examination procedure referred to in Article 93(2);

Article 9 (1): Cross-border transfers of personal data are prohibited if an adequate level of protection of the rights of personal data subjects is not ensured in the territory of a foreign state, except in cases where:

- the consent of the subject of personal data is given, provided that the subject of personal data is informed of the risks arising from the lack of the appropriate level of their protection;
- personal data was obtained on the basis of an agreement concluded (concluded) with the subject of personal data, in order to perform the actions established by this agreement;
- personal data can be obtained by any person by sending such transfer is necessary to protect the life, health or other vital interests of the subject of personal data or other persons, if obtaining the consent of the subject of personal data is impossible;

Other mechanisms for data transfers (cont'd)

- |  |   |
|--|---|
| <p>(c) standard data protection clauses adopted by the Commission in accordance with the examination procedure referred to in Article 93(2);</p> <p>(d) standard data protection clauses adopted by a supervisory authority and approved by the Commission pursuant to the examination procedure referred to in Article 93(2);</p> <p>(e) an approved code of conduct pursuant to Article 40 together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights; or</p> <p>(f) an approved certification mechanism pursuant to Article 42 together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights.</p> <p>(3) Subject to the authorisation from the competent supervisory authority, the appropriate safeguards referred to in paragraph 1 may also be provided for, in particular, by:</p> <p>(a) contractual clauses between the controller or processor and the controller, processor or the recipient of the personal data in the third country or international organisation; or</p> <p>(b) provisions to be inserted into administrative arrangements between public authorities or bodies which include enforceable and effective data subject rights.</p> | <ul style="list-style-type: none"> <li>• processing of personal data is carried out within the framework of the execution of international treaties of the Republic of Belarus;</li> <li>• such transfer is carried out by the financial monitoring body in order to take measures to prevent the legalisation of proceeds from crime, the financing of terrorist activities and the financing of the proliferation of weapons of mass destruction in accordance with the law; and</li> <li>• the relevant permission of the authorised body for the protection of rights has been received.</li> </ul> |
|--|---|

Data localisation

<p>Not applicable.</p>	<p>Not applicable.</p>
------------------------	------------------------



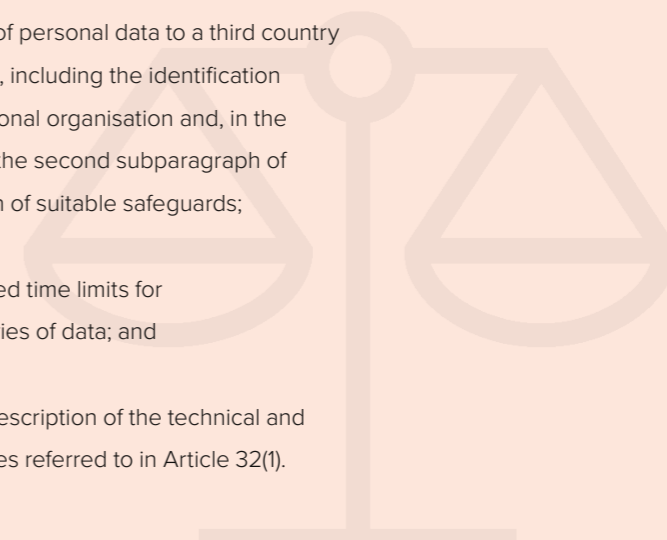
## 4.2. Data processing records

Unlike the GDPR, the PDP Law does not stipulate an obligation for operators and/or their authorised persons to maintain data processing records.

Data controller obligation

<p>Article 30(1): Each controller and, where applicable, the controller's representative, shall maintain a record of processing PDP Law activities under its responsibility. That record shall contain all of the following information:</p>	<p>The PDP Law does not explicitly provide data processing record requirements.</p>
--	---

- (a) the name and contact details of the controller and, where applicable, the joint controller, the controller's representative and the data protection officer;
- (b) the purposes of the processing;
- (c) a description of the categories of data subjects and of the categories of personal data;
- (d) the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organisations;
- (e) where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards;
- (f) where possible, the envisaged time limits for erasure of the different categories of data; and
- (g) where possible, a general description of the technical and organisational security measures referred to in Article 32(1).



**Data processor obligation**

Article 30(2): Each processor and, where applicable, the processor's representative shall maintain a record of all categories of processing PDP Lawivities carried out on behalf of a controller, containing:

- (a) the name and contPDP Law details of the processor or processors and of each controller on behalf of which the processor is PDP Lawing, and, where applicable, of the controller's or the processor's representative, and the data protection officer;
- (b) the categories of processing carried out on behalf of each controller;
- (c) where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards; and
- (d) where possible, a general description of the technical and organisational security measures referred to in Article 32(1).

Article 7(1): the authorised person is obliged to comply with the requirements for the processing of personal data provided for by the PDP Law.

**Records format**

Article 30(3): The records referred to in paragraphs 1 and 2 shall be in writing, including in electronic form.

The PDP Law does not explicitly provide data processing record requirements.

**Required to make available**

Article 30(4): The controller or the processor and, where applicable, the controller's or the processor's representative, shall make the record available to the supervisory authority on request.

The PDP Law does not explicitly provide data processing record requirements.

**Exemptions**

Article 30(5): The obligations referred to in paragraphs 1 and 2 shall not apply to an enterprise or an organisation employing fewer than 250 persons unless the processing it carries out is likely to result in a risk to the rights and freedoms of data subjects, the processing is not occasional, or the processing includes special categories of data as referred to in Article 9(1) or personal data relating to criminal convictions and offences referred to in Article 10.

The PDP Law does not explicitly provide data processing record requirements.

**General Data Processing Notification ('DPN')**

Not applicable.

Not applicable.



# 4.3. Data protection impact assessment



Unlike the GDPR, the PDP Law does not require or refer to DPIAs.

GDPR	PDP Law
------	---------

## When is a DPIA required

Article 35(1): Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks.

The PDP Law does not explicitly provide a requirement to conduct a DPIA.

[...] (3) A data protection impact assessment referred to in paragraph 1 shall in particular be required in the case of:

- (a) a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;
- (b) processing on a large scale of special categories of data referred to in Article 9(1), or of personal data relating to criminal convictions and offences referred to in Article 10; or
- (c) a systematic monitoring of a publicly accessible area on a large scale.

## DPIA content requirements

Article 35(7): The assessment shall contain at least:

- (a) a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller;
- (b) an assessment of the necessity and proportionality of the processing operations in relation to the purposes;
- (c) an assessment of the risks to the rights and freedoms of data subjects referred to in paragraph 1; and
- (d) the measures envisaged to address the risks, including

The PDP Law does not explicitly provide a requirement to conduct a DPIA.

GDPR	PDP Law
------	---------

## DPIA content requirements

safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned.

## Consultation with authority

Article 36(1): The controller shall consult the supervisory authority prior to processing where a data protection impact assessment under Article 35 indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk. [Article 36 goes on to detail requirements related to such prior consultation].

