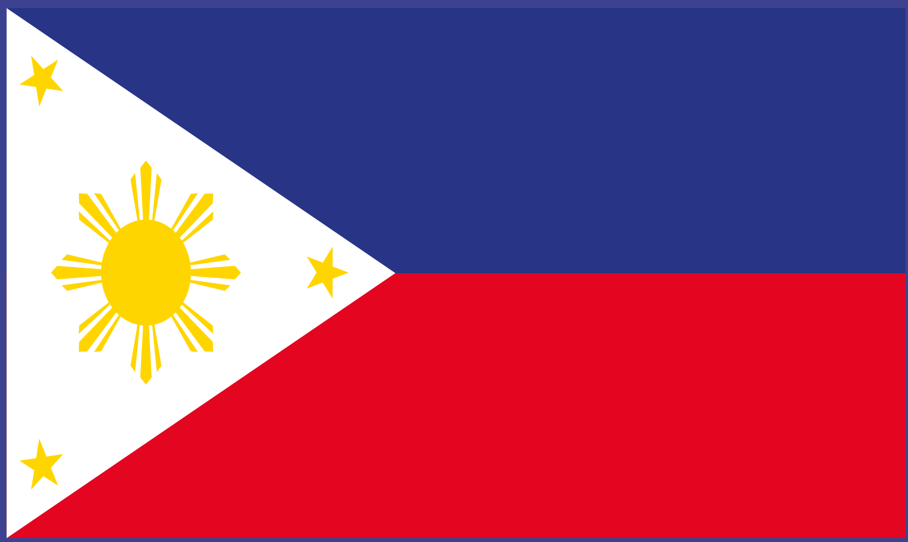


## Comparing privacy laws:

# GDPR v. Data Privacy Act and IRRs

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 I 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 I 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 11

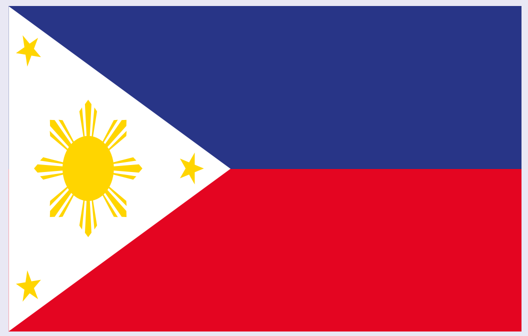
2. Key definitions
2.1. Personal data 15
2.2. Pseudonymisation 17
2.3. Controller and processors 18
2.4. Children 22
2.5. Research 23

3. Legal basis 25

4. Controller and processor obligations
4.1. Data transfers 28
4.2. Data processing records 31
4.3. Data protection impact assessment 36
4.4. Data protection officer appointment 38
4.5. Data security and data breaches 40
4.6. Accountability 43

5. Individuals' rights
5.1. Right to erasure 44
5.2. Right to be informed 48
5.3. Right to object 52
5.4. Right of access 55
5.5. Right not to be subject to discrimination 59
5.6. Right to data portability 61

6. Enforcement
6.1. Monetary penalties 63
6.2. Supervisory authority 66
6.3. Civil remedies for individuals 71



# 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. The Data Privacy Act of 2012 (Republic Act No. 10173) ('the Act') came into force on 8 September 2012 and is the first comprehensive law covering data privacy in the Philippines. The National Privacy Commission ('NPC'), which was established in early 2016 as the authority in charge of enforcing the Act, later issued the Implementing Rules and Regulations of Republic Act No. 10173 ('the IRRs'). The IRRs provide, in greater detail, the requirements that individuals and entities must comply with when processing personal data.

In general terms, both the GDPR and the Act set out similar approaches in terms of data subjects rights, principles of accountability, and obligations relating to data security, breach notifications, and the protection of privacy. Furthermore, the Act provides the NPC with similar responsibilities, as well as corrective and investigative powers, as the data protection authorities under the GDPR. However, the Act and the GDPR differ in some respects, including with regards to pseudonymisation, the protection of children's rights, data processing for research purposes, data transfers, as well as requirements for Data Protection Impact Assessments ('DPIAs').

This report organises provisions from the GDPR and the Act 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.

Introduction (cont'd)

## Structure and overview of the Guide

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

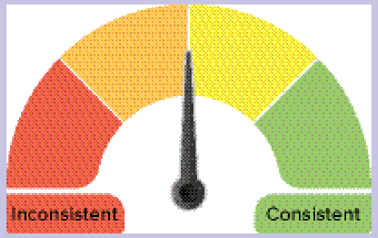
1. Scope
2. Key definitions
3. Legal basis
4. Controller and processor obligations
5. Individuals' rights
6. Enforcement

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 Act.

### Key for giving the consistency rate

**Consistent:** The GDPR and the Act bear a high degree of similarity in the rationale, core, scope, and the application of the provision considered.

**Fairly consistent:** The GDPR and the Act 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 Act 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 Act 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 acted upon without specific legal advice based on particular circumstances.



# 1. Scope

Fairly consistent

## 1.1. Personal scope

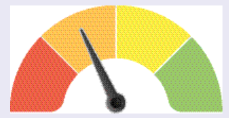
The Act and the GDPR provide similar definitions of data controllers and data processors. However, the definition of 'data subject' under the GDPR is more detailed than under the Act, and the two pieces of legislation differ on the nationality of the data subjects. Namely, while the GDPR applies to the processing of natural persons' data regardless of their nationality, the Act specifies that it applies to the processing of data in the Philippines or relating to a citizen or resident of the Philippines.

