Comparing privacy laws:
GDPR v. Kenya Data Protection Draft Law

OneTrust DataGuidance™
REGULATORY RESEARCH SOFTWARE

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 regulations 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

Introduction 5

1. Scope
1.1. Personal scope 7
1.2. Territorial scope 9
1.3. Material scope 10

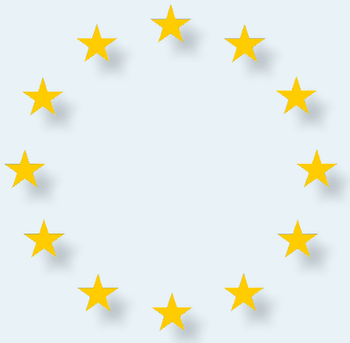
2. Key definitions
2.1. Personal data 13
2.2. Pseudonymisation 15
2.3. Controller and processors 16
2.4. Children 18
2.5. Research 19

3. Legal basis 21

4. Controller and processor obligations
4.1. Data transfers 23
4.2. Data processing records 25
4.3. Data protection impact assessment 30
4.4. Data protection officer appointment 32
4.5. Data security and data breaches 34
4.6. Accountability 36

5. Individuals' rights
5.1. Right to erasure 37
5.2. Right to be informed 41
5.3. Right to object 45
5.4. Right of access 48
5.5. Right not to be subject to discrimination 51
5.6. Right to data portability 52

6. Enforcement
6.1. Monetary penalties 54
6.2. Supervisory authority 57
6.3. Civil remedies for individuals 63



Introduction

The General Data Protection Regulation (Regulation (EU) 2016/679) ('GDPR') came into effect on 25 May 2018 and governs the protection of personal data in EU and EEA Member States. Ukraine's draft Law on Personal Data Protection (only available in Ukrainian here) ('the Draft Law') was introduced, on 7 June 2021 to the Parliament of Ukraine ('Verkhovna Rada') and is currently under consideration. If passed, the Draft Law would establish a supervisory authority to exercise supervision and control over compliance with the requirements of the Draft Law.

In general terms, there are broad similarities between the GDPR and the Draft Law. The two legislations address matters such as data subject rights, provide lawful bases for data processing, and impose restrictions on international data transfers. Furthermore, the Draft Law imposes similar responsibilities on data controllers with regards to the protection of personal data including the implementation of Privacy by Design, the appointment of a data protection officer, and the conducting of Data Protection Impact Assessments ('DPIA'). However, the Draft Law and the GDPR differ in some respects, in particular, the Draft Law provides minimal information on the powers of the supervisory authority while the GDPR contains detailed information on this matter. Moreover, the Draft Law establishes data processing requirements for specific types of processing activities including the processing of biometric data, video surveillance, audio, and video, or photo recording of public events, while the GDPR only provides processing requirements for general and sensitive personal information.

This overview organises provisions from the GDPR and the Draft 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 Draft Law.

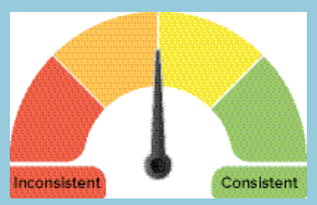
Key for giving the consistency rate

Consistent: The GDPR and the Draft 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 Draft 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 Draft 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 Draft 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 Draft Lawed upon without specific legal advice based on particular circumstances.

1. Scope

1.1. Personal scope

The Draft Law and the GDPR both regulate the processing of personal data by private organisations as well as public bodies. However, unlike the GDPR, the Draft Law does not explicitly refer to the nationality or place of residence of personal data subjects. Further to this, the Draft Law addresses the processing of the personal information of deceased persons while the GDPR is silent on this matter.

GDPR	Draft 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 2(1): 'personal data controller' means any natural or legal person, subject of authority or any other body that independently or jointly with others determines the purposes and means of processing personal data, as well as other natural or legal persons for whom the purposes and methods of processing are determined by law.
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 2(1): 'personal data operator' means a natural or legal person, a subject of authority or any other body that processes personal data on behalf of the controller and is authorised to do so by him or by law.
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 fDraft Lawors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.	Article 2(1): 'personal data subject' means an individual whose personal data is processed.
Public bodies	
Article 4(7): 'controller' means the natural or legal person, public authority, agency or other body.	Article 2(1): 'personal information controller' means any natural or legal person, subject of authority or any other body.

GDPR	Draft Law

Nationality of data subject

GDPR	Draft Law
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 Draft Law does not explicitly refer to the nationality of data subjects. However, Article 33 of the Draft Law provides that a controller or operator that is established and/or operates in other states must appoint its representative on the territory of Ukraine for one of the following conditions: • the processing of personal data is related to the provision of goods, works or services on a paid or gratuitous basis to personal data subjects located on the territory of Ukraine; • the processing of personal data is related to monitoring the behaviour of personal data subjects during their stay in Ukraine; or • the controller processes personal data of Ukrainian citizens.

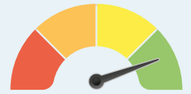
Place of residence

See Recital 14, above.	The Draft Law does not explicitly refer to the place of residence of data subjects. However, please see Article 33 above

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.	Article 16 provides rules for the processing of personal data after the death of the personal data subject. Specifically, Article 16(1) outlines that the consent of the personal data subject is valid for 10 years after his/her death, and if the data subject died before the age of 18, his/her consent would be valid for 20 years after their death, unless the data subject decided differently prior to their death.

1.2. Territorial scope



The GDPR and the Draft Law bear many similarities in terms of territorial scope. In particular, the Draft Law, analogous to the GDPR, has extraterritorial application, applying to personal data controllers and operators that function outside of Ukraine in relation to the provision of services to personal data subjects located on the territory of Ukraine, monitoring the behaviour of personal data subjects during their stay in Ukraine, and where the controller processes personal data of Ukrainian citizens.

GDPR	Draft Law

Establishment in jurisdiction

GDPR	Draft Law
Article 3: This Regulation applies to the processing of personal data in the context of the Draft Lawivities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not. Recital 22: Establishment implies the effective and real exercise of Draft Lawivity through stable arrangements.	The Draft Law does not explicitly refer to personal data controllers or operators being established within Ukraine. However, Article 33 of the Draft Law provides that a controller or operator that is established and/or operates in other states must appoint its representative on the territory of Ukraine for one of the following conditions: • the processing of personal data is related to the provision of goods, works, or services on a paid or gratuitous basis to personal data subjects located on the territory of Ukraine; • the processing of personal data is related to monitoring the behaviour of personal data subjects during their stay in Ukraine; and • the controller processes personal data of Ukrainian citizens.

Extraterritorial

See Article 3, above.	Please see Article 33 above.

Goods & servicies 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 Draft Lawivities are related to offering goods or services to such data subjects irrespective of whether connected to a payment.	Please see Article 33 above.

GDPR	Draft Law
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.	Please see Article 33 above.