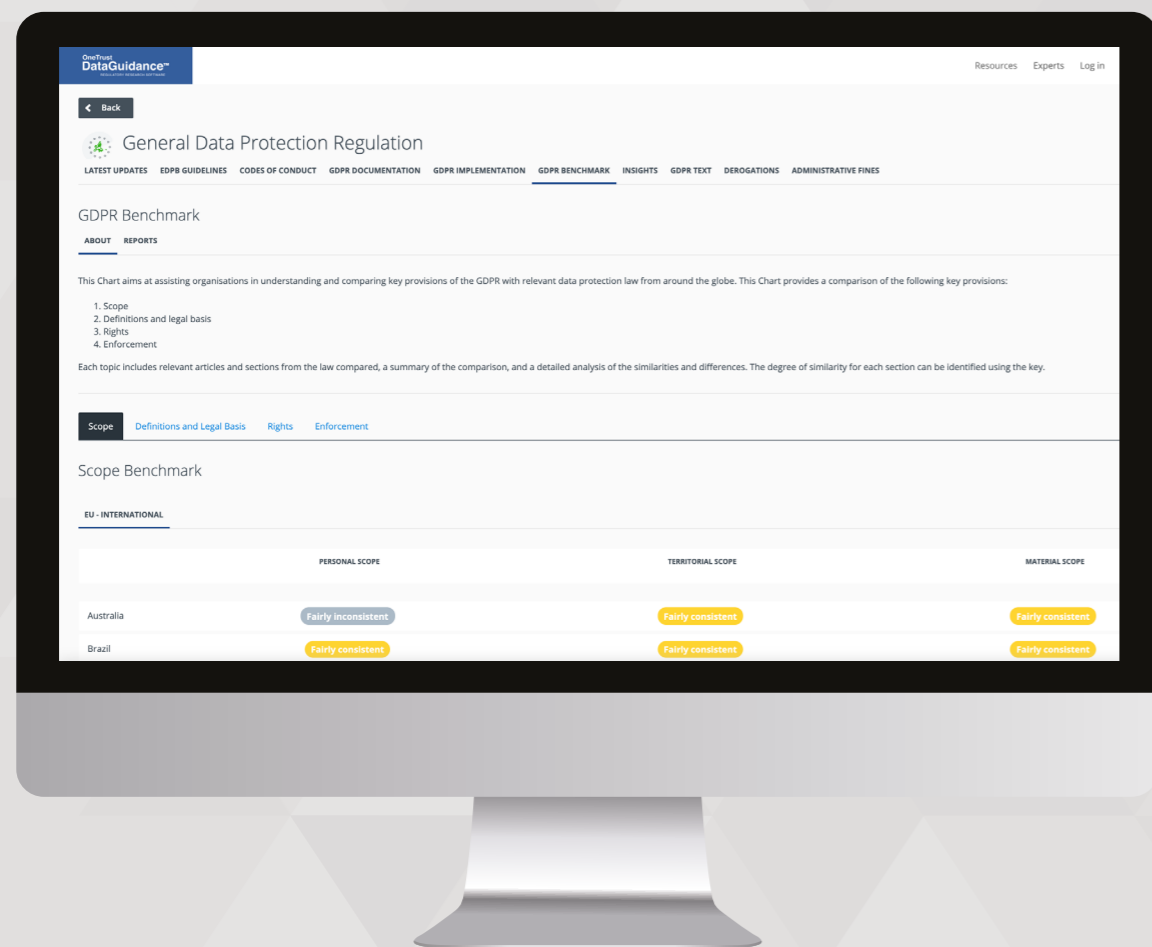
The PDP Law does not explicitly provide a requirement to conduct a DPIA.



# Global Regulatory Research Software

40 In-House Legal Researchers, 500 Lawyers  
Across 300 Jurisdictions

Monitor regulatory developments, mitigate risk,  
and achieve global compliance



## Build a global privacy program by comparing key legal frameworks against the GDPR

CCPA | Russia | Thailand | Brazil | Japan | China  
and 20+ other global laws & frameworks

Understand and compare key provisions of the GDPR  
with relevant data protection laws from around the globe

The GDPR Benchmarking tool provides comparison of the various pieces of legislation on the following key provisions



Scope



Rights



Definitions and legal basis



Enforcement

- Employ topic specific guidance to develop your compliance activities
- Monitor news and access written opinion pieces on the most recent developments

OneTrust  
**DataGuidance**<sup>™</sup>  
REGULATORY RESEARCH SOFTWARE

Start your free trial at  
[www.dataguidance.com](http://www.dataguidance.com)

# 4.4. Data protection officer appointment



Unlike the GDPR, the PDP Law does not specifically address DPO appointments. The PDP Law does, however, require the appointment of a department or person responsible for internal control over the processing of personal data by the operator. However, the PDP Law does not specify any additional requirements for such unit/person.

GDPR	PDP Law
------	---------

### DPO tasks

<p>Article 39(1): The data protection officer shall have at least the following tasks:</p> <ul style="list-style-type: none"> <li>(a) to inform and advise the controller or the processor and the employees who carry out processing of their obligations pursuant to this Regulation and to other Union or Member State data protection provisions;</li> <li>(b) to monitor compliance with this Regulation, with other Union or Member State data protection provisions and with the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits;</li> <li>(c) to provide advice where requested as regards the data protection impact assessment and monitor its performance pursuant to Article 35;</li> <li>(d) to cooperate with the supervisory authority; and</li> <li>(e) to PDP Law as the contPDP Law point for the supervisory authority on issues relating to processing, including the prior consultation referred to in Article 36, and to consult, where appropriate, with regard to any other matter.</li> </ul>	<p>The PDP Law does not provide requirements for DPO appointments.</p>
--	--

### When is a DPO required

<p>Article 37(1): The controller and the processor shall designate a data protection officer in any case where:</p> <ul style="list-style-type: none"> <li>(a) the processing is carried out by a public authority or body, except for courts PDP Lawing in their judicial capacity;</li> <li>(b) the core PDP Lawivities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or</li> </ul>	<p>The PDP Law does not provide requirements for DPO appointments.</p>
---	--

GDPR	PDP Law
------	---------

### When is a DPO required (cont'd)

<p>(c) the core PDP Lawivities of the controller or the processor consist of processing on a large scale of special categories of data pursuant to Article 9 and personal data relating to criminal convictions and offences referred to in Article 10.</p>	
---	--

### Group appointments

<p>Article 37(2): A group of undertakings may appoint a single data protection officer provided that a data protection officer is easily accessible from each establishment.</p>	<p>The PDP Law does not address group appointment of a DPO.</p>
--	---

### Notification of DPO

<p>Article 37(7): The controller or the processor shall publish the contPDP Law details of the data protection officer and communicate them to the supervisory authority.</p>	<p>The PDP Law does not provide requirements for DPO appointments.</p>
---	--

### Qualifications

<p>Article 37(5): The data protection officer shall be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and prPDP Lawices and the ability to fulfil the tasks referred to in Article 39.</p>	<p>The PDP Law does not provide requirements for DPO appointments.</p>
---	--





## 4.5. Data security and data breaches



Fairly inconsistent

The PDP Law provides a list of measures to ensure the protection of personal data, which are similar to those contained in the GDPR. Both the GDPR and the PDP Law require data breach notification to the supervisory authority. However, the GDPR includes a requirement to notify individuals of data breaches in circumstances, whereas the PDP Law does not provide such an obligation.

GDPR	PDP Law
------	---------

### Security measures defined

Article 32(1): Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

- (a) the pseudonymisation 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 organisational measures for ensuring the security of the processing.