| GDPR | The Act / the IRRs |
| --- | --- |
| **Similarities** | |
| Article 4(7) of the GDPR: '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. | Sections 3(h) of the Act and 3(m) of the IRRs: 'personal information controller' refers to a person or organisation who controls the collection, holding, processing, or use of personal information, including a person or organisation who instructs another person or organisation to collect, hold, process, use, transfer, or disclose personal information on his or her behalf. The term excludes:<br><br>(1) A person or organisation who performs such functions as instructed by another person or organisation; and<br><br>(2) An individual who collects, holds, processes, or uses personal information in connection with the individual's personal, family, or household affairs. |
| Article 4(8) of the GDPR: 'processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller. | Sections 3(i) of the Act and 3(n) of the IRRs: 'personal information processor' refers to any natural or juridical person qualified to act as such under the Act to whom a personal information controller may outsource the processing of personal data pertaining to a data subject. |
| **Differences** | |
| Article 4(1) of the GDPR: '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 factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. | Sections 3(c) of the Act and 3(d) of the IRRs: 'data subject' refers to an individual whose personal information is processed. |

| GDPR | The Act / the IRRs |
|---|---|
| **Differences (cont'd)** | |
| Article 4(7) of the GDPR: 'controller' means the natural or legal person, public authority, agency or other body. | Section 4 of the IRRs: The Act and the IRRs apply to the processing of personal data by any natural and juridical person in the government or private sector. |
| Recital 14 of the GDPR: 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. | Sections 6 of the Act and 4 of the IRRs: The Act applies to an act done or practice engaged in and outside of the Philippines by an entity if:<br><br>(a) The act, practice, or processing relates to personal information about a Philippine citizen or a resident;<br><br>(b) The entity has a link with the Philippines, and the entity is processing personal information in the Philippines or even if the processing is outside the Philippines as long as it is about Philippine citizens or residents. |
| See Recital 14 of the GDPR, above. | See Section 6 of the Act above. |
| Recital 27 of the GDPR: 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. | Sections 17 of the Act and 35 of the IRRs: The lawful heirs and assigns of the data subject may invoke the rights of the data subject for which he or she is an heir or assignee at any time after the death of the data subject or when the data subject is incapacitated or incapable of exercising the rights as enumerated in the immediately preceding section. |



## 1.2. Territorial scope



Fairly inconsistent

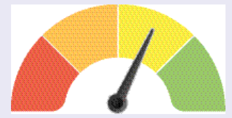
The GDPR and the Act generally differ in terms of the territorial scope of application. Although both legislations apply to the processing of personal data by controllers or processors established in their respective jurisdiction, the Act provides for a broader extraterritorial application by applying to any use of equipment in the Philippines or any act related to Philippine citizens or residents.

| GDPR | The Act / the IRRs |
|---|---|
| **Similarities** | |
| Under Article 3, the GDPR applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.<br><br>Recital 22 of the GDPR: establishment implies the effective and real exercise of activity through stable arrangements. | Sections 4 of the Act and 4 of the IRRs: The Act applies to the processing of all types of personal information and to any natural and juridical person involved in personal information processing including those personal information controllers and processors who, although not found or established in the Philippines, use equipment that is located in the Philippines, or those who maintain an office, branch, or agency in the Philippines, subject to Section 5 of the Act.<br><br>Section 4(a) of the IRRs: The Act and the IRRs apply to an act done or practice engaged in and outside of the Philippines if the natural or juridical person involved in the processing of personal data is found or established in the Philippines.<br><br>[Note: Section 5 of the Act establishes exemptions for journalists. See section 2.3. below.] |
| **Differences** | |
| In relation to extraterritorial scope, see Article 3 of the GDPR, above. | See Section 4 of the Act above.<br><br>Sections 6 of the Act and 4 of the IRRs: The Act applies to an act done or practice engaged in and outside of the Philippines by an entity if:<br><br>(a) The act, practice, or processing relates to personal information about a Philippine citizen or a resident;<br><br>(b) The entity has a link with the Philippines, and the entity is processing personal information in the Philippines or even if the processing is outside the Philippines as long as it is about Philippine citizens or residents such as, but not limited to, the following:<br><br>(1) A contract is entered in the Philippines; |

| GDPR | The Act / the IRRs |
|---|---|
| **Differences (cont'd)** | |
| | (2) A juridical entity unincorporated in the Philippines but has central management and control in the country; or<br><br>(3) An entity that has a branch, agency, office, or subsidiary in the Philippines, and the parent or affiliate of the Philippine entity has access to personal information;<br><br>(c) The entity has other links in the Philippines such as, but not limited to:<br><br>(1) The entity carries on business in the Philippines; or<br><br>(2) The personal information was collected or held by an entity in the Philippines. |
| Recital 23 of the GDPR: 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 activities are related to offering goods or services to such data subjects irrespective of whether connected to a payment. | Neither the Act nor the IRRs specifically refer to goods and services from abroad. However, the Act and the IRRs generally apply to any act, practice, or processing with links to the Philippines, including an entity that carries on business in the Philippines. See Sections 6 of the Act and 4 of the IRRs above. |
| Recital 24 of the GDPR states that 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. | Neither the Act nor the IRRs refer to general monitoring or profiling from abroad. |



## 1.3. Material scope



Fairly consistent

The GDPR and the Act provide similar definitions for personal data/personal information, data processing, as well as special categories of data/sensitive personal information. However, unlike the GDPR, there is no explicit mention of anonymised or pseudonymised data under the Act or the IRRs. Notably, the Act and the IRRs also provide for the protection of privileged information concerning data subjects.

| GDPR | The Act / the IRRs |
|---|---|
| **Similarities** | |
| Article 4(1) of the GDPR: '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 factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. | Sections 3(g) of the Act and 3(l) of the IRRs: 'personal information' refers to any information whether recorded in a material form or not, from which the identity of an individual is apparent or can be reasonably and directly ascertained by the entity holding the information, or when put together with other information would directly and certainly identify an individual. |
| Article 4(2) of the GDPR: '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. | Section 3(j) of the Act: 'processing' refers to any operation or any set of operations performed upon personal information including, but not limited to, the collection, recording, organisation, storage, updating or modification, retrieval, consultation, use, consolidation, blocking, erasure or destruction of data. |
| Article 9(1) of the GDPR: 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. | Section 3(o) of the IRRs: Processing may be performed through automated means, or manual processing, if the personal data are contained or are intended to be contained in a filing system.<br><br>Sections 3(l) of the Act and 3(t) of the IRRs: 'sensitive personal information' refers to personal information:<br><br>(1) About an individual's race, ethnic origin, marital status, age, colour, and religious, philosophical, or political affiliations;<br><br>(2) About an individual's health, education, genetic or sexual life of a person, or to any proceeding for any offence committed or alleged to have been committed by such person, the disposal of such proceedings, or the sentence of any court in such proceedings; |