1.3. Material scope

The Draft Law and the GDPR adopt similar concepts of personal data, data processing, as well as pseudonymised and anonymised data, referred to as 'depersonalisation of personal data' under the Draft Law. In addition, both legislations provide general exceptions for the processing of personal data for purely personal or household activities and afford enhanced protection to certain types of personal data, including data related to racial or ethnic origin, political, religious or ideological beliefs, membership in trade unions, as well as genetic and biometric data, and data related to health.

GDPR	Draft 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 fDraft Lawors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.	Article 2(1): 'personal data' means any information concerning an individual who is identified or 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 2(1): 'processing of personal data' means any action or set of actions with personal data with or without the use of automated means, in particular collection, recording, ordering, structuring, storage, adaptation, modification, restoration, familiarisation, pseudonymisation, profiling, depersonalisation, use, disclosure by transmitting or distributing or otherwise providing access, grouping or combining, restriction, deletion, or destruction.
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.	The Draft Law does not explicitly define special categories of data. However, Article 7(1) which provides special requirements for the processing of personal data (sensitive personal data) establishes that the processing of personal data on racial or ethnic origin, political, religious or ideological beliefs, membership in trade unions, as well as genetic and biometric data, data related to health, sexual life or sexual orientation, and psychometric data is prohibited.

GDPR	Draft 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.

Article 2(1): 'depersonalisation of personal data' means a set of measures to permanently remove from aggregate data about an individual any information that allows identifying an individual and/or in relation to the irreversible break of any connection between the information and the individual.

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 2(1): 'pseudonymisation' means the processing of personal data in a way that does not allow for the identifying of the subject of personal data without using additional information, which must be stored separately using all necessary technical and organisational measures that do not make it possible to recreate communication with the subject of personal data or identify him.

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 1(1): This Law applies to relations related to the processing of personal data using automated means, as well as to the processing of personal data contained in a file cabinet or assigned before entering it in file cabinets, using non-automated means.

General exemptions

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

(a) in the course of an Draft Lawivity which falls outside the scope of Union law;

(b) by the Member States when carrying out Draft 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 Draft Lawivity.

Article 1(3): This Law does not apply to the processing of personal data by individuals for personal or household needs that are not related to the implementation of professional or any other activity aimed at making a profit.

Article 1(4): The processing of personal data for personal or household needs covers, in particular, the maintenance of correspondence and the preservation of postal (electronic) addresses, the maintenance of social contacts, as well as communication on the Internet, which is carried out in the context of such activities.

2. Key definitions

2.1. Personal data

The Draft Law and GDPR both provide definitions of personal data, health, biometric, and genetic data. However, unlike the GDPR, the Draft Law does not explicitly define special categories of personal data, nor does it define 'online identifiers.'

GDPR	Draft 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 fDraft Lawors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Article 2(1): 'personal data' means any information concerning an individual who is identified or 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.

The Draft Law does not explicitly define special categories of data.

However, Article 7(1) which provides special requirements for the processing of personal data (sensitive personal data) establishes that the processing of personal data on racial or ethnic origin, political, religious or ideological beliefs, membership in trade unions, as well as genetic and biometric data, data related to health, sexual life or sexual orientation, and psychometric data is prohibited.

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 Draft Law does not explicitly refer to online identifiers.

GDPR	Draft Law
Health Data	
Article 4(15): 'data concerning health' means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status.	Article 2(1): 'health data' means personal data about the state of physical or mental health of an individual, including data on the provision of medical services or assistance, which contain information about the state of health of an individual.
Biometric Data	
Article 4(14): 'biometric data' means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data.	Article 2(1): 'biometric data' personal data concerning physical, physiological or behavioural characteristics of an individual, which, as a result of special technical processing, make it possible to identify or verify an individual.
Genetic Data	
Article 4(13):'genetic data' means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question.	Article 2(1): 'genetic data' personal data concerning the innate or acquired genetic characteristics of an individual, which provide unique information about the physiology or health of such an individual and such that obtained, in particular, as a result of the analysis of a biological sample taken from the relevant individual.

2.2. Pseudonymisation

The Draft Law and GDPR both provide a definition for the anonymisation/depersonalisation of personal data and pseudonymisation. In addition, both legislations require the implementation of technical and organisational measures to ensure that personal data is not attributable to a data subject.

GDPR	Draft 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.	Article 2(1): 'depersonalisation of personal data' means a set of measures to permanently remove from aggregate data about an individual any information that allows identifying an individual and/or in relation to the irreversible break of any connection between the information and the individual.
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 2(1): 'pseudonymisation' means the processing of personal data in a way that does not allow for the identifying of the subject of personal data without using additional information, which must be stored separately using all necessary technical and organisational measures that do not make it possible to recreate communication with the subject of personal data or identify him.

2.3. Controllers and processors

The Draft Law and the GDPR both provide definitions of personal data controller/ data controllers and operator/data processors, respectively, and require the execution of a contract between the same. In addition, both the GDPR and Draft Law do not contain explicit definitions of data protection officer and DPIA.

GDPR	Draft 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 2(1): 'personal data controller' means any natural or legal person, subject of authority or any other body that independently or jointly with others determines the purposes and means of processing personal data, as well as other natural or legal persons for whom the purposes and methods of processing are determined by law.

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 2(1): 'personal data operator' means a natural or legal person, a subject of authority or any other body that processes personal data on behalf of the controller and is authorised to do so by him or by law.

Controller and processor contracts

Article 28(3): Processing by a processor shall be governed by a contrDraft Law or other legal Draft 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 contrDraft Law.]

Article 31(3): The processing of personal data by the operator must be carried out on the basis of a contract or regulatory legal act, which must foresee the type and categories of personal data to be processed, the term, nature and purpose of processing, the type and categories of personal data subjects whose data is subject to processing, and the rights and obligations of the controller.

[Article 31 goes on to stipulate necessary information to be included in such a contract.]

GDPR	Draft Law

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).

Assessment of the impact of personal data processing is not specifically defined, however Article 39 sets out requirements for such assessments (see section 4.3. for further information).

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).

The responsible person for personal data protection is not specifically defined, however Article 41 sets out requirements related to such person (see section 4.4. for further information).

2.4. Children

Both the GDPR and the Draft Law address the processing of children/minors' personal data and require consent from their parent/guardian or legal representative to process such personal data. Notably, the GDPR outlines requirements for privacy notice aimed at children/minors while the Draft Law is silent on the matter.

GDPR	Draft 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 Draft Law does not explicitly define 'child' or 'minor'.

However, Article 6(10) states the controller is obliged to take all reasonable measures to verify that the consent was given by a personal data subject who has reached the age of 14, and if the subject is a minor, that the consent was given on his behalf by a legal representative.

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 6(9): Consent to the processing of personal data of a minor is provided by his/her legal representative.

Please also see Article 6(10) above.

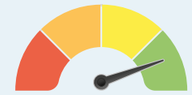
Privacy notice (children)

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 Draft Law does not provide specific requirements in relation to privacy notices for children.

However, Article 43(3)(8) states that the procedure for protecting children as subjects of personal data and providing them with information, as well as the method of withdrawing consent to the processing of personal data of young children from their representatives should be included in codes of conduct for personal data protection.