Article 17(1): The operator is obliged to take legal, organisational, and technical measures to ensure protection personal data from unauthorised or accidental access, modification, blocking, copying, distributing, providing, deleting personal data, as well as from other illegal actions in relation to personal data.

Article 17(2): The operator determines the composition and list of measures required and sufficient to fulfil the obligations to ensure the protection of personal data, taking into account the requirements of this Law and other legislative acts.

Article 17(3): Mandatory measures to ensure the protection of personal data are:

- appointment by the operator (authorised person) being the state body, legal entity of the Republic of Belarus, other organisation, structural department or person responsible for the implementation of internal control for the processing of personal data;
- publication by the operator (authorised person), which is a legal entity of the Republic of Belarus, another organisation, an individual entrepreneur, documents defining the operator's (authorised person's) policy regarding processing of personal data;
- familiarisation of the operator's employees and other persons, directly processing personal data, with the provisions legislation on personal data, including protection requirements personal data, documents defining politics operator in relation to the processing of personal data, as well as training the specified employees and other persons in the manner prescribed by law;
- establishing the procedure for accessing personal data, including processed in the information resource (system);
- implementation of technical and cryptographic protection of personal data in accordance with the procedure established by the Operational and Analytical Center

GDPR	PDP Law
------	---------

### Security measures defined

- under the President of the Republic of Belarus ('OAC'), in accordance with the classification of information resources (systems) containing personal data.
- Article 17(5): Classification of information resources (systems) containing personal data, in order to determine the technical requirements imposed on them and cryptographic protection of personal data is established by the authorised body for the protection of the rights of subjects of personal data.

### Data breach notification to authority

Article 33(1): In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.

Article 16(1): the operator is obliged: to [...] notify the authorised body for the protection of the rights of personal data subjects about violations of personal data protection systems immediately, but no later than three working days after the operator became aware of such violations, except as provided by the authorised body for the protection of the rights of personal data subjects.

### Timeframe for breach notification

See Article 33(1) above.

See Article 16(1) above.

### Notifying data subjects of data breach

Article 34(1): When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay.

The PDP Law does not explicitly address this point.

### Data processor notification of data breach

Article 33(2): The processor shall notify the controller without undue delay after becoming aware of a personal data breach.

The PDP Law does not address this point.

However, Article 7(1) states that the authorised person is obliged to comply with the requirements for the processing of personal data provided for by this Law and other legislative acts.

### Exceptions

Article 34(3): The communication to the data subject referred to in paragraph 1 shall not be required if any of the following conditions are met:

(a) the controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption;

(b) the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects referred to in paragraph 1 is no longer likely to materialise;

(c) it would involve disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.

Article 16(1): Exceptions to the requirement to notify the DPA of a data breach may be established by the DPA.

## 4.6. Accountability



In comparison to the GDPR, the PDP Law does not explicitly address the principle of accountability or contain provisions with similar principles.

### Principle of accountability

Article 5(2): The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability'). [Paragraph 1 details principles of: lawfulness, fairness and transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity and confidentiality.]

The principle of accountability is not explicitly addressed in the PDP Law.

### Liability of data controllers and data processors

Article 82(2): Any controller involved in processing shall be liable for the damage caused by processing which infringes this Regulation. A processor shall be liable for the damage caused by processing only where it has not complied with obligations of this Regulation specifically directed to processors or where it has PDP Lawed outside or contrary to lawful instructions of the controller.

The principle of accountability is not explicitly addressed in the PDP Law.



# 5. Rights

## 5.1. Right to erasure

Similar to the GDPR, the PDP Law provides data subjects with the right to request the erasure or deletion of their personal data at any time. Both laws clarify timeframes, fees, and the data subjects right to be informed about this right. In addition, the PDP Law and GDPR detail requirements associated with the format of the response, and provide exceptions to the exercising of this right.



GDPR	PDP Law
------	---------

### Grounds for erasure

Article 17(1): The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:

- (a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
- (b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing;
- (c) the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2);
- (d) the personal data have been unlawfully processed;
- (e) the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject;
- (f) the personal data have been collected in relation to the offer of information society services referred to in Article 8(1).

Article 13(1): The subject of personal data has the right to demand from the operator the free termination of the processing of their personal data, including their deletion, in the absence of grounds for the processing of personal data provided for by this Law and other legislative acts. To exercise this right, the subject of personal data submits to the operator free of charge, unless otherwise provided by this Law and other legislative application in the manner prescribed by Article 14 of this Law.

### Inform data subject of right

Article 12(1): The controller shall take appropriate measures to provide any information referred to in Articles 13 and 14 and any communication under Articles 15 to 22 and 34 relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child. The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means.

While the PDP Law does not explicitly refer to informing the data subject of this specific right, Article 16(1) does state that the operator is obliged to explain to the subject their personal data rights related to the processing of personal data.

Additionally, Article 5(5) states that: Prior to obtaining the consent of the subject of personal data, the operator in writing or in electronic form, corresponding to the form of expressing such consent, is obliged to provide the subject of personal data with information containing:

GDPR	PDP Law
------	---------

### Inform data subject of right

Article 12(1): The controller shall take appropriate measures to provide any information referred to in Articles 13 and 14 and any communication under Articles 15 to 22 and 34 relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child. The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means.

- the purposes of processing personal data;
- a list of personal data for the processing of which the consent of the subject of personal data is given;
- the period for which the consent of the subject of personal data is given;
- information about authorised persons in case the processing of personal data will be carried out by such persons;
- a list of actions with personal data, for which the consent of the subject of personal data is given, a general description of the methods used by the operator to process personal data; and
- other information necessary to ensure the transparency of the processing of personal data.

Article 5(5) further confirms that: Before obtaining the consent of the subject of personal data, the operator is obliged to explain in simple and clear language to the subject of personal data their rights related to the processing of personal data, the mechanism for exercising such rights, as well as the consequences of giving the consent of the subject of personal data or refusing to give such consent. This information must be provided by the operator to the subject of personal data in written or electronic form, corresponding to the form of expressing their consent, separately from other information provided to him.

### Fees

Article 12(5): Information provided under Articles 13 and 14 and any communication and any PDP Law actions taken under Articles 15 to 22 and 34 shall be provided free of charge. Where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character, the controller may either:

- (a) charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the PDP Law action requested; or
- (b) refuse to PDP Law on the request. The controller shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request.

Please see Article 13(1) above.

## Response timeframe

Article 12(3): The controller shall provide information on action taken on a request under Articles 15 to 22 to the data subject without undue delay and in any event within one month of receipt of the request. That period may be extended by two further months where necessary, taking into account the complexity and number of the requests. The controller shall inform the data subject of any such extension within one month of receipt of the request, together with the reasons for the delay. Where the data subject makes the request by electronic form means, the information shall be provided by electronic means where possible, unless otherwise requested by the data subject.

Article 13(2): The operator is obliged to delete the personal data and notify the data subject, if there are no other grounds for such actions provided for by this Law and other legislative acts, within 15 days of receiving the data subject's application. If it is not technically possible to delete the personal data, the operator is obliged to take measures to prevent further processing of personal data, including blocking, and notify the subject of personal data about this in the same timeframe.

## Format of response

Article 12(1): The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means.

Article 14(3): The response to the application is sent to the data subject in the corresponding form, unless otherwise indicated in the data subject's application itself.