| GDPR | The Act / the IRRs |
|---|---|
| **Similarities (cont'd)** | |
| | (3) Issued by government agencies peculiar to an individual which includes, but not limited to, social security numbers, previous or current health records, licences or its denials, suspension, or revocation, and tax returns; and<br><br>(4) Specifically established by an executive order or an act of Congress to be kept classified.<br><br>[Note: In addition to sensitive personal information, the Act and the IRRs also protects privileged information to the same extent as sensitive personal information (see section 4 below).<br><br>Accordingly, Sections 3(k) of the Act and 3(q) of the IRRs define 'privileged information' as any and all forms of data which under the Rules of Court and other pertinent laws constitute privileged communication.] |
| **Differences** | |
| According to Recital 26 of the GDPR, 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. | Neither the Act nor the IRRs generally refer to anonymised data. However, Section 19(e)(2) of the IRRs provides that personal data which is aggregated or kept in a form which does not permit the identification of data subjects may be kept longer than necessary for the declared, specified, and legitimate purpose. |
| Article 4(5) of the GDPR: '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. | Neither the Act nor the IRRs explicitly refer to pseudonymised data. |
| Article 2(1) of the GDPR: 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. | See Section 3(o) of the IRRs above.<br><br>Section 48 of the IRRs: The personal information controller carrying out any wholly or partly automated processing operations or set of such operations intended to serve a single purpose or several related purposes shall notify the NPC when the automated processing becomes the sole basis for making decisions about a data subject, and when the decision would significantly affect the data subject. |



| GDPR | The Act / the IRRs |
|---|---|
| **Differences (cont'd)** | |
| Article 2(2) of the GDPR: this Regulation does not apply to the processing of personal data:<br><br>(a) in the course of an activity which falls outside the scope of Union law;<br><br>(b) by the Member States when carrying out activities which fall within the scope of Chapter 2 of Title V of the Treaty on European Union; or<br><br>(c) by a natural person in the course of a purely personal or household activity. | Section 4 of the Act: The Act does not apply to the following:<br><br>(a) Information about any individual who is or was an officer or employee of a government institution that relates to the position or functions of the individual, including:<br><br>(1) The fact that the individual is or was an officer or employee of the government institution;<br><br>(2) The title, business address, and office telephone number of the individual;<br><br>(3) The classification, salary range, and responsibilities of the position held by the individual; and<br><br>(4) The name of the individual on a document prepared by the individual in the course of employment with the government;<br><br>(b) Information about an individual who is or was performing service under contract for a government institution that relates to the services performed, including the terms of the contract, and the name of the individual given in the course of the performance of those services;<br><br>(c) Information relating to any discretionary benefit of a financial nature such as the granting of a licence or permit given by the government to an individual, including the name of the individual and the exact nature of the benefit;<br><br>(d) Personal information processed for journalistic, artistic, literary, or research purposes;<br><br>(e) Information necessary in order to carry out the functions of public authority which includes the processing of personal data for the performance by the independent, central monetary authority and law enforcement and regulatory agencies of their constitutionally and statutorily mandated functions. Nothing in the Act shall be construed as to have amended or repealed Republic Act No. 1405, otherwise known as the Secrecy of Bank Deposits Act; Republic Act No. 6426, otherwise known as the Foreign Currency Deposit Act; and Republic Act No. 9510, otherwise known as the Credit Information System Act; |

| GDPR | The Act / the IRRs |
|---|---|
| **Differences (cont'd)** | |
| | (f) Information necessary for banks and other financial institutions under the jurisdiction of the independent, central monetary authority or the Central Bank of the Philippines to comply with the Credit Information System Act and Republic Act No. 9160, as amended, otherwise known as the Anti-Money Laundering Act and other applicable laws; and<br><br>(g) Personal information originally collected from residents of foreign jurisdictions in accordance with the laws of those foreign jurisdictions, including any applicable data privacy laws, which is being processed in the Philippines.<br><br>[Note: Section 5 of the IRRs provides further details on such exemptions.] |





# 2. Key definitions

Fairly consistent

## 2.1. Personal data

The GDPR and the Act provide similar definitions of personal information. In addition, the GDPR's definition of special categories of data is comparable to the definition of sensitive personal information under the Act. Both definitions include, among other things, information relating to race, ethnicity, genetic, sexual life, and political and philosophical affiliation. However, the Act does not provide information on online identifiers.

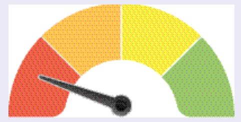
| GDPR | The Act / the IRRs |
|---|---|
| **Similarities** | |
| Article 4(1) of the GDPR: 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. | Sections 3(g) of the Act and 3(l) of the IRRs: 'personal information' refers to any information whether recorded in a material form or not, from which the identity of an individual is apparent or can be reasonably and directly ascertained by the entity holding the information, or when put together with other information would directly and certainly identify an individual. |
| Article 9(1) of the GDPR: 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. | Section 3(l) of the Act: 'sensitive personal information' refers to personal information:<br><br>(1) About an individual's race, ethnic origin, marital status, age, colour, and religious, philosophical, or political affiliations;<br><br>(2) About an individual's health, education, genetic or sexual life of a person, or to any proceeding for any offence committed or alleged to have been committed by such person, the disposal of such proceedings, or the sentence of any court in such proceedings;<br><br>(3) Issued by government agencies peculiar to an individual which includes, but not limited to, social security numbers, previous or current health records, licences or its denials, suspension, or revocation, and tax returns; and<br><br>(4) Specifically established by an executive order or an act of Congress to be kept classified. |

| GDPR | The Act / the IRRs |
|---|---|
| **Diferences** | |
| Recital 30 of the GDPR: 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. | Neither the Act nor the IRRs explicitly refer to online identifiers. |
| Article 4 of the GDPR: 'profiling' means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements. | Section 3(p) of the IRRs: 'profiling' refers to any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location, or movements. |





## 2.2. Pseudonymisation

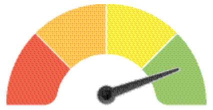


Inconsistent

Unlike the GDPR, neither the Act nor the IRRs explicitly refer to anonymised or pseudonymised data, beyond a brief reference to storing personal data that does not permit the identification of the data subject.

| GDPR | The Act / the IRRs |
|---|---|
| **Differences** | |
| Recital 26 of the GDPR defines 'anonymous information' as 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. | Neither the Act nor the IRRs have similar provisions.<br><br>However, Section 19(e)(2) of the IRRs provides that personal data which is aggregated or kept in a form which does not permit the identification of data subjects may be kept longer than necessary for the declared, specified, and legitimate purpose. |
| Article 4(5) of the GDPR: '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. | Neither the Act nor the IRRs have similar provisions. |

# 2.3. Controllers and processors



Consistent

The GDPR and the Act provide similar definitions for the concepts of data controllers and data processors. Furthermore, both legislations stipulate nearly identical requirements for controller and processor contracts, which address, among other things, confidentiality, security obligations, and assistance with ensuring compliance.