2.5. Research



Both the GDPR and the Draft Law permit personal data to be processed for scientific research purposes including historical, archiving, or statistical purposes, allowing for further processing on this basis as well as the limitation of data subject rights in specific circumstances. Moreover, both legislations require the implementation of appropriate safeguards to protect the rights and freedoms of personal data subjects when further processing personal data.

GDPR	Draft 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.

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.

The Draft Law refers to the processing of personal data for archiving purposes in the public interest, for scientific or historical research purposes, or for statistical purposes but does not provide definitions thereof.

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').

Article 13(1): The processing of personal data for a different purpose (new purpose) than the one for which it was collected (primary purpose) is prohibited, unless the new purpose is compatible with the primary one [...]
Article 13(2): Processing for archiving purposes in the public interest, for scientific or historical research purposes, or for statistical purposes is considered to be processing compatible with the original purpose.

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

Article 13(1): To determine whether the new goal is compatible with the primary goal, the following criteria are taken into account [...]:

- the availability of appropriate and sufficient guarantees to protect the rights and freedoms of the personal data subject in the primary processing of personal data and processing that is planned, which may include encryption or pseudonymisation.

GDPR	Draft Law

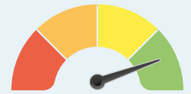
Data subject rights (research)

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.

Article 14(2): The controller that processes personal data for the purpose of scientific or historical research may restrict the rights of the subject of personal data provided for in Articles 19, 21, 22, 24 of this Law, to the extent that their implementation will lead to the impossibility of achieving these goals and such restriction is necessary to achieve them.

Restrictions on the rights of the personal data subject provided for in Article 14(2) of this Law are legitimate if technical and organisational measures are taken to comply with the principle of personal data minimisation.

3. Legal basis



The Draft Law and GDPR outline grounds for the lawful processing of general and special category personal information. Further to this, both legislations provide detailed requirements for valid consent from data subjects and expressly provide data subjects with a right to withdraw consent at any time. Furthermore, the Draft Law, similar to the GDPR, provides exemptions in regard to processing for journalism and artistic/creative purposes.

GDPR	Draft 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 contrDraft Law 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 contrDraft Law;

(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 5(1): The processing of personal data is lawful in the following cases:

1) giving the consent of the personal data subject to the processing of his / her personal data for one or more precisely defined purposes;

2) the conclusion and execution of a transaction to which the personal data subject is a party, as well as the implementation of measures necessary for the conclusion of a transaction, at the request of the personal data subject;

3) the need to fulfil the legal obligation of the personal data controller;

4) protection of vital interests of the personal data subject or other natural person;

5) the need to perform tasks in the public interest or the powers assigned to the controller by law; and

6) necessary for the purposes of a legitimate interest of the controller or a third party, unless such interests are not dominated by the interests or fundamental rights and freedoms of the personal data subject, which require the protection of personal data, especially if the personal data subject is a child.

GDPR	Draft Law

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 (sensitive personal data), see Article 7 of the Draft 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 Draft Lawion, signifies agreement to the processing of personal data relating to him or her.

Article 6(8): If the processing of personal data is carried out on the basis of the consent of the personal data subject, the relevant subject has the right to withdraw consent at any time.

Article 6(1)(3): The consent of the personal data subject to the processing of his/her personal data may be provided by [...]:

- by selecting the appropriate technical settings in the website interface, operating system, software, or mobile application that provides for the processing of personal data; and
- through another affirmative action or behaviour that clearly indicates that the subject of personal data in a particular case agrees to the processing of his 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 15(1): The provisions of Article 4(1)(1) concerning the principles of integrity and transparency, Article 4(1)(4)(6), Articles 18-27, 34, and 36-40 of the Law do not apply to the processing of personal data for the purposes of journalistic and creative activities.

Article 15(2): Article 15(1) applies only if the controller processes personal data exclusively for the purposes of journalistic and creative activities, reasonably believes that the disclosure of information is carried out in the public interest, and the harm from the disclosure of such information exceeds the public interest in obtaining it.

4. Controller and processor obligations

4.1. Data transfers

Fairly consistent

The PDPA and GDPR both provide for data transfers based on adequate protection. In addition, both legislations outline additional mechanisms including contractual clauses or corporate rules to enable international data transfers, and do not contain requirements for data residency.

GDPR	Draft 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 44(1)(1): The transfer of personal data to foreign states and/or international organisations may be carried out by the controller where a foreign state or an international organisation provides an adequate level of personal data protection.

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);
(e) an approved code of conduct pursuant to Article 40 together

Article 44(1)(2)(3): The transfer of personal data to foreign states and/or international organisations may be carried out by the controller in the following cases [...]:

the controller and / or operator have provided adequate guarantees for the protection of personal data.
mandatory corporate rules have been approved in accordance with the requirements of this Law.
Article 44(2): Personal data may also be transferred to a foreign State or an international organisation in the cases provided for by this Law.

GDPR	Draft Law
Other mechanisms for data transfers (cont'd)	
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 (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. (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: (a) contrDraft Lawual 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 (b) provisions to be inserted into administrative arrangements between public authorities or bodies which include enforceable and effective data subject rights.	
Data localisation	
Not applicable.	Not applicable.

4.2. Data processing records

Fairly consistent

The GDPR and the Draft Law both impose an obligation on controllers and processors/operators to record their processing activities, and require such records be made available to supervisory authorities where requested. Furthermore, the Draft Law requires personal information controllers and operators to register with the supervisory authority while the GDPR does not.

GDPR	Draft Law
Data controller obligation	
Article 30(1): Each controller and, where applicable, the controller's representative, shall maintain a record of processing Draft Lawivities under its responsibility. That record shall contain all of the following information: (a) the name and contDraft Law 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).	Article 34(1): Each controller or, if available, a representative of the controller is obliged to register operations related to the processing of personal data, for which the controller is responsible. Transactions are registered by keeping a protocol. The protocol for processing personal data must contain information about: • the name(s) and contact details of the controller, if any, the general controller, the controller's representative and the responsible person for personal data protection; • purpose of processing; • description of categories of personal data subjects and categories of personal data; • categories of recipients to whom personal data has been or may be disclosed, including recipients in other States or international organisations; • transfer of personal data to other states or international organisations, including the name of this state or international organisation, as well as in the case of transfer of personal data to another state in accordance with part four of Article 48 of this Law - information on documents confirming the existence of appropriate protective guarantees; • time limit for deleting various categories of personal data, if possible; and • a general description of the technical and organisational security measures provided for in the first part of Article 35 of this Law.

GDPR	Draft Law

Data processor obligation

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

(a) the name and contDraft Law details of the processor or processors and of each controller on behalf of which the processor is Draft 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 34(2): Each operator and, if available, a representative of the operator must register all types of processing operations that are performed on behalf of the controller, by maintaining a protocol. The protocol must contain information about:

- the name(s) and contact details of the operator(s), the name of each controller on whose behalf the processing is carried out, if there is a representative of the controller or operator and a person responsible for personal data protection;
- categories of actions for processing personal data performed on behalf of each controller;
- transfer of personal data to other states or international organisations, including the name of this state or international organisation, as well as in the case of transfer of personal data to another state in accordance with part four of Article 48 of this Law - information on documents confirming the existence of appropriate protective guarantees; and
- a general description of the technical and organisational security measures provided for in Article 35 of this Law.