## Publicly available data

Article 17(2): Where the controller has made the personal data public and is obliged pursuant to paragraph 1 to erase the personal data, the controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data.

The PDP Law does not address data made publicly available by the personal data subject in the context of the right to erasure.

## Exceptions

Article 17(3): Paragraphs 1 and 2 shall not apply to the extent that processing is necessary:

- (a) for exercising the right of freedom of expression and information;
- (b) for compliance with a legal obligation which requires processing by Union or Member State law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
- (c) for reasons of public interest in the area of

Article 13(3): The operator has the right to refuse the subject of personal data request to stop processing their personal data and (or) delete them if there are grounds for processing personal data provided for by this Law and other legislative acts, including if it is necessary for the stated purposes of processing, notification of the same to the subject of personal data must be done within 15 days.

Article 13(3): The operator has the right to refuse the subject of personal data request to stop processing their personal

## Exceptions (cont'd)

public health in accordance with points (h) and (i) of Article 9(2) as well as Article 9(3);

(d) for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) in so far as the right referred to in paragraph 1 is likely to render impossible or seriously impair the achievement of the objectives of that processing; or

(e) for the establishment, exercise or defence of legal claims.

Article 12(5): Information provided under Articles 13 and 14 and any communication and any PDP Law actions taken under Articles 15 to 22 and 34 shall be provided free of charge. Where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character, the controller may either:

- (a) charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the PDP Law action requested; or
- (b) refuse to PDP Law on the request. The controller shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request.

The PDP Law does not provide specific exceptions to a right to erasure.

data and (or) delete them if there are grounds for processing personal data provided for by this Law and other legislative acts, including if it is necessary for the stated purposes of processing, notification of the same to the subject of personal data must be done within 15 days.

Where erasure of personal data is not feasible for technical reasons, then the controller is not in violation of the PDP Law for failing to comply with a request for erasure of the personal data under Section 15(1), if:

- (a) the controller collected the personal data from the data subject; and
- (b) the information provided to the data subject under Section 11(2)(h) was explicit, clear and prominent with respect to the manner of processing the personal data and expressly stated that erasure of the personal data at the request of the data subject would not be feasible.





## 5.2. Right to be informed

Similar to the GDPR, the PDP Law provides that operators involved in the processing of personal data must give clarifications to the data subject regarding the processing of their personal data prior to consent collection. The PDP Law also contains some detail on matters such as intelligibility, format, and modifications to information that must be provided to data subject. However, the PDP Law is less detailed than the GDPR on information that must be provided to data subjects when personal data is obtained from third parties.

GDPR	PDP Law
------	---------

### Informed prior to/ at collection

Article 13(1): Where personal data relating to a data subject are collected from the data subject, the controller shall, at the time when personal data are obtained, provide the data subject with all of the following information:

- (a) the identity and the contact details of the controller and, where applicable, of the controller's representative;
- (b) the contact details of the data protection officer, where applicable;
- (c) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;
- (d) where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller or by a third party;
- (e) the recipients or categories of recipients of the personal data, if any;
- (f) where applicable, the fact that the controller intends to transfer personal data to a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1), reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available.

(2) In addition to the information referred to in paragraph 1, the controller shall, at the time when personal data are obtained, provide the data subject with the following further information necessary to ensure fair and transparent processing:

- (a) the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;
- (b) the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability;
- (c) where the processing is based on point (a) of Article 6(1) or point (a) of Article 9(2), the existence of the right to

Article 5(5): Prior to obtaining the consent of the subject of personal data, the operator in writing or in electronic form, corresponding to the form of expressing such consent, is obliged to provide the subject of personal data with information containing:

- name (surname, first name, patronymic (if any)) and location (address of residence (place of stay)) of the operator receiving the consent of the subject of personal data;
- the purposes of processing personal data;
- a list of actions with personal data, for which the consent of the subject of personal data is given, a general description of the methods used by the operator to process personal data;
- other information necessary to ensure the transparency of the processing of personal data.

Prior to obtaining the consent of the subject of personal data, the operator is obliged to explain in simple and clear language to the subject of personal data their rights related to the processing of personal data, the mechanism for exercising such rights, as well as the consequences of giving the consent of the subject of personal data or refusing to give such consent. This information must be provided by the operator to the subject of personal data in written or electronic form, corresponding to the form of expressing their consent, separately from other information provided to him.

Article 16(1): The operator is obliged:

- to explain to the subject of personal data their rights related to the processing of personal data;
- obtain the consent of the subject of personal data, except in cases where provided for by this Law and other legislative acts;
- ensure the protection of personal data in the process of their processing; provide the subject of personal data with information about their personal data, as well as about the provision of their personal data to third parties, except as

GDPR	PDP Law
------	---------

### Informed prior to/ at collection (cont'd)

withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;

(d) the right to lodge a complaint with a supervisory authority;

(e) whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data;

(f) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

- otherwise provided by this Law and other legislative acts;
- make changes to personal data that are incomplete, outdated or inaccurate, unless a different procedure for making changes to personal data is established by legislative acts or if the purposes of processing personal data do not imply subsequent changes to such data; stop the processing of personal data, as well as delete or block them (ensure the termination of the processing of personal data, as well as their removal or blocking by an authorized person) in the absence of grounds for the processing of personal data provided for by this Law and other legislative acts;
- notify the authorised body for the protection of the rights of personal data subjects about violations of personal data protection systems immediately, but no later than three working days after the operator became aware of such violations, except as provided by the authorised body for the protection of the rights of personal data subjects;
- change, block or delete inaccurate or illegally obtained personal data of the subject of personal data at the request of the authorised body for the protection of the rights of subjects of personal data, unless a different procedure for making changes to personal data, blocking or deleting them is established by legislative acts; and
- fulfil other requirements of the authorised body for the protection of the rights of subjects of personal data to eliminate violations of the legislation on personal data; perform other duties stipulated by this Law and other legislative acts.

### What information is to be provided

See Article 13(1) and (2) above

See Articles 5(5) above.

### When data is from third party

In addition to the information required under Article 13, Article 14(2) replaces the requirement that data subjects are provided with information on the legitimate interests pursued by the controller or by a third party, with an obligation to inform data subjects of the categories of personal data. Furthermore, paragraph (e) of Article 13(2) is replaced with a requirement to inform data subjects of the source from which the personal data originate, and if applicable, whether it came from publicly accessible sources.

The PDP Law does not explicitly address this point.

## Intelligibility requirements

Article 12(1): The controller shall take appropriate measures to provide any information referred to in Articles 13 and 14 and any communication under Articles 15 to 22 and 34 relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child. The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means.

Article 5(5): Prior to obtaining the consent of the subject of personal data, the operator in writing or in electronic form, corresponding to the form of expressing such consent, is obliged to provide the subject of personal data with information containing:

- the purposes of processing personal data;
- a list of personal data for the processing of which the consent of the subject of personal data is given;
- the period for which the consent of the subject of personal data is given;
- information about authorised persons in case the processing of personal data will be carried out by such persons;
- a list of actions with personal data, for which the consent of the subject of personal data is given, a general description of the methods used by the operator to process personal data; and
- other information necessary to ensure the transparency of the processing of personal data.

Before obtaining the consent of the subject of personal data, the operator is obliged to explain in simple and clear language to the subject of personal data their rights related to the processing of personal data, the mechanism for exercising such rights, as well as the consequences of giving the consent of the subject of personal data or refusing to give such consent. This information must be provided by the operator to the subject of personal data in written or electronic form, corresponding to the form of expressing their consent, separately from other information provided to him.