.

| GDPR | The Act / the IRRs |
|---|---|
| **Similarities** | |
| Article 4(7) of the GDPR: '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. | Sections 3(h) of the Act and 3(m) of the IRRS: 'personal information controller' refers to a person or organisation who controls the collection, holding, processing, or use of personal information, including a person or organisation who instructs another person or organisation to collect, hold, process, use, transfer, or disclose personal information on his or her behalf. The term excludes:<br><br>(1) A person or organisation who performs such functions as instructed by another person or organisation; and<br><br>(2) An individual who collects, holds, processes, or uses personal information in connection with the individual's personal, family, or household affairs.<br>Section 21 provides, 'A responsible party must, in terms of a **written contract** between the responsible party and the operator, ensure that the operator which processes personal information for the responsible party establishes and maintains the security measures referred to in Section 19.' |
| Article 4(8) of the GDPR: 'processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller. | Sections 3(i) of the Act and 3(n) of the IRRs: 'personal information processor' refers to any natural or juridical person qualified to act as such under the Act to whom a personal information controller may outsource the processing of personal data pertaining to a data subject. |
| According to Article 28(3) of the GDPR, processing by a processor shall be governed by a contract or other legal act 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 | Sections 14 of the Act and 43 of the IRRs: A personal information controller may subcontract the processing of personal information, provided that the personal information controller shall be responsible for ensuring that proper safeguards are in place to ensure the confidentiality of the personal information processed, prevent its use for unauthorised purposes, and generally comply with the requirements of the |



| GDPR | The Act / the IRRs |
|---|---|
| **Similarities (cont'd)** | |
| and rights of the controller. [Article 28 goes on to stipulate necessary information to be included in such a contract.] | Act and other laws for processing of personal information. The personal information processor shall comply with all the requirements of the Act and other applicable laws. |
| Recital 30 of the GDPR: 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.<br><br>Article 4 of the GDPR: 'profiling' means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements. | Section 44 of the IRRs: Processing by a personal information processor shall be governed by a contract or other legal act that binds the personal information processor to the personal information controller.<br><br>(a) The contract or legal act shall set 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, the obligations and rights of the personal information controller, and the geographic location of the processing under the subcontracting agreement.<br><br>(b) The contract or other legal act shall stipulate, in particular, that the personal information processor shall:<br><br>(1) Process the personal data only upon the documented instructions of the personal information controller, including transfers of personal data to another country or an international organisation, unless such transfer is authorised by law;<br><br>(2) Ensure that an obligation of confidentiality is imposed on persons authorised to process the personal data;<br><br>(3) Implement appropriate security measures and comply with the Act, the IRRs, and other issuances of the NPC;<br><br>(4) Not engage another processor without prior instruction from the personal information controller, provided that any such arrangement shall ensure that the same obligations for data protection under the contract or legal act are implemented, taking into account the nature of the processing;<br><br>(5) Assist the personal information controller, by appropriate technical and organisational measures and to the extent possible, fulfil the obligation to respond to requests by data subjects relative to the exercise of their rights;<br><br>(6) Assist the personal information controller in ensuring compliance with the Act, the IRRs, other relevant |

| GDPR | The Act / the IRRs |
|---|---|

## Similarities (cont'd)

| GDPR | The Act / the IRRs |
|---|---|
| | laws, and other issuances of the NPC, taking into account the nature of processing and the information available to the personal information processor;<br><br>(7) At the choice of the personal information controller, delete or return all personal data to the personal information controller after the end of the provision of services relating to the processing, provided that this includes deleting existing copies unless storage is authorised by the Act or another law;<br><br>(8) Make available to the personal information controller all information necessary to demonstrate compliance with the obligations laid down in the Act, and allow for and contribute to audits, including inspections, conducted by the personal information controller or another auditor mandated by the latter; and<br><br>(9) Immediately inform the personal information controller if, in its opinion, an instruction infringes the Act, the IRRs, or any other issuance of the NPC.<br><br>Section 26(f) of the IRRs: The personal information controller, through appropriate contractual agreements, shall ensure that its personal information processors, where applicable, shall also implement the security measures required by the Act and the IRRs. It shall only engage those personal information processors that provide sufficient guarantees to implement appropriate security measures specified in the Act and the IRRs and ensure the protection of the rights of the data subject. |

## Differences

| GDPR | The Act / the IRRs |
|---|---|
| DPIA is not specifically defined in the GDPR, however Article 35 sets out requirements for DPIAs (see section 5.3. for further information). | Neither the Act nor the IRRs explicitly refer to DPIAs. |
| DPO is not specifically defined in the GDPR, however Article 37 sets out requirements related to DPOs (see section 5.4. for further information). | DPO is not specifically defined, however Section 26(b) of the IRRs notes that any natural or juridical person or other body involved in the processing of personal data |

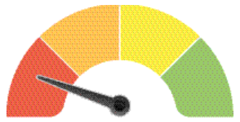


| GDPR | The Act / the IRRs |
|---|---|

## Differences (cont'd)

| GDPR | The Act / the IRRs |
|---|---|
| | shall designate an individual or individuals who shall function as DPO, compliance officer, or otherwise be accountable for ensuring compliance with applicable laws and regulations for the protection of data privacy and security (see section 5.4. below for further information). |

## 2.4. Children



Inconsistent

Unlike the GDPR, the Act and the IRRs do not provide a definition of children, nor do they implement special requirements for the processing of children's information.

| GDPR | The Act / the IRRs |
|---|---|
| **Differences** | |
| 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. | Neither the Act nor the IRRs have similar provisions. |
| Article 8(2) of the GDPR: 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. | Neither the Act nor the IRRs have similar provisions. |
| Recital 58 of the GDPR: 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. | Neither the Act nor the IRRs have similar provisions. |



## 2.5. Research

Fairly consistent

Like the GDPR, the Act establishes certain exemptions for processing for journalistic, artistic, literary, or research purposes, although the Act provides this through a more general exception. Both legislations also introduce the concept of purpose limitation when it comes to personal data collected for research purposes and set out requirements for security measures to safeguard the confidentiality of the information. There are, though, nuanced differences between the GDPR with the Act and the IRRs in relation to data subjects' rights and processing for research purposes.