Records format

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

The Draft Law does not contain specific requirements for the format of the protocol.

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.

Article 34(3): The controller or operator, as well as the controller's or operator's representative in case of appointment, are obliged to provide protocols of personal data processing to the supervisory authority in response to the request.

GDPR	Draft Law

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.

Article 34(4): 4. The provisions of Article 34 (1) and (2) shall not apply to microenterprise entities, enterprises, organisations and institutions, regardless of their form of ownership and legal form, with fewer than 10 employees, unless:

- processing of personal data may pose a risk of violation of the rights and freedoms of the personal data subject;
- the processing of personal data is systematic; and
- personal data is processed in accordance with the first part of Article 7 and Article 8 of this Law.

General Data Processing Notification ('DPN')

Not applicable.

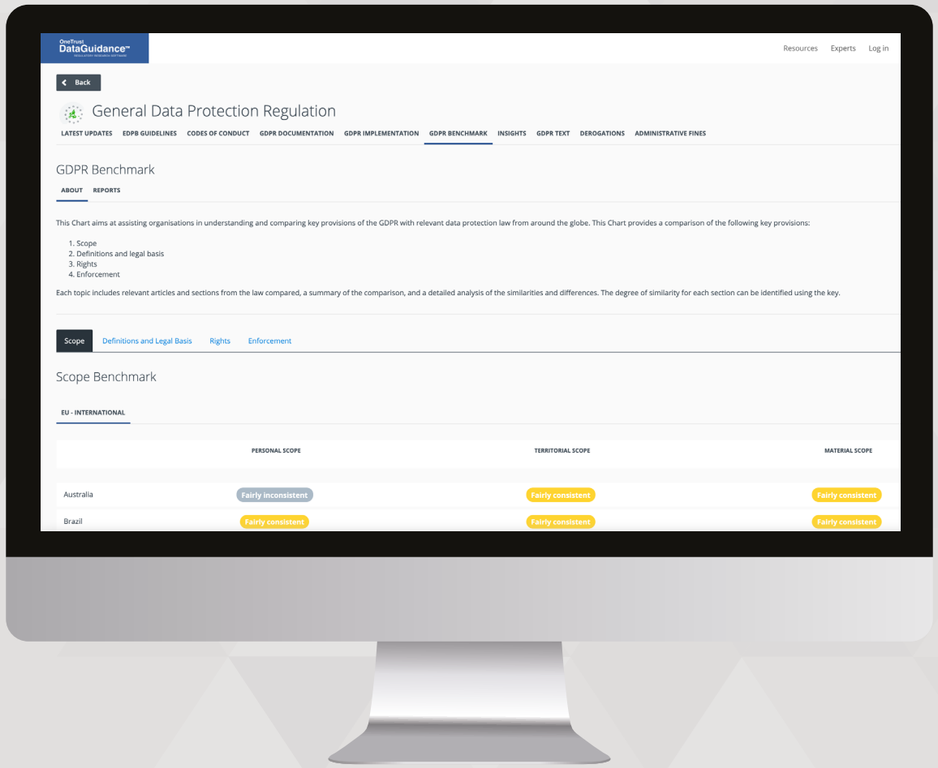
Article 34(1)(2): Each controller and operator or, if available, a representative of the controller or operator is obliged to register operations related to the processing of personal data, for which the controller is responsible. Transactions are registered by keeping a protocol.

Please see Articles 34(1)(2) above for further information on protocols.

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™
REGULATORY RESEARCH SOFTWARE

Start your free trial at
www.dataguidance.com

4.3. Data protection impact assessment

The GDPR and Draft Law contain similar provisions regarding DPIA and assessments of the impact of personal data processing, respectively. In particular, both legislations outline requirements for when an assessment must be conducted, the content of the assessment, and consultation with relevant authorities.

GDPR	Draft 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.

[...] (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.

Article 39(1): The controller is obliged to assess the impact of the processing of personal data on the protection of personal data, prior to the start of such processing, if the use of new technologies or the nature, scope, context and purpose of the processing is likely to lead to a high level of risk to the rights and freedoms of an individual.

[...]

Article 39(3)(3): The impact assessment provided for in Article 39(1) shall be carried out in the event of the implementation of:

- systematic and large-scale analysis of personal aspects of the life of individuals, which is carried out by automated processing tools, including profiling, and on the results of which decisions are based that have legal consequences for the individual or any other similar way affecting it;
- large-scale processing of personal data provided for in Articles 7 and 8 of this Law; and
- systematic and large-scale monitoring of publicly accessible places or sources.

[Please see the definition of large-scale monitoring in Article 2(1) of the Draft Law.]

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;

- information on the assessment of the necessity and proportionality of processing personal data for the following purposes;
- information on risk assessment for the rights and freedoms of personal data subjects; and
- information on measures that are envisaged to respond to risks, including guarantees, security measures and mechanisms to ensure the protection of personal data and demonstrate compliance with the requirements of this Law.

GDPR	Draft Law

DPIA content requirements (cont'd)

(c) an assessment of the risks to the rights and freedoms of data subjects referred to in paragraph 1; and

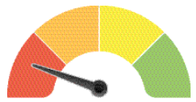
(d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned.

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].

Article 40(1): If the impact assessment carried out in accordance with Article 39 of this Law indicates that the processing of personal data may lead to a high degree of risk due to the lack of measures taken to eliminate them, the controller is obliged to conduct a preliminary consultation with the supervisory authority before starting the processing of personal data.

4.4. Data protection officer appointment



Inconsistent

The Draft Law provides for the appointment of a responsible person for personal data protection, similar to the DPO requirements under the GDPR. Specifically, both laws outline the responsibilities and qualifications of such individuals and required that DPOs and responsible persons be reported to the relevant authority. Furthermore, both the GDPR and Draft Law permit the appointment of a single DPO or responsible person for group undertakings.

GDPR	Draft Law

DPO tasks

Article 39(1): The data protection officer shall have at least the following tasks:

(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;

(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;

(c) to provide advice where requested as regards the data protection impact assessment and monitor its performance pursuant to Article 35;

(d) to cooperate with the supervisory authority; and

(e) to Draft Law as the contDraft 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.

Article 41(4): The responsible person for personal data protection must:

- provide information and recommendations to the controller or operator and employees who are directly involved in the processing of personal data about their obligations under this Law;
- monitor compliance with the requirements of this Law, including the distribution of responsibilities, and raise awareness among employees of the controller or operator on personal data protection issues that are directly involved in the processing of personal data;
- provide recommendations for assessing the impact on personal data protection and monitor its implementation;
- cooperate with the supervisory authority; and
- be a contact person for the supervisory authority on issues related to the processing of personal data, including preliminary consultations and other issues related to the implementation of the requirements of this Law.