## Format

See Article 12(1) above.

Article 5(5): The operator is obliged to provide the information to the data subject in writing, or in an electronic form corresponding to the form of expression of consent from the data subject.

## Exceptions

The requirements of Article 13 do not apply where the data subject already has the information.

The requirements of Article 14 do not apply where:

- (a) the data subject already has the information;
- (b) the provision of such information proves impossible or would involve a disproportionate effort, in particular for processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to the conditions and safeguards referred to in Article 89(1) or in so far as the obligation referred to in paragraph 1 of this Article is likely to render impossible or seriously impair the achievement of the objectives of that processing. In such cases the controller shall take appropriate measures to protect the data subject's rights and freedoms and legitimate interests, including making the information publicly available;
- (c) obtaining or disclosure is expressly laid down by Union or Member State law to which the controller is subject and which provides appropriate measures to protect the data subject's legitimate interests; or
- (d) where the personal data must remain confidential subject to an obligation of professional secrecy regulated by Union or Member State law, including a statutory obligation of secrecy.

The PDP Law does not address exceptions to this point.





## 5.3. Right to object

Unlike the GDPR, the PDP Law does not provide an explicit right to object to direct marketing, or any grounds in this regard. The PDP Law does, however, provide data subjects with a general right to demand the free termination of the processing of their personal data, including their deletion, in the absence of grounds for the processing of such personal data, and outlines the responsibilities of agencies to notify data subjects of this right. Notably, however, the PDP Law does not address the withdrawal of a data subject's consent, or provide any exemptions to this right, whereas the GDPR explicitly provides this right.

### GDPR

### PDP Law

#### Grounds for right to object/ opt out

Article 21(1): The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her which is based on point (e) or (f) of Article 6(1), including profiling based on those provisions. The controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.

Articles 13(1): The subject of personal data has the right to demand from the operator the free termination of the processing of their personal data, including their deletion, in the absence of grounds for the processing of personal data provided for by this Law and other legislative acts.

#### Withdraw consent

Article 7(3): The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent.

Article 10(1): The subject of personal data has the right to withdraw their consent at any time without giving reasons by submitting an application to the operator in the manner prescribed by Article 14 of this Law, or in the form through which their consent was obtained.

Further to this, Articles 5(8) and 16(1) also provide that a data subject has the right, at any time, without giving reasons, to withdraw their consent by submitting an application to the operator.

#### Restrict processing

Article 18(1): The data subject shall have the right to obtain from the controller restriction of processing where one of the following applies:  
(a) the accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy of the personal data;

The PDP Law does not address this point.

[However, Article 33 of the Law on Information provides that the owner of information has the right to permit and restrict access to their personal information, and determine conditions for such access.]

### GDPR

### PDP Law

#### Restrict processing (cont'd)

- (b) the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead;
- (c) the controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims;
- (d) the data subject has objected to processing pursuant to Article 21(1) pending the verification whether the legitimate grounds of the controller override those of the data subject.

#### Object to direct marketing

Article 21(3): Where the data subject objects to processing for direct marketing purposes, the personal data shall no longer be processed for such purposes.

The PDP Law does not specifically reference grounds for objecting to direct marketing.

#### Inform data subject of right

See Article 12(1) in section 5.1. above. In addition, Article 21(4) provides: At the latest at the time of the first communication with the data subject, the right referred to in paragraphs 1 and 2 shall be explicitly brought to the attention of the data subject and shall be presented clearly and separately from any other information.

Article 5(5): Prior to obtaining the consent of the subject of personal data, the operator in writing or in electronic form, corresponding to the form of expressing such consent, is obliged to provide the subject of personal data with information containing:  
the purposes of processing personal data;  
a list of personal data for the processing of which the consent of the subject of personal data is given;  
the period for which the consent of the subject of personal data is given;  
information about authorised persons in case the processing of personal data will be carried out by such persons;  
a list of actions with personal data, for which the consent of the subject of personal data is given, a general description of the methods used by the operator to process personal data; and  
other information necessary to ensure the transparency of the processing of personal data.  
Before obtaining the consent of the subject of personal data, the operator is obliged to explain in simple and clear language to the subject of personal data their rights related to the processing of personal data, the mechanism for exercising such rights, as well as the consequences of giving the consent of the subject of personal data or refusing to give such consent. This

## Inform data subject of right (cont'd)

information must be provided by the operator to the subject of personal data in written or electronic form, corresponding to the form of expressing their consent, separately from other information provided to him.

Article 16(1): the operator is obliged: to [...] notify the authorised body for the protection of the rights of personal data subjects about violations of personal data protection systems immediately, but no later than three working days after the operator became aware of such violations, except as provided by the authorised body for the protection of the rights of personal data subjects.

## Fees

See Article 12(5) in section 5.1. above.

Article 13(1): Data subjects can exercise the right to terminate processing free of charge.

## Response timeframe

See Article 12(3) in section 5.1. above.

**Termination of processing**

Article 13(2): The operator, in the case provided for in paragraph 1 of this article, is obliged, within 15 days after receiving the application of the subject of personal data, to stop processing personal data, as well as to delete them (ensure the termination of the processing of personal data, as well as their removal by an authorised person) and notify subject of personal data.

If it is not technically possible to delete personal data, the operator is obliged to take measures to prevent further processing of personal data, including their blocking, and notify the subject of personal data about this within the same period.

Article 13(3): The operator has the right to refuse the subject of personal data to satisfy the requirements to stop processing their personal data and (or) delete them if there are grounds for processing personal data provided for by this Law and other legislative acts, including if they are necessary for the stated purposes of their processing, with notification of this to the subject of personal data within 15 days.

**Withdrawal of consent**

Article 10(2): The operator is obliged, within 15 days after receiving the application of the subject of personal data in accordance with its content, to stop processing personal data, delete them and notify the subject of personal data about this, if there are no other grounds for such actions with personal

## Response timeframe (cont'd)

See Article 12(5) in section 5.1. above.

data provided for by this Law and other legislative acts.

If it is not technically possible to delete personal data, the operator is obliged to take measures to prevent further processing of personal data, including their blocking, and notify the subject of personal data about this within the same period.

## Format of response

See Article 12(1) in section 5.1. above.

See Article 14(1) in section 6.1

## Exceptions

See Article 12(5) in section 5.1. above.

Article 13(3): The operator has the right to refuse the subject of personal data to satisfy the requirements to stop processing their personal data and (or) delete them if there are grounds for processing personal data provided for by this Law and other legislative acts, including if they are necessary for the stated purposes of their processing, with notification of this to the subject of personal data within 15 days.







## 5.4. Right of access

Both the GDPR and the PDP Law provide a right of access and specify what information can be accessed by the data subject, in addition to timeframes in which the operator must respond to the request from the data subject. Notably, however, the legislations diverge in how much information should be provided; the GDPR provides a comprehensive detailed list of information that should be provided to a data subject, whereas the PDP Law does not.

### GDPR

### PDP Law

#### Grounds for right of access

Article 15(1): The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed.