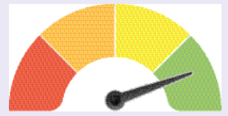
| GDPR | The Act / the IRRs |
|---|---|
| **Similarities** | |
| Recital 159 of the GDPR: where personal data are processed for scientific research purposes, this Regulation should also apply to that processing. For the purposes of this Regulation, the processing of personal data for scientific research purposes should be interpreted in a broad manner including for example technological development and demonstration, fundamental research, applied research and privately funded research. | Neither the Act nor the IRRs explicitly define the concept of research purposes. Both the Act and the IRRs, though, establish provisions regulating such purposes.<br><br>Section 4(d) of the Act: The Act does not apply to personal information processed for journalistic, artistic, literary, or research purposes. |
| Recital 160 of the GDPR: 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. | Section 5(c) of the IRRs: The Act and the IRRs shall not apply to personal information that will be processed for research purpose, intended for a public benefit, subject to the requirements of applicable laws, regulations, or ethical standards, only to the minimum extent of collection, access, use, disclosure, or other processing necessary to the purpose, function, or activity concerned. |
| Article 5(1)(b) of the GDPR: 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'). | Section 11(f) of the Act: Personal information must be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected and processed, provided that personal information collected for other purposes may lie processed for historical, statistical, or scientific purposes, and in cases laid down in law may be stored for longer periods, provided, further, that adequate safeguards are guaranteed by said laws authorising their processing. |
| Article 89(1) of the GDPR: Processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, shall be subject to appropriate safeguards, in accordance with this Regulation, for the rights and freedoms of the data subject. Those safeguards shall ensure that technical and organisational measures are in place in particular in order to ensure respect for the principle of data minimisation. Those measures may include pseudonymisation provided that those purposes can be fulfilled in that manner. | See Section 11(f) of the Act above. In addition, see Section 19(e) of the IRRs.<br><br>Section 19(e)(1) of the IRRs: Any authorised further processing shall have adequate safeguards. Personal data originally collected for a declared, specified, or legitimate purpose may be processed further for historical, statistical, or scientific purposes, and, in cases laid down in law, may be stored for longer periods, subject to implementation of the appropriate organisational, |

| GDPR | The Act / the IRRs |
|---|---|
| **Similarities (cont'd)** | |
| | physical, and technical security measures required by the Act in order to safeguard the rights and freedoms of the data subject. |
| Article 17(3) of the GDPR: 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. | Section 19 of the Act: The sections providing the rights of the data subject are not applicable if the processed personal information is used only for the needs of scientific and statistical research and, on the basis of such, no activities are carried out and no decisions are taken regarding the data subject, provided that the personal information shall be held under strict confidentiality and shall be used only for the declared purpose.<br><br>[Note: Section 37 of the IRRs provides a similar provision as Section 19 of the Act, while also emphasising that any limitations on the rights of the data subject shall only be to the minimum extent necessary to achieve the purpose of said research.<br><br>Furthermore, Section 34(2)(b) of the IRRs notes that the data subject shall be notified and furnished with certain information before the entry of his or her personal data into the processing system of the personal information controller, or at the next practical opportunity, including the purposes for which they are being or will be processed, including processing for direct marketing, profiling or historical, statistical, or scientific purpose.] |





# 3. Legal basis



Consistent

The GDPR and the Act and IRRs provide similar requirements for the lawful processing of personal data. Indeed, both legislations establish, among other things, the following legal bases: consent of the data subject, fulfilment of a contract, compliance with legal obligations, and legitimate interest. In addition, Article 9 of the GDPR and Section 13 of the Act show similarities in their prohibitions of the processing of sensitive personal data unless it is carried out under strict legal conditions. For both regulations, consent should be specific, freely given, informed, and can also be withdrawn by the data subject. Moreover, both pieces of legislation highlight that data protection requirements, in the case of processing for journalistic purposes, should be balanced against freedom of expression and information.

| GDPR | The Act / the IRRs |
|---|---|
| **Similarities** | |
| Article 6(1) of the GDPR: processing shall be lawful only if and to the extent that at least one of the following applies:<br><br>(a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;<br><br>(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;<br><br>(c) processing is necessary for compliance with a legal obligation to which the controller is subject;<br><br>(d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;<br><br>(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<br><br>(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. | Sections 12 of the Act and 21 of the IRRs: The processing of personal information shall be permitted only if not otherwise prohibited by law, and when at least one of the following conditions exists:<br><br>(a) The data subject has given his or her consent;<br><br>(b) The processing of personal information is necessary and is related to the fulfilment of a contract with the data subject or in order to take steps at the request of the data subject prior to entering into a contract;<br><br>(c) The processing is necessary for compliance with a legal obligation to which the personal information controller is subject;<br><br>(d) The processing is necessary to protect vitally important interests of the data subject, including life and health;<br><br>(e) The processing is necessary in order to respond to national emergency, to comply with the requirements of public order and safety, or to fulfil functions of public authority which necessarily includes the processing of personal data for the fulfilment of its mandate; or<br><br>(f) The processing is necessary for the purposes of the legitimate interests pursued by the personal information controller or by a third party or parties to whom the data is disclosed, except where such interests are overridden by fundamental rights and freedoms of the data subject which require protection under the Philippine Constitution. |