When is a DPO required

Article 37(1): The controller and the processor shall designate a data protection officer in any case where:

(a) the processing is carried out by a public authority or body, except for courts Draft Lawing in their judicial capacity;

Article 41(1): In order to organise and implement measures to comply with the requirements of this Law, the controller and the operator must appoint a responsible person for the protection of personal data in one of the following cases:

GDPR	Draft Law

When is a DPO required (cont'd)

(b) the core Draft 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

(c) the core Draft 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.

- the processing of personal data is carried out by the subject of authority;
- the main activity of the controller or operator is the processing of personal data; by its nature, scope and / or purpose, it requires regular and systematic and large-scale monitoring of the actions or inactivity of personal data subjects;
- the main activity of the controller or operator is or is related to large-scale processing of personal data; and
- the main activity of the controller or operator is or is related to the processing of personal data defined in Articles 7-10.

Group appointments

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.

Article 41(2): General controllers or a group of operators may, by mutual agreement, determine one responsible person for the protection of personal data, if each of them has free access to it.

Notification of DPO

Article 37(7): The controller or the processor shall publish the contDraft Law details of the data protection officer and communicate them to the supervisory authority.

Article 41(10): The controller or operator must disclose the contact details of the person responsible for personal data protection and notify them to the supervisory authority.

Qualifications

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 prDraft Lawices and the ability to fulfil the tasks referred to in Article 39.

Article 41(6): A person who has at least a bachelor's degree of higher education and experience in the field of personal data protection may be appointed as the responsible person for personal data protection.

4.5. Data security and data breaches

The Draft Law and the GDPR have similar provisions with regards to security measures that should be implemented by controllers and processors/operators. In particular, both legislations require data breaches to be notified to the relevant supervisory authority within 72 hours where the breach is likely to result in harm/risk to the rights and freedoms of the individual. In addition, the Draft Law similar to the GDPR, requires operators to notify personal information controllers of data breaches without undue delay and provides exceptions to data breach notification requirements where the controller has taken appropriate and sufficient technical and organisational security measures to eliminate the possibility of violation of the rights of personal data subjects.

GDPR	Draft 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 35(1): The controller and the operator are obliged to take appropriate technical and organisational measures to ensure the proper security of personal data processing at a level comparable to the risk of personal data processing for the rights and freedoms of personal data subjects, while respecting the principle of proportionality. Security measures may include:

- pseudonymisation and encryption of personal data;
- continuous provision of confidentiality, integrity, availability of personal data and sustainability of processing systems and services;
- ensuring timely restoration of access to personal data in the event of an emergency or incident;
- regular testing, evaluation and measurement of the effectiveness of technical and organisational measures to ensure processing security; and
- ensuring compliance with the personal data processing code by employees of the controller and operator.

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 37(1): The controller is obliged to report the leak to the supervisory authority no later than 72 hours from the moment when it became aware of the leak, except in cases where the leak is unlikely to lead to a risk to the rights and freedoms of an individual.
Article 37(2): If it is impossible to make a leak report within the time period provided for in part one of this Article, the controller is obliged to inform the supervisory authority about it without undue delay from the moment when it became aware of the leak, with justification for the reasons for non-compliance with the time period provided for in part one of this Article.

GDPR	Draft Law

Timeframe for breach notification

See Article 33(1) above.

See Article 37(1)(2) 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.

Article 38(1): The controller is obliged to report a leak to the personal data subject without undue delay if there is a possibility of a high degree of risk to the rights and freedoms of an individual.

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.

Article 37(3): The operator is obliged to inform the controller about the leak without undue delay from the moment when they became aware of it.

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 38(3): The Controller is not obliged to report a personal data subject's leak if one of the following conditions is met:

- the controller has taken appropriate and sufficient technical and organisational security measures and such measures have been applied to the personal data affected by the leak, in particular, to eliminate the possibility of violation of the rights of personal data subjects.
- the controller has taken measures to prevent the occurrence of high risks to the rights and freedoms of the personal data subject; and
- the message represents an excessive burden for the controller.

Article 38(4): If notifying the subject of personal data is an excessive burden for the controller, it is obliged to take other measures to inform the subject of personal data about the leak, for example, to send messages using mass media, social networks and official websites.

4.6. Accountability

Both the GDPR and the Draft Law refer to the concept of accountability. In addition, both legislations contain provisions regarding the liability of data controllers and processors/operators.

GDPR	Draft Law

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.]

Article 4(7): Accountability: The Controller is responsible for compliance with the principles provided for in Article 4(1) and is obliged to take all appropriate organisational and technical measures for this purpose.

Liability of data controllers and data processors

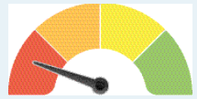
Article 82(2): Any controller involved in processing shall be liable for the damage caused by processing which infringes this Regulation. A processor shall be liable for the damage caused by processing only where it has not complied with obligations of this Regulation specifically directed to processors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

Article 26(2): The subject of personal data has the right to compensation for material and/or moral damage caused as a result of violation of his rights provided for in this Law. The controller is responsible for the violation. The operator is liable for damage caused by processing only if it does not comply with its obligations under this Law directed directly at the operator, or if the operator acts contrary to the legal instructions of the controller.

Article 26(3): The Controller is released from liability for damage caused to the subject of personal data, if it proves that the events that caused such damage did not occur through its fault and it took all reasonable measures to prevent the violation of rights and the occurrence of harm.

Article 71(3): Personal data controllers or operators may be held liable under this Law.

5. Rights



5.1. Right to erasure

The GDPR and the Draft Law offer rights to erasure and to be forgotten. In terms of the right to erasure, both legislations provide similar grounds and exceptions for exercising this right including the withdrawal of consent and the right to freedom of expression and information, respectively. In addition, both legislations outline a timeframe and format for responding to such requests. Furthermore, the Draft Law, similar to the GDPR, requires personal information controllers to notify other parties, with whom the information may have been shared, about a request.

GDPR	Draft 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 21(1): The subject of personal data has the right to be forgotten, that is, to complete destruction by the controller of his personal data without undue delay.

Article 21(2): The Controller is obliged to destroy personal data without undue delay within a period not exceeding 30 days if:

- there is no need for further processing of personal data for the purposes for which they were collected or processed;
- the personal data subject has withdrawn the consent on the basis of which the processing of personal data was carried out, and there are no other legal grounds for processing;
- the personal data subject objects to processing in accordance with the first part of Article 22 of this Law and there are no prevailing legal grounds for processing, or if the personal data subject objects to processing in accordance with the second part of Article 22 of this Law;
- the processing of personal data was carried out unlawfully; and
- personal data was collected for the purpose of offering information society services to the personal data subject.

GDPR	Draft 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.

Article 18(1)(13): If personal data is collected directly from the subject of personal data, the controller that collects personal data, upon receipt of personal data or earlier, is obliged to inform such subject of information about [...] the rights of the personal data subject in accordance with this Law.
Article 18(3): If personal data is not collected from the personal data subject, the information provided for in Article 18(1), as well as information about the sources of personal data collection, must be communicated to the personal data subject by the controller:

- no later than thirty days from the date of collection of personal data;
- if the personal data will be used for communication with the personal data subject — simultaneously with the first contact; and
- if personal data is supposed to be distributed- before the first fact of such distribution.