Articles 11(1): The subject of personal data has the right to receive information regarding the processing of their personal data, containing:

- the name (surname, first name, patronymic (if any)) and location (address of residence (place of stay)) of the operator;
- confirmation of the fact of processing personal data by the operator (authorised person);
- his personal data and the source of their receipt; legal grounds and purposes of personal data processing;
- the period for which their consent is given;
- the name and location of the authorised person, which is a state body, a legal entity of the Republic of Belarus, another organisation, if the processing of personal data is entrusted to such a person;
- criminal procedure, data; and
- other information provided by law.

To obtain the information specified in part one of this paragraph, the subject of personal data submits an application to the operator in accordance with Article 14 of this Law.

At the same time, the subject of personal data does not have to justify their interest in the requested information.

Article 12(1): The subject of personal data has the right to receive information from the operator about the provision of their personal data to third parties once a calendar year free of charge, unless otherwise provided by this Law and other legislative acts. To obtain the information specified in part one of this paragraph, the subject of personal data submits an application to the operator in the manner prescribed by Article 14 of this Law.

### GDPR

### PDP Law

#### Information to be accessed

Article 15(1): The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information:

- the purposes of the processing;
- the categories of personal data concerned;
- the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;
- where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;
- the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;
- the right to lodge a complaint with a supervisory authority;
- where the personal data are not collected from the data subject, any available information as to their source; and
- the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

Article 12(1): The subject of personal data has the right to receive information from the operator about the provision of their personal data to third parties once a calendar year free of charge, unless otherwise provided by this Law and other legislative acts. To obtain the information specified in part one of this paragraph, the subject of personal data submits an application to the operator in the manner prescribed by Article 14 of this Law.

Article 12(2): The operator is obliged, within 15 days after receiving the application of the subject of personal data, to provide him with information about what personal data of this subject and to whom were provided during the year preceding the date of filing the application, or notify the subject of personal data about the reasons for the refusal to provide it.

#### Inform data subject of right

See Article 12(1) in section 5.1.

Article 5(5): Prior to obtaining the consent of the subject of personal data, the operator in writing or in electronic form, corresponding to the form of expressing such consent, is obliged to provide the subject of personal data with information containing:

- the purposes of processing personal data;

### Inform data subject of right

- a list of personal data for the processing of which the consent of the subject of personal data is given;
- the period for which the consent of the subject of personal data is given;
- information about authorised persons in case the processing of personal data will be carried out by such persons;
- a list of actions with personal data, for which the consent of the subject of personal data is given, a general description of the methods used by the operator to process personal data; and
- other information necessary to ensure the transparency of the processing of personal data.

Before obtaining the consent of the subject of personal data, the operator is obliged to explain in simple and clear language to the subject of personal data their rights related to the processing of personal data, the mechanism for exercising such rights, as well as the consequences of giving the consent of the subject of personal data or refusing to give such consent. This information must be provided by the operator to the subject of personal data in written or electronic form, corresponding to the form of expressing their consent, separately from other information provided to them.

### Fees

See Article 12(5) in section 5.1. above.

Article 11(2): Such information is provided to the subject of personal data free of charge, with the exception of cases provided for by legislative acts.

Article 12(1): Information on the transfer of personal data to third parties can be obtained from the operator by the data subject free of charge once in a year.

### Verify data subject request

Recital 64: The controller should use all reasonable measures to verify the identity of a data subject who requests access, in particular in the context of online services and online identifiers. A controller should not retain personal data for the sole purpose of being able to react to potential requests.

Article 14(1): Legislative acts may provide for the mandatory personal presence of the subject of personal data and the presentation of an identity document when submitting an application to the operator in writing.

### Response timeframe

See Article 12(3) in section 5.1. above.

Article 11(2): The operator is obliged, within five working days after receiving the relevant statements of the data subject, unless another period is set by legislative acts, provide him in an accessible form with the information specified in Article 11(1), and the operator is required to notify the data of the reasons for refusing their request, when applicable.  
Article 12(2): The operator is obliged, within 15 days after receiving the application of the data subject, to provide him with information about what personal data of that entity and to which third parties were provided their personal data during the year preceding the filing date statements, or notify the data subject the reasons for refusing it providing.

### Format of response

See Article 12(1) in section 5.1. above.

Article 11(2): The operator is required to provide the data subject with the information specified in Article 11(1) in an accessible form.

Article 14(3): The response to the application is sent to the subject of personal data in the form of the relevant application form, unless otherwise stated in the application itself.

### Exceptions

See Article 12(5) in section 5.1. above.

Article 11(3): The information specified in the first part of paragraph 1 of this article, shall not be provided if:

- if personal data can be obtained by any person by sending a request in the manner prescribed by law, or by accessing an information resource (system) on the global computer network Internet;
- if the processing of personal data is carried out: in accordance with the legislation on state statistics;
- in accordance with the legislation in the field of national security, on defence, on the fight against corruption, on the fight against terrorism and countering extremism, on the prevention of legalisation of proceeds from crime, the financing of terrorist activities and the financing of the proliferation of weapons of mass destruction, on the State Border of the Republic of Belarus;
- in accordance with the legislation on operational-search activities, on administrative penitentiary legislation or criminal procedure;

### Exceptions

See Article 12(5) in section 5.1. above.

- on the issues of conducting forensic records; and
- in other cases provided for by legislative acts.
- Article 12(3): The information specified in this article may not be provided in the cases provided for in paragraph 3 of Article 11 of this Law, as well as if the processing of personal data is carried out on enforcement proceedings, in the administration of justice and the organisation of the activities of courts of general jurisdiction.



## 5.5. Right not to be subject to discrimination

Unlike the GDPR, which provides the right not to be subject to decisions based on automated processing, and implies the right not to be subject to discrimination, the PDP Law does not establish either right.

### Definition of right

The GDPR only implies this right and does not provide an explicit definition for it.

The PDP Law does not refer to or address this right.

### Automated processing

Article 22(1): The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her. [Article 22 goes on to detail this right, including exceptions]

The PDP Law does not refer to or address this right.





## 5.6. Right to data portability

Unlike the GDPR, the PDP Law does not refer to a right to data portability.

GDPR	PDP Law
------	---------

### Grounds for portability

Article 20(1): The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, where:

- (a) the processing is based on consent pursuant to point (a) of Article 6(1) or point (a) of Article 9(2) or on a contract pursuant to point (b) of Article 6(1); and
- (b) the processing is carried out by automated means.

The PDP Law does not explicitly provide a right to data portability.

### Inform data subject of right

See Article 12(1) in section 5.1.

The PDP Law does not explicitly provide a right to data portability.

### Fees

See Article 12(5) in section 5.1. above.

The PDP Law does not explicitly provide a right to data portability.

### Response timeframe

See Article 12(3) in section 5.1. above.

The PDP Law does not explicitly provide a right to data portability.

### Format

See Article 20(1) above.

The PDP Law does not explicitly provide a right to data portability.

### Controller to controller

Article 20(2): In exercising his or her right to data portability pursuant to paragraph 1, the data subject shall have the right to have the personal data transmitted directly from one controller to another, where technically feasible.

The PDP Law does not explicitly provide a right to data portability.

GDPR	PDP Law
------	---------

### Technically feasible

See Article 20(2) above.

The PDP Law does not explicitly provide a right to data portability.

### Exceptions

See Article 12(5) in section 5.1. above.

The PDP Law does not explicitly provide a right to data portability.