| GDPR | The Act / the IRRs |
|---|---|
| **Similarities (cont'd)** | |
| There are specific requirements for processing special categories of data, see Article 9 of the GDPR for further information. | Sections 13 of the Act and 22 of the IRRs: The processing of sensitive personal information and privileged information shall be prohibited, except in the following cases:<br><br>(a) The data subject has given his or her consent, specific to the purpose prior to the processing, or in the case of privileged information, all parties to the exchange have given their consent prior to processing;<br><br>(b) The processing of the same is provided for by existing laws and regulations, provided that such regulatory enactments guarantee the protection of the sensitive personal information and the privileged information, provided, further, that the consent of the data subjects are not required by law or regulation permitting the processing of the sensitive personal information or the privileged information;<br><br>(c) The processing is necessary to protect the life and health of the data subject or another person, and the data subject is not legally or physically able to express his or her consent prior to the processing;<br><br>(d) The processing is necessary to achieve the lawful and non-commercial objectives of public organisations and their associations, provided that such processing is only confined and related to the bona fide members of these organisations or their associations, provided, further, that the sensitive personal information is not transferred to third parties, provided, finally, that consent of the data subject was obtained prior to processing;<br><br>(e) The processing is necessary for purposes of medical treatment, is carried out by a medical practitioner or a medical treatment institution, and an adequate level of protection of personal information is ensured; or<br><br>(f) The processing concerns such personal information as is necessary for the protection of lawful rights and interests of natural or legal persons in court proceedings, or the establishment, exercise, or defence of legal claims, or when provided to government or public authority. |





| GDPR | The Act / the IRRs |
|---|---|
| **Similarities (cont'd)** | |
| Article 7(3) of the GDPR says that 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. | Section 19(a)(1) of the IRRs: Consent is required prior to the collection and processing of personal data, subject to exemptions provided by the Act and other applicable laws and regulations. When consent is required, it must be time-bound in relation to the declared, specified and legitimate purpose. Consent given may be withdrawn. |
| 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 action, signifies agreement to the processing of personal data relating to him or her. | Section 3(b) of the Act: Consent of the data subject refers to any freely given, specific, informed indication of will, whereby the data subject agrees to the collection and processing of personal information about and/or relating to him or her. Consent shall be evidenced by written, electronic or recorded means. It may also be given on behalf of the data subject by an agent specifically authorised by the data subject to do so. |
| Article 85(1) of the GDPR: 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. | Section 4(d) of the Act: The Act does not apply to personal information processed for journalistic, artistic, literary, or research purposes.<br><br>Section 5(b) of the IRRs: The Act and the IRRs shall not apply to personal information processed for journalistic, artistic, or literary purpose, in order to uphold freedom of speech, of expression, or of the press, subject to requirements of other applicable law or regulations, only to the minimum extent of collection, access, use, disclosure, or other processing necessary to the purpose, function, or activity concerned. |

# 4. Controller and processor obligations

## 4.1. Data transfers

Fairly inconsistent

The GDPR establishes adequate protection as a requirement for the lawful transfer of personal data and sets out a range of mechanisms to enable international transfers of data. In contrast, the Act and its IRRs do not stipulate equivalent provisions, but instead note that personal information controllers are responsible for the protection of personal data being transferred. In addition, the IRRs outline that protections for transfers of personal data should be implemented through the contracts binding controllers and processors and that appropriate security measures should be adopted to protect the information transferred.

Section 20 of the IRRs also provides requirements for data sharing, which is defined as 'the disclosure or transfer to a third party of personal data under the custody of a personal information controller or personal information processor.' These provisions do not explicitly refer to cross-border arrangements, although they do set out obligations such as requiring consent even when data is shared with an 'affiliate or mother company, or similar relationships.' In this regard, the NPC has issued NPC Circular 20-03 on Data Sharing Agreements.

| GDPR | The Act / the IRRs |
|---|---|
| **Similarities** | |
| Article 45(1) of the GDPR: 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. | Sections 21 of the Act and 50 of the IRRs: Each personal information controller is responsible for personal information under its control or custody, including information that has been transferred to a third party for processing, whether domestically or internationally, subject to cross-border arrangement and cooperation.<br><br>(a) The personal information controller is accountable for complying with the requirements of the Act and shall use contractual or other reasonable means to provide a comparable level of protection while the information is being processed by a third party.<br><br>(b) The personal information controller shall designate an individual or individuals who are accountable for the organisation's compliance with the Act. The identity of the individual(s) so designated shall be made known to any data subject upon request. |





| GDPR | The Act / the IRRs |
|---|---|
| **Similarities (cont'd)** | |
| | Section 20(a) of the IRRs: Data sharing shall be allowed when it is expressly authorised by law, provided, that there are adequate safeguards for data privacy and security, and processing adheres to the principles of transparency, legitimate purpose, and proportionality. |
| Article 46(1) of the GDPR: 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.<br><br>(2) The appropriate safeguards referred to in paragraph 1 may be provided for, without requiring any specific authorisation from a supervisory authority, by:<br><br>(a) a legally binding and enforceable instrument between public authorities or bodies;<br><br>(b) binding corporate rules in accordance with Article 47;<br><br>(c) standard data protection clauses adopted by the Commission in accordance with the examination procedure referred to in Article 93(2);<br><br>(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);<br><br>(e) an approved code of conduct pursuant to Article 40 together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights; or<br><br>(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.<br><br>(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: | See Sections 21 of the Act and 50 of the IRRs above.<br><br>Section 20(b) of the IRRs: Data sharing shall be allowed in the private sector if the data subject consents to data sharing, and the following conditions are complied with:<br><br>(1) Consent for data sharing shall be required even when the data is to be shared with an affiliate or mother company, or similar relationships;<br><br>(2) Data sharing for commercial purposes, including direct marketing, shall be covered by a data sharing agreement.<br><br>(a) The data sharing agreement shall establish adequate safeguards for data privacy and security and uphold rights of data subjects.<br><br>(b) The data sharing agreement shall be subject to review by the NPC, on its own initiative or upon complaint of data subject;<br><br>(3) The data subject shall be provided with the following information prior to collection or before data is shared:<br><br>(a) Identity of the personal information controllers or personal information processors that will be given access to the personal data;<br><br>(b) Purpose of data sharing;<br><br>(c) Categories of personal data concerned;<br><br>(d) Intended recipients or categories of recipients of the personal data;<br><br>(e) Existence of the rights of data subjects, including the right to access and correction, and the right to object;<br><br>. |

| GDPR | The Act / the IRRs |
|---|---|
| **Similarities (cont'd)** | |
| (a) contractual clauses between the controller or processor and the controller, processor or the recipient of the personal data in the third country or international organisation; or<br><br>(b) provisions to be inserted into administrative arrangements between public authorities or bodies which include enforceable and effective data subject rights. | (f) Other information that would sufficiently notify the data subject of the nature and extent of data sharing and the manner of processing. |





## 4.2. Data processing records

Fairly consistent

Although the Act does not establish specific requirements for data processing records, the IRRs provide for comparable requirements to those found under the GDPR. Notably, however, the IRRs also establishes requirements to register with the NPC when processing sensitive personal information and to notify the NPC in certain cases of automated processing.