Fees

Article 12(5): Information provided under Articles 13 and 14 and any communication and any Draft Lawions 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 charDraft Lawer, the controller may either:
(a) charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the Draft Lawion requested; or
(b) refuse to Draft Law on the request. The controller shall bear the burden of demonstrating the manifestly unfounded or excessive charDraft Lawer of the request.

Article 27(6): The exercise of the rights of the personal data subject provided for in this Law is free of charge.

Response timeframe

Article 12(3): The controller shall provide information on Draft Lawion 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

Article 21(2) provides the controller is obliged to destroy personal data without undue delay within a period not exceeding 30 days if certain criteria are met.
Article 27(3): The controller makes a decision on the application of the personal data subject immediately, within no more than one month from the date of its receipt. If the application concerns the processing of personal data specified in Article 7 of this Law, the controller makes a decision

GDPR	Draft Law

Response timeframe

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.

within 10 days from the date of receipt of the application. If, in order to review the application in compliance with the requirements of this Law, the controller needs to obtain additional information from the personal data subject for its identification, it notifies the personal data subject about this within 10 days from the date of receipt of the application. Acceptance period the decision is counted from the day when the data subject provided the necessary information for identification. Proof of the need to obtain additional information from the personal data subject is the responsibility of the controller.

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 27(5): The controller provides the personal data subject with a written response about the decision taken on the application.

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.

Article 21(3): If the controller that is required to destroy personal data has distributed it earlier, it must take all sufficient measures, taking into account the available technological capabilities, to notify other controllers that process personal data about the request of the personal data subject to destroy any links or copies of personal data, except in cases where such notification is an excessive burden for the controller.

Exceptions

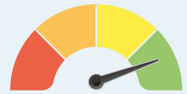
Article 17(3): Paragraphs 1 and 2 shall not apply to the extent that processing is necessary:
(a) for exercising the right of freedom of expression and information;
(b) for compliance with a legal obligation which requires processing by Union or Member State law to which the controller is subject or 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 public health in accordance with points (h) and (i) of Article 9(2) as well as Article 9(3);

Article 21(4): Article 21(1) and (2) do not apply if the processing of personal data is necessary for the following purposes:

- exercise of the right to freedom of expression and information;
- fulfilment of a legal obligation that provides for processing on the grounds specified by law;
- goals of public interest in the areas of health protection in accordance with paragraphs 7 and 8 of the first and second parts of Article 7 of this Law;
- for archiving purposes in the public interest, for scientific or historical research purposes, or for statistical purposes, if the exercise of the right provided for in

GDPR	Draft Law
Exceptions (cont'd)	
(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 Draft Lawions 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 charDraft Lawer, the controller may either: (a) charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the Draft Lawion requested; or (b) refuse to Draft Law on the request. The controller shall bear the burden of demonstrating the manifestly unfounded or excessive charDraft Lawer of the request.	this article makes it impossible or seriously hinders the achievement of the processing purposes; and • it is necessary to present, justify or defend a legal claim. Article 27(6): The controller may reasonably refuse to satisfy the application of the personal data subject if the personal data subject abuses its rights.
The The Draft Law does not provide specific exceptions to a right to erasure.	

5.2. Right to be informed



The GDPR and the Draft Law provide requirements for data controllers to notify data subjects when collecting and processing their personal data. In particular, both pieces of legislation outline what information must be disclosed and when such information must be given to data subjects. In addition, the GDPR and the Draft Law differentiate between information collected directly from the individual and information obtained from third parties. Furthermore, both legislations provide exceptions to the right to be informed including where the data subject has already been provided with the information.

GDPR	Draft 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 contDraft Law details of the controller and, where applicable, of the controller's representative; (b) the contDraft Law 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 fDraft Law 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 withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;	Article 18(1): If personal data is collected directly from the subject of personal data, the controller that collects personal data, upon receipt of personal data or earlier, is obliged to inform such subject of information about: • personal data controller - identification and contact details of the controller, and if there is a representative of the controller; • information about the operator(s), if any; • contact details of the person responsible for personal data protection by the controller; • purpose, goals, and processing methods; • actions or a set of actions that will be performed with personal data; • personal data to be processed; • grounds for processing personal data in accordance with this Law; • recipients or categories of recipients to whom personal data is or may be transferred; • transfer of personal data to foreign states or international organisations, as well as information about the presence or absence of an adequate level of protection in this state or international organisation; • the period during which personal data will be stored or the criteria for determining it, if a specific period cannot be determined at the time of collection of personal data; • the right to file a complaint with the supervisory authority and contact details of such body; • the form, content and procedure for granting or withdrawing consent to the processing of personal data, if the processing of such data is carried out on the basis of consent; • the rights of the personal data subject in accordance with this Law; • consequences related to the provision or non-provision of personal data;

GDPR	Draft Law

Informed prior to/ at collection (cont'd)

(d) the right to lodge a complaint with a supervisory authority;
(e) whether the provision of personal data is a statutory or contrDraft Lawual requirement, or a requirement necessary to enter into a contrDraft Law, 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.

- availability of an automated decision-making mechanism, including profiling and necessary information about the algorithms (logic) used in such mechanisms, as well as the significance and expected consequences of such processing for the personal data subject; and
- processing of personal data for direct marketing purposes, as well as the right to refuse to process personal data for such purposes.

What information is to be provided

See Article 13(1) and (2) above.

See Article 18(1) above.

GDPR	Draft Law

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.

Article 18(3): If personal data is not collected from the personal data subject, the information provided for in Article 18(1), as well as information about the sources of personal data collection must be communicated to the personal data subject by the controller:

- no later than 30 days from the date of collection of personal data;
- if the personal data will be used for communication with the personal data subject — simultaneously with the first contact; and
- if personal data is supposed to be distributed- before the first fact of such distribution.

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 18(5): The information specified in this Article must be provided to the subjects of personal data in an accessible way and in a clear language that ensures its clarity and comprehensibility for the relevant subjects of personal data.

Format

See Article 12(1) above.

Article 27(5): The controller provides the personal data subject with a written response about the decision taken on the application.

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;

Article 18(2): The provisions of Article 18(1) of this Article do not apply if the personal data subject already has this information.

Article 18(4): The provisions of Article 18(3) shall not apply in the following cases:

GDPR	Draft Law

Exceptions

(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 personal data subject already has the information provided for in part one of this article;
- the provision of such information is impossible due to the lack of contact details of the personal data subject or the inability to establish communication with him using the available contact details;
- collection and disclosure of personal data directly provided for by law;
- if information about the processing of personal data by the controller is a secret provided for by law; and
- if the provision of such information would place an excessive burden on the controller, in particular if the processing is carried out for archiving purposes in the public interest, for scientific or historical research purposes, or for statistical purposes, provided that the conditions provided for in Article 14 of this Law are met.