# 6. Enforcement



## 6.1. Monetary penalties

Like the GDPR, the PDP Law provides for monetary penalties and other actions relating to violations of the PDP Law. However, the GDPR provides for maximum fines and gives the option to base fine amounts on a percentage of annual turnover, while the PDP Law does not provide such information regarding penalties.

GDPR	PDP Law
------	---------

### Provides for monetary penalties

The GDPR provides for monetary penalties.

The PDP Law provides for monetary penalties.

### Issued by

Article 58(2) Each supervisory authority shall have all of the following corrective powers:  
[...] (i): to impose an administrative fine pursuant to Article 83, in addition to, or instead of measures referred to in this paragraph, depending on the circumstances of each individual case.

The PDP Law does not explicitly address this point, however Article 18(1) states that authorised body for the protection of the rights of subjects of personal data (the DPA) takes measures to protect the rights of subjects of personal data during processing personal data.  
Article 19(1): Persons guilty of violating this Law shall be liable, as provided by legislative acts.

### Fine maximum

Article 83(5): infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher:  
(a) the basic principles for processing, including conditions for consent, pursuant to Articles 5, 6, 7 and 9;  
(b) the data subjects' rights pursuant to Articles 12 to 22;  
(c) the transfers of personal data to a recipient in a third country or an international organisation pursuant to Articles 44 to 49;  
(d) any obligations pursuant to Member State law adopted under Chapter IX;  
(e) non-compliance with an order or a temporary or definitive limitation on processing or the suspension of data flows by the supervisory authority pursuant to Article 58(2) or failure to provide access in violation of Article 58(1).  
(6) Non-compliance with an order by the supervisory authority as referred to in Article 58(2) shall, in accordance with paragraph 2 of this Article, be subject to administrative fines up to 20 000 000 EUR, or in the case of an undertaking,

The PDP Law does not provide for maximum fine amounts.

GDPR	PDP Law
------	---------

### Fine maximum (cont'd)

up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher.

### Percentage of turnover

Under Article 83(4), (5), and (6), fines may be issued that equate to 2% or 4% of the total worldwide annual turnover of the preceding financial year.

The PDP Law does not provide sanctions in the form of a percentage of turnover.

### Mitigating factors

Article 83(2): When deciding whether to impose an administrative fine and deciding on the amount of the administrative fine in each individual case due regard shall be given to the following:  
(a) the nature, gravity and duration of the infringement taking into account the nature scope or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them;  
(b) the intentional or negligent character of the infringement;  
(c) any PDP Law on taken by the controller or processor to mitigate the damage suffered by data subjects;  
(d) the degree of responsibility of the controller or processor taking into account technical and organisational measures implemented by them pursuant to Articles 25 and 32;  
(e) any relevant previous infringements by the controller or processor;  
(f) the degree of cooperation with the supervisory authority, in order to remedy the infringement and mitigate the possible adverse effects of the infringement;  
(g) the categories of personal data affected by the infringement;  
(h) the manner in which the infringement became known to the supervisory authority, in particular whether, and if so to what extent, the controller or processor notified the infringement;  
(i) where measures referred to in Article 58(2) have previously been ordered against the controller or processor concerned with regard to the same subject-matter, compliance with those measures;  
(j) adherence to approved codes of conduct pursuant to Article 40 or approved certification mechanisms pursuant to Article 42; and

The PDP Law does not provide for mitigating factors.

Mitigating factors (cont'd)

(k) any other aggravating or mitigating fPDP Lawor applicable to the circumstances of the case, such as financial benefits gained, or losses avoided, directly or indirectly, from the infringement.

Imprisonment

Not applicable.

Not applicable.

DPO liability

Not applicable.

Not applicable



Fairly consistent

## 6.2. Supervisory authority

The GDPR and the PDP Law establish data protection authorities and provide them with investigatory, corrective, and advisory powers. Although the tasks and powers of these authorities vary in the particulars, there are general similar. The Belarusian DPA, the NDPC, was recently established and is expected to give official clarifications and interpretations of provisions of the personal data legislation.

Provides for data protection authority

Article 51(1): Each Member State shall provide for one or more independent public authorities to be responsible for monitoring the application of this Regulation, in order to protect the fundamental rights and freedoms of natural persons in relation to processing and to facilitate the free flow of personal data within the Union ('supervisory authority').

Article 18(1): The authorised body for the protection of the rights of subjects ('DPA') takes measures to protect the rights of subjects of personal data during processing of personal data.  
Article 18(2): the DPA acts independently on the basis of the PDP Law and other legislative acts. It is not allowed to impose functions that are incompatible with protecting the rights of data subjects, with the exception of the processing of personal data when exercise of the powers provided for in Article 18(3).

Investigatory powers

Article 58(1): Each supervisory authority shall have all of the following investigative powers:

- (a) to order the controller and the processor, and, where applicable, the controller's or the processor's representative to provide any information it requires for the performance of its tasks;
- (b) to carry out investigations in the form of data protection audits;
- (c) to carry out a review on certifications issued pursuant to Article 42(7);
- (d) to notify the controller or the processor of an alleged infringement of this Regulation;
- (e) to obtain, from the controller and the processor, access to all personal data and to all information necessary for the performance of its tasks;
- (f) to obtain access to any premises of the controller and the processor, including to any data processing equipment and means, in accordance with Union or Member State procedural law.

Article 18(3): The authorised body for the protection of the rights of subjects of personal data: monitors the processing of personal data by operators in accordance with legislative acts, and considers complaints of data subjects.

[Please note: further detail on the powers of the Belarusian DPA is yet to be given.]

## Corrective powers

Article 58(2): Each supervisory authority shall have all of the following corrective powers:

- (a) to issue warnings to a controller or processor that intended processing operations are likely to infringe provisions of this Regulation;
- (b) to issue reprimands to a controller or a processor where processing operations have infringed provisions of this Regulation;
- (c) to order the controller or the processor to comply with the data subject's requests to exercise his or her rights pursuant to this Regulation;
- (d) to order the controller or processor to bring processing operations into compliance with the provisions of this Regulation, where appropriate, in a specified manner and within a specified period;
- (e) to order the controller to communicate a personal data breach to the data subject;
- (f) to impose a temporary or definitive limitation including a ban on processing;
- (g) to order the rectification or erasure of personal data or restriction of processing pursuant to Articles 16, 17 and 18 and the notification of such PDP Lawions to recipients to whom the personal data have been disclosed pursuant to Article 17(2) and Article 19;
- (h) to withdraw a certification or to order the certification body to withdraw a certification issued pursuant to Articles 42 and 43, or to order the certification body not to issue certification if the requirements for the certification are not or are no longer met;
- (i) to impose an administrative fine pursuant to Article 83, in addition to, or instead of measures referred to in this paragraph, depending on the circumstances of each individual case;
- (j) to order the suspension of data flows to a recipient in a third country or to an international organisation.

Article 18(3): the DPA can require operators to change, block, or delete inaccurate or unlawfully obtained personal data.

[Please note: further detail on the powers of the Belarusian DPA is yet to be given.]