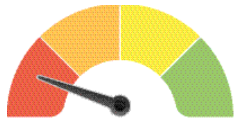
| GDPR | The Act / the IRRs |
|---|---|
| **Similarities** | |
| Article 30(1) of the GDPR: Each controller and, where applicable, the controller's representative, shall maintain a record of processing activities under its responsibility. That record shall contain all of the following information:<br><br>(a) the name and contact details of the controller and, where applicable, the joint controller, the controller's representative and the data protection officer;<br><br>(b) the purposes of the processing;<br><br>(c) a description of the categories of data subjects and of the categories of personal data;<br><br>(d) the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organisations;<br><br>(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;<br><br>(f) where possible, the envisaged time limits for erasure of the different categories of data; and<br><br>(g) where possible, a general description of the technical and organisational security measures referred to in Article 32(1). | Section 26(c) of the IRRs: Any natural or juridical person or other body involved in the processing of personal data shall maintain records that sufficiently describe its data processing system and identify the duties and responsibilities of those individuals who will have access to personal data. Records should include:<br><br>(1) Information about the purpose of the processing of personal data, including any intended future processing or data sharing;<br><br>(2) A description of all categories of data subjects, personal data, and recipients of such personal data that will be involved in the processing;<br><br>(3) General information about the data flow within the organisation, from the time of collection, processing, and retention, including the time limits for disposal or erasure of personal data;<br><br>(4) A general description of the organisational, physical, and technical security measures in place;<br><br>(5) The name and contact details of the personal information controller and, where applicable, the joint controller, its representative, and the compliance officer or DPO, or any other individual or individuals accountable for ensuring compliance with the applicable laws and regulations for the protection of data privacy and security.<br><br>[Note: Section 26(e) of the IRRs sets out requirements for policies and procedures.] |
| Article 30(2) of the GDPR: Each processor and, where applicable, the processor's representative shall maintain a record of all categories of processing activities carried out on behalf of a controller, containing: | See Section 26(c) of the IRRs above. |

| GDPR | The Act / the IRRs |
|---|---|
| **Similarities (cont'd)** | |
| (a) the name and contact details of the processor or processors and of each controller on behalf of which the processor is acting, and, where applicable, of the controller's or the processor's representative, and the data protection officer;<br><br>(b) the categories of processing carried out on behalf of each controller;<br><br>(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<br><br>(d) where possible, a general description of the technical and organisational security measures referred to in Article 32(1). | |
| Article 30(4) of the GDPR: 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. | See Section 26(c) of the IRRs above.<br><br>In addition, Section 47 of the IRRs provides information on the registration of personal data processing systems, as well as the content of the registration. |
| Article 30(5) of the GDPR: 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. | See Sections 4 of the Act and 5 of the IRRs for general exemption. |



| GDPR | The Act / the IRRs |
|---|---|
| **Differences** | |
| Article 30(3) of the GDPR: The records referred to in paragraphs 1 and 2 shall be in writing, including in electronic form. | Neither the Act nor the IRRs specify the format for records. For information on records of processing activities, please refer to Section 26(c) of the IRRs above. |
| Not applicable. | Section 46(b) of the IRRs: Pursuant to the mandate of the NPC to administer and implement the Act, and to ensure the compliance of personal information controllers with its obligations under the law, the NPC requires the following:<br><br>(a) Registration of personal data processing systems operating in the country that involves accessing or requiring sensitive personal information of at least 1,000 individuals, including the personal data processing system of contractors, and their personnel, entering into contracts with government agencies;<br><br>(b) Notification of automated processing operations where the processing becomes the sole basis of making decisions that would significantly affect the data subject.[Note: Sections 47 and 48 of the IRRs detail processing registration and notification requirements. In particular, Section 47 of the IRRs provides that the personal information controller or personal information processor that employs fewer than 250 persons shall not be required to register unless the processing it carries out is likely to pose a risk to the rights and freedoms of data subjects, the processing is not occasional, or the processing includes sensitive personal information of at least 1,000 individuals. |

# 4.3. Data protection impact assessment



Inconsistent

Unlike the GDPR, neither the Act nor its IRRs provide for the requirement to conduct DPIAs.

However, please note that the NPC has issued many guidelines and circulars on privacy impact assessments, including NPC Privacy Impact Assessments. See Philippines – Privacy Impact Assessment for further information.

| GDPR | The Act / the IRRs |
|---|---|
| **Differences** | |
| Article 35(1) of the GDPR: 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.<br><br>[...] (3) A data protection impact assessment referred to in paragraph 1 shall in particular be required in the case of:<br><br>(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;<br><br>(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<br><br>(c) a systematic monitoring of a publicly accessible area on a large scale. | Neither the Act nor the IRRs explicitly refer to DPIAs. |
| Article 35(7) of the GDPR: The assessment shall contain at least:<br><br>(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; | Neither the Act nor the IRRs explicitly refer to DPIAs. |



| GDPR | The Act / the IRRs |
|---|---|
| **Differences (cont'd)** | |
| (b) an assessment of the necessity and proportionality of the processing operations in relation to the purposes;<br><br>(c) an assessment of the risks to the rights and freedoms of data subjects referred to in paragraph 1; and<br><br>(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. | |
| 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]. | Neither the Act nor the IRRs explicitly refer to DPIAs. |

# 4.4. Data protection officer appointment

Fairly inconsistent

Both the GDPR and the IRRs provide for the appointment of a DPO/compliance officer in charge of ensuring compliance with applicable laws and regulations. However, the Act and the IRRs do not provide information on the specific case where a DPO is required, group appointments, or required qualifications to be appointed as a DPO. However, the NPC has clarified such requirements in NPC Advisory No. 2017-01 on Designation of Data Protection Officers. See Philippines – Data Protection Officer Appointment for further information.