5.3. Right to object

The Draft Law and the GDPR both provide data subjects with a right to object to the processing of his/her personal data, in particular, in relation to personal data processed for direct marketing purposes. In addition, both pieces of legislation provide data subjects with a right to restrict processing with similar ground for exercising this right, and the right to withdraw consent at any time.

GDPR	Draft 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.

Article 22(1): A personal data subject has the right to object at any time to the processing of his / her personal data, which is carried out on the basis of Article 5(5) and (6) of this Law, including direct marketing and profiling based on these provisions. The controller is obliged to stop further processing, unless the processing of personal data is carried out on legal grounds that are dominated by the interests, rights and freedoms of the personal data subject, or the processing is necessary to present, justify or defend a legal claim. Bringing predominance, the legal basis for processing personal data is the responsibility of the controller.

Article 22(2): In the field of providing information society services, the subject of personal data may exercise his right to object by automated means.

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 6(8): If the processing of personal data is carried out on the basis of the consent of the personal data subject, the relevant subject has the right to withdraw consent at any time.

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:

Article 24(1): The personal data subject has the right to restrict the processing of personal data by the controller if:

GDPR	Draft Law

Restrict processing (cont'd)

(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;

(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.

- the personal data subject has appealed against the accuracy of personal data – during the period of verification of the accuracy of personal data by the controller;
- the processing of personal data is illegal and the personal data subject objects to the deletion of personal data and instead requests that their use be restricted;
- the controller no longer has the need to process personal data for the purposes of processing, but it is necessary for the personal data subject to present, justify or defend a legal claim;
- the personal data subject objected to the processing of personal data in accordance with Article 22 of this Law-before the controller makes a decision on the predominance of legitimate grounds for processing over the interests and rights of the personal 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.

Article 12(3): If personal data is processed for the purpose provided for in Article 12(1) the personal data subject has the right to withdraw his consent to such processing and the right to object to processing, including profiling for direct marketing, at any time.
Article 22(1): A personal data subject has the right to object at any time to the processing of his / her personal data, which is carried out on the basis of Article 5(5) and (6) of this Law, including direct marketing and profiling based on these provisions.

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 18 (1)(13): If personal data is collected directly from the subject of personal data, the controller that collects personal data, upon receipt of personal data or earlier, is obliged to inform such subject of information about [...] the rights of the personal data subject in accordance with this Law.
Article 18(3): If personal data is not collected from the personal data subject, the information provided for in Article 18(1), as well as information about the sources of personal data collection, must be communicated to the personal data subject by the controller [...]

GDPR	Draft Law

Fees

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

See Article 27(6) in section 5.1. above.

Response timeframe

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

See Article 27(3) in section 5.1. above.

Format of response

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

See Article 27(5) in section 5.1. above.

Exceptions

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

Article 22(4): If the processing of personal data is carried out for archiving purposes in the public interest, for scientific or historical research purposes, or for statistical purposes, the subject has the right to object to the processing, except in cases where it is necessary to perform tasks in the public interest.

Also see Article 27(6) in section 6.1. above.

5.4. Right of access

The right of access is recognised in both the GDPR and the Draft Law and provide data subjects with a right to obtain information about whether or not personal data concerning him/her are being processed. In addition, both legislations contain a detailed list of information that must be provided to the data subject upon request. Furthermore, both the GDPR and Draft Law refer to the identity of the data subject and require verification of the same.

GDPR	Draft 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.

Article 19(1): The subject of personal data has the right to receive information from the controller about the processing or lack of processing of his/her personal data.

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:

(a) the purposes of the processing;
(b) the categories of personal data concerned;
(c) 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;
(d) where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;
(e) 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;
(f) the right to lodge a complaint with a supervisory authority;
(g) where the personal data are not collected from the data subject, any available information as to their source; and

Article 19(1): The subject of personal data has the right to receive information from the controller about the processing or lack of processing of his personal data, and in the case of processing-the right to access personal data and the right to receive information about:

- processing goals;
- the composition of personal data that is being processed;
- recipients and/or categories of recipients;
- the period during which personal data will be stored or the criteria for determining it, if a specific period cannot be determined at the time of personal data collection;
- the right to rectification or to be forgotten, to restrict the processing of personal data, or to object to the processing of personal data;
- the right to file a complaint with the supervisory authority;
- the source of personal data collection if the data was not collected from the personal data subject;
- availability of an automated decision-making mechanism, including profiling and information about the algorithms (logic) used in such mechanisms, as well as the significance and intended consequences of such processing for the personal data subject; and
- appropriate guarantees for the protection of the rights of the personal data subject in the event of the transfer of personal data to another State or international organisation.

GDPR	Draft Law

Information to be accessed (cont'd)

(h) 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.

Inform data subject of right

See Article 12(1) in section 5.1.

See Articles 18(1)(13) and 18(3) in section 6.1.

Fees

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

See Article 27(6) in section 6.1.

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 reDraft Law to potential requests.

Article 27(1): In order to exercise the rights provided for in this Law, the subject of personal data applies to the controller with a statement that should contain personal data sufficient to identify the personal data subject [...].

Response timeframe

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

See Article 27(3) in section 6.1. above.

Format of response

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

See Article 27(5) in section 6.1. above.

Exceptions

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

Article 19(4): The right of access of a personal data subject may be restricted on grounds defined by this Law and other laws, if such restriction pursues a legitimate purpose and is proportionate.

Also see Article 27(6) in section 6.1. above.

GDPR	Draft Law
Response timeframe	
See Article 12(3) in section 5.1. above.	See Article 27(3) in section 6.1. above.
Format of response	
See Article 12(1) in section 5.1. above.	See Article 27(5) in section 6.1. above.
Exceptions	
See Article 12(5) in section 5.1. above.	Article 19(4): The right of access of a personal data subject may be restricted on grounds defined by this Law and other laws, if such restriction pursues a legitimate purpose and is proportionate. Also see Article 27(6) in section 6.1. above.

5.5. Right not to be subject to discrimination

Similar to the GDPR, the right not to be subject to discrimination in exercising rights is not explicitly mentioned in the Draft Law. However, under both legislations such a right can be inferred from the fundamental rights provided to data subjects. In addition, the GDPR and the Draft Law provide a right to object to automated processing and outlines exceptions to the same.

GDPR	Draft Law
Definition of right	
The GDPR only implies this right and does not provide an explicit definition for it.	The Draft Law only implies this right and does not provide an explicit definition for it.
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]	Article 25(1): It is prohibited to make a decision that has legal consequences for the personal data subject or otherwise has a significant impact on his/her solely on the basis of automated processing of his/her personal data [Article 25 goes on to detail this right, including exceptions].

5.6. Right to data portability

Fairly consistent

The GDPR and the Draft Law both recognise a right to data portability for data subjects. Nevertheless, the scope of this right under the two legislations differ. Specifically, the GDPR imposes a much narrower scope for exercising this right in comparison to the Draft Law. Furthermore, the Draft Law provides specific provisions regarding compensation for expenses when exercising this right while the GDPR does not.