## Authorisation/ advisory powers

Article 58(3): Each supervisory authority shall have all of the following authorisation and advisory powers:

- (a) to advise the controller in accordance with the prior consultation procedure referred to in Article 36;
- (b) to issue, on its own initiative or on request, opinions to the national parliament, the Member State government or, in accordance with Member State law, to other institutions and bodies as well as to the public on any issue related to the protection of personal data;
- (c) to authorise processing referred to in Article 36(5), if the law of the Member State requires such prior authorisation;
- (d) to issue an opinion and approve draft codes of conduct pursuant to Article 40(5);
- (e) to accredit certification bodies pursuant to Article 43;
- (f) to issue certifications and approve criteria of certification in accordance with Article 42(5);
- (g) to adopt standard data protection clauses referred to in Article 28(8) and in point (d) of Article 46(2);
- (h) to authorise contrPDP Lawual clauses referred to in point (a) of Article 46(3);
- (i) to authorise administrative arrangements referred to in point (b) of Article 46(3);
- (j) to approve binding corporate rules pursuant to Article 47.

Article 18(3): The authorised body for the protection of the rights of subjects of personal data:

- exercises control over the processing of personal data by operators (authorised persons) in accordance with legislative acts;
- considers complaints of personal data subjects regarding the processing of personal data;
- requires operators (authorised persons) to change, block, or delete false or illegally obtained personal data, eliminate other violations of this Law;
- determines the list of foreign states on whose territory an appropriate level of protection of the rights of personal data subjects is ensured;
- issues permits for cross-border transfer of personal data if an adequate level of protection of the rights of personal data subjects is not ensured in the territory of a foreign state; participates in the preparation of draft acts of legislation on personal data;
- gives clarifications on the application of legislation on personal data, conducts other explanatory work on legislation on personal data;
- participates in the work of international organisations on the protection of personal data;
- annually, no later than 15 March, publishes in the media a report on its activities for the previous year; and
- exercise other powers provided for by this Law and other legislative acts.

## Tasks of authority

Article 57(1): Without prejudice to other tasks set out under this Regulation, each supervisory authority shall on its territory:

- (a) monitor and enforce the application of this Regulation;
- (b) promote public awareness and understanding of the risks, rules, safeguards and rights in relation to processing. Activities addressed specifically to children shall receive specific attention;
- (c) advise, in accordance with Member State law, the national parliament, the government, and other institutions and bodies on legislative and administrative measures relating to the protection of natural persons' rights and freedoms with regard to processing;
- (d) promote the awareness of controllers and processors of their obligations under this Regulation;

Please see Article 18(3) above.

## Tasks of authority

(e) upon request, provide information to any data subject concerning the exercise of their rights under this Regulation and, if appropriate, cooperate with the supervisory authorities in other Member States to that end;

(f) handle complaints lodged by a data subject, or by a body, organisation or association in accordance with Article 80, and investigate, to the extent appropriate, the subject matter of the complaint and inform the complainant of the progress and the outcome of the investigation within a reasonable period, in particular if further investigation or coordination with another supervisory authority is necessary;

(g) cooperate with, including sharing information and provide mutual assistance to, other supervisory authorities with a view to ensuring the consistency of application and enforcement of this Regulation;

(h) conduct investigations on the application of this Regulation, including on the basis of information received from another supervisory authority or other public authority;

(i) monitor relevant developments, insofar as they have an impact on the protection of personal data, in particular the development of information and communication technologies and commercial practices;

(j) adopt standard contractual clauses referred to in Article 28(8) and in point (d) of Article 46(2);

(k) establish and maintain a list in relation to the requirement for data protection impact assessment pursuant to Article 35(4);

(l) give advice on the processing operations referred to in Article 36(2);

(m) encourage the drawing up of codes of conduct pursuant to Article 40(1) and provide an opinion and approve such codes of conduct which provide sufficient safeguards, pursuant to Article 40(5);

(n) encourage the establishment of data protection certification mechanisms and of data protection seals and marks pursuant to Article 42(1), and approve the criteria of certification pursuant to Article 42(5);

(o) where applicable, carry out a periodic review of certifications issued in accordance with Article 42(7);

(p) draft and publish the criteria for accreditation of a body for monitoring codes of conduct pursuant to Article 41 and of a certification body pursuant to Article 43;

(q) conduct the accreditation of a body for monitoring codes of conduct pursuant to Article 41 and of a certification body pursuant to Article 43;

Please see Article 18(3) above.

## Tasks of authority (cont'd)

(r) authorise contractual clauses and provisions referred to in Article 46(3);

(s) approve binding corporate rules pursuant to Article 47;

(t) contribute to the activities of the Board;

(u) keep internal records of infringements of this Regulation and of measures taken in accordance with Article 58(2); and

(v) fulfil any other tasks related to the protection of personal data.

## Annual report

Article 59: Each supervisory authority shall draw up an annual report on its activities, which may include a list of types of infringement notified and types of measures taken in accordance with Article 58(2). Those reports shall be transmitted to the national parliament, the government and other authorities as designated by Member State law. They shall be made available to the public, to the Commission and to the Board.

Please see Article 18(3) above.





## 6.3. Civil remedies for individuals



Fairly inconsistent

Neither the GDPR nor the PDP Law specify how monetary damages will be calculated. The GDPR and the PDP Law differ, however, in regard to mandates for representation, processor liabilities, and exceptions from such compensation. Further to this, the PDP Law does not establish civil liabilities, as these are covered by the Code on Administrative Liability (only available in Russian here) ('the Code on Administrative Liability').

GDPR	PDP Law
------	---------

### Provides for claims/ cause of PDP Lawion

Article 79: Without prejudice to any available administrative or non-judicial remedy, including the right to lodge a complaint with a supervisory authority pursuant to Article 77, each data subject shall have the right to an effective judicial remedy where he or she considers that his or her rights under this Regulation have been infringed as a result of the processing of his or her personal data in non-compliance with this Regulation.

Article 15(1): The data subject has the right to appeal against actions, or inaction, and decisions of the operator that violate their rights when processing personal data, to the DPA established by the legislation on appeals of citizens and legal entities.

### Material and non-material damage

Article 82(1): Any person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered.

Article 19(2): Moral harm caused to the subject of personal data due to violations of their rights established by this Law shall be subject to compensation. Reimbursement moral harm carried out whatever from reimbursement property damage and losses incurred by the subject of personal data.

### Mandate for representation

Article 80(1): The data subject shall have the right to mandate a not-for-profit body, organisation or association which has been properly constituted in accordance with the law of a Member State, has statutory objectives which are in the public interest, and is PDP Lawive in the field of the protection of data subjects' rights and freedoms with regard to the protection of their personal data to lodge the complaint on his or her behalf, to exercise the rights referred to in Articles 77, 78 and 79 on his or her behalf, and to exercise the right to receive compensation referred to in Article 82 on his or her behalf where provided for by Member State law.

The PDP Law does not address this point.

### Specifies amount for damages

Not applicable.

Not applicable.

GDPR	PDP Law
------	---------

Article 82(2): Any controller involved in processing shall be liable for the damage caused by processing which infringes this Regulation. A processor shall be liable for the damage caused by processing only where it has not complied with obligations of this Regulation specifically directed to processors or where it has acted outside or contrary to lawful instructions of the controller.

Article 7(3): In the event that the operator instructs the processing of personal data to an authorised person, the operator is responsible for the actions of said person. The authorised person is responsible to the operator.

### Exceptions

Article 82(3): A controller or processor shall be exempt from liability under paragraph 2 if it proves that it is not in any way responsible for the event giving rise to the damage.

The PDP Law does not provide explicit exceptions from compensation.