GDPR	Draft 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 contrDraft Law pursuant to point (b) of Article 6(1); and

(b) the processing is carried out by automated means.

Article 23(1): A personal data subject has the right to request from the controller to provide a copy of any personal data of such a subject collected by the controller during automated processing in a structured and machine-readable format.

Inform data subject of right

See Article 12(1) in section 5.1.

See Articles 18(1)(13) and 18(3) in section 6.1.

Fees

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

Article 23(3): If the claim of the personal data subject provided for Article 23(1) imposes an excessive burden on the controller, the controller has the right to demand compensation for such expenses at the expense of the relevant personal data subject, provided that they are properly justified. The provision on compensation of expenses does not apply if:

- as a result of processing personal data, the controller has received a profit, the amount of which exceeds the cost of fulfilling the requirements of part one of this article;
- as a result of the processing of personal data, the legitimate interests of the personal data subject were harmed; and
- the processing of personal data was carried out in violation of the requirements of this Law.

GDPR	Draft Law

Response timeframe

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

See Article 27(3) in section 6.1. above.

Format

See Article 20(1) above.

See Article 27(5) in section 6.1. above.

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.

Article 23(2): The personal data subject has the right to receive personally and/or transfer the specified personal data from one controller to another without interference from the first controller on the basis of the corresponding request of the personal data subject, if there is an appropriate technical possibility.

Technically feasible

See Article 20(2) above.

See Article 23(2) above.

Exceptions

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

Article 23(4): The right of the subject of personal data provided for in this article may be restricted by law if the restriction pursues a legitimate aim and is necessary in a democratic society.

Also see Article 27(6) in section 6.1. above.

6. Enforcement

Fairly consistent

6.1. Monetary penalties

Both the GDPR and the Draft Law provide for monetary penalties and set out maximum fines that may be a percentage of an organisation's annual worldwide turnover. In addition, neither pieces of legislation provides for imprisonment as a sanction, nor do they impose liability on a DPO or responsible persons. Notably, however, unlike the GDPR, the Draft Law does not contain mitigating factors that must be taken into consideration when fines are assessed.

GDPR	Draft Law

Provides for monetary penalties

GDPR	Draft Law
The GDPR provides for monetary penalties.	The Draft Law provides for monetary penalties.

Issued by

GDPR	Draft Law
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.	Article 71(2): The decision to bring to responsibility violations in the field of personal data protection, as well as on applying other measures provided for by law, is made by the supervisory authority in accordance with the procedure established by law or by a court.

Fine maximum

GDPR	Draft Law
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).	Article 72(7)(3): The total amount of fines provided for in Articles 72(1) to (3) of the Law may not exceed the following limits [...] for fines provided for Article 72(3) of the Law, the maximum amount of the fine is: for individuals in the amount of up to UAH 20 million (approx. €609, 600), for legal entities in the amount of up to 150 million (approx. € 4.5 million) or up to 8% of the total annual turnover of such a legal entity for the last reporting year preceding the year in which the fine is imposed.

GDPR	Draft Law

Fine maximum (cont'd)

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

Percentage of turnover

GDPR	Draft Law
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.	Under Article 72(7)(3): fines may be issued that equate to 3%, 5%, and 8% of the total worldwide annual turnover for the last reporting year preceding the year in which the fine is imposed.

Mitigating factors

GDPR	Draft Law
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 charDraft Lawer of the infringement; (c) any Draft Lawion 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;	The Draft Law does not expressly refer to mitigating factors.

GDPR	Draft Law
Mitigating factors (cont'd)	
(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 (k) any other aggravating or mitigating fDraft 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

6.2. Supervisory authority

Fairly inconsistent

Both the GDPR and the Draft Law provide for a supervisory authority. However, the Draft Law unlike the GDPR, does not contain any provisions specific to the role or powers of the supervisory authority, nor does it address the issuance of an annual report by the same.

GDPR	Draft Law
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 2(1): 'supervisory authority' an authorised body that exercises supervision and control over compliance with the requirements of this Law and whose powers are provided for by this Law and a separate Law.
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.	The Draft Law does not explicitly address the investigatory powers of the supervisory authority. However, Article 36(1) states that the controller and operator, as well as their representative, in the case of appointment, to whom the supervisory authority has applied, are obliged to: • provide access to premises, facilities, information and telecommunication systems, materials and documents, including on the principles defined by legislative acts on the protection of restricted access information; • provide information and give explanations regarding the actual and legal basis of their actions and decisions related to the processing of personal data; and • comply with other legal requirements of the supervisory authority.

GDPR	Draft Law

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 Draft 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.

The Draft Law does not explicitly address the corrective powers of the supervisory authority.

GDPR	Draft Law

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 contrDraft 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.

The Draft Law does not explicitly address the authorisation/ advisory powers of the supervisory authority.

However, Article 39 stipulates that the controller is obliged to consult with the supervisory authority for the processing of personal data if the results of the impact assessment indicate that the processing of personal data involves a high degree of risk, which cannot be eliminated by the controller's measures taking into account the available technologies and the costs of their implementation. The controller is obliged to consult with the controller before processing personal data. by an administrative body in accordance with article 40 of this Law.

In addition, Article 47 provides that the supervisory authority is required to approve mandatory corporate rules in certain circumstances.

GDPR	Draft Law

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; (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);	The Draft Law does not explicitly outline the task of the supervisory authority.

GDPR	Draft Law

Tasks of authority (cont'd)

(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; (r) authorise contrDraft Lawual clauses and provisions referred to in Article 46(3); (s) approve binding corporate rules pursuant to Article 47; (t) contribute to the Draft Lawivities 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.	

GDPR	Draft Law
Annual report	
Article 59: Each supervisory authority shall draw up an annual report on its Draft Lawivities, 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.	The Draft Law does not explicitly require the supervisory authority to draw up an annual report.

6.3. Civil remedies for individuals

Fairly consistent

The GDPR and the Draft Law provide that data subjects may seek compensation including non-material and moral damage, respectively. Correspondingly, both pieces of legislation explicitly clarify data processor liabilities. Notably, the GDPR allows for the mandating of a representative, while the Draft Law is silent on this matter.

GDPR	Draft Law
Provides for claims/ cause of Draft 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 26(1): The subject of personal data has the right to file a complaint with the supervisory authority or the court about the violation of his rights under this Law or the violation of any provisions of this Law.
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 26(2): The subject of personal data has the right to compensation for material and/or moral damage caused as a result of violation of his rights provided for in this Law.
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 Draft 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 Draft Law does not explicitly address the right to mandate representation.
Specifies amount for damages	
Not applicable.	Not applicable.

GDPR	Draft Law
Processor liability	
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 Draft Lawed outside or contrary to lawful instructions of the controller.	Article 26(2): The operator is liable for damage caused by processing only if it does not comply with its obligations under this Law directed directly at the operator, or if the operator acts contrary to the legal instructions of the controller.
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.	Article 26(3): The controller is released from liability for damage caused to the subject of personal data, if it proves that the events that caused such damage did not occur through its fault and it took all reasonable measures to prevent the violation of rights and the occurrence of harm.