| GDPR | The Act / the IRRs |
| --- | --- |
| **Similarities** | |
| Article 39(1) of the GDPR: The data protection officer shall have at least the following tasks:<br><br>(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;<br><br>(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;<br><br>(c) to provide advice where requested as regards the data protection impact assessment and monitor its performance pursuant to Article 35;<br><br>(d) to cooperate with the supervisory authority; and<br><br>(e) to act as the contact 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. | See Section 26(a) of the IRRs above. |
| Article 37(1) of the GDPR: The controller and the processor shall designate a data protection officer in any case where:<br><br>(a) the processing is carried out by a public authority or body, except for courts acting in their judicial capacity; | See Section 26(a) of the IRRs above. |



| GDPR | The Act / the IRRs |
| --- | --- |
| **Similarities (cont'd)** | |
| (b) the core activities 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<br><br>(c) the core activities 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. | |
| Article 37(7) of the GDPR: The controller or the processor shall publish the contact details of the data protection officer and communicate them to the supervisory authority. | Section 47(a)(10) of the IRRs: The contents of registration shall include the name and contact details of the compliance officer or DPO, which shall immediately be updated in case of changes.<br><br>[Note: According to Section 47 of the IRRs, the requirement to register with the NPC applies where the processing is likely to pose a risk to the rights and freedoms of data subjects, the processing is not occasional, or the processing includes sensitive personal information of at least 1,000 individuals. See section 5.2. above.] |
| **Differences** | |
| Article 37(2) of the GDPR: A group of undertakings may appoint a single data protection officer provided that a data protection officer is easily accessible from each establishment. | Neither the Act nor the IRRs explicitly refer to group appointments. |
| Article 37(5) of the GDPR: The data protection officer shall be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfil the tasks referred to in Article 39. | Neither the Act nor the IRRs specify qualification requirements. |

# 4.5. Data security and data breaches

Fairly consistent

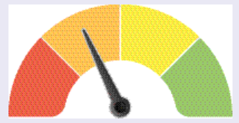
Both the Act and the GDPR define and establish security measures for the protection of personal information and data breach notification requirements. The specifics of these requirements, however, differ in certain aspects.

| GDPR | The Act / the IRRs |
| --- | --- |
| **Similarities** | |
| Article 32(1) of the GDPR: 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:<br><br>(a) the pseudonymisation and encryption of personal data;<br><br>(b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;<br><br>(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;<br><br>(d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.<br><br>The GDPR provides a list of technical and organisational measures, where appropriate, that data controllers and data processors must implement such as pseudonymisation, encryption and the ability to restore availability and access to personal data in a timely manner in the event of physical or technical incidents, to ensure integrity and confidentiality. | Section 20 of the Act: (a) The personal information controller must implement reasonable and appropriate organisational, physical, and technical measures intended for the protection of personal information against any accidental or unlawful destruction, alteration, and disclosure, as well as against any other unlawful processing.<br><br>(b) The personal information controller shall implement reasonable and appropriate measures to protect personal information against natural dangers such as accidental loss or destruction, and human dangers such as unlawful access, fraudulent misuse, unlawful destruction, alteration, and contamination.<br><br>(c) The determination of the appropriate level of security under this section must take into account the nature of the personal information to be protected, the risks represented by the processing, the size of the organisation and complexity of its operations, current data privacy best practices, and the cost of security implementation. Subject to guidelines as the NPC may issue from time to time, the measures implemented must include:<br><br>(1) Safeguards to protect its computer network against accidental, unlawful or unauthorised usage, or interference with or hindering of their functioning or availability;<br><br>(2) A security policy with respect to the processing of personal information;<br><br>(3) A process for identifying and accessing reasonably foreseeable vulnerabilities in its computer networks, and for taking preventive, corrective, and mitigating action against security incidents that can lead to a security breach; and |
| **Similarities (cont'd)** | |
| | (4) Regular monitoring for security breaches and a process for taking preventive, corrective, and mitigating action against security incidents that can lead to a security breach.<br><br>Section 28 of the IRRs: Where appropriate, personal information controllers and personal information processors shall adopt and establish the following technical security measures:<br><br>(e) The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;<br><br>(f) A process for regularly testing, assessing, and evaluating the effectiveness of security measures;<br><br>(g) Encryption of personal data during storage and while in transit, authentication process, and other technical security measures that control and limit access.<br><br>[Note: Sections 26 and 27 of the IRRs provides further detail on organisational and physical measures to be adopted.] |
| Article 33(1) of the GDPR: 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. | Section 20(f) of the Act: The personal information controller shall promptly notify the NPC and affected data subjects when sensitive personal information or other information that may, under the circumstances, be used to enable identity fraud are reasonably believed to have been acquired by an unauthorised person, and the personal information controller or the NPC believes that such unauthorised acquisition is likely to give rise to a real risk of serious harm to any affected data subject. The notification shall at least describe the nature of the breach, the sensitive personal information possibly involved, and the measures taken by the entity to address the breach. Notification may be delayed only to the extent necessary to determine the scope of the breach, to prevent further disclosures, or to restore reasonable integrity to the information and communications system. |

| GDPR | The Act / the IRRs |
|---|---|
| **Similarities (cont'd)** | |
| See Article 33(1) of the GDPR above. | Section 38(a) of the IRRs: The NPC and affected data subjects shall be notified by the personal information controller within 72 hours upon knowledge of, or when there is reasonable belief by the personal information controller or personal information processor that a personal data breach requiring notification has occurred.<br><br>Section 20(f)(3) of the Act: The NPC may authorise postponement of notification where it may hinder the progress of a criminal investigation related to a serious breach.<br><br>[Note: Section 40 of the IRRs also permits a delay in notification.] |
| Article 34(1) of the GDPR: 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. | See Sections 20(f) of the Act and 38(a) of the IRRs above. |
| Article 33(2) of the GDPR: The processor shall notify the controller without undue delay after becoming aware of a personal data breach. | Neither the Act of the IRRs specifically refer to data processors data breach notification requirements. See, however, Section 38(a) of the IRRs above as well as processor contract requirements in section 3.3. above. |
| Article 34(3) of the GDPR: The communication to the data subject referred to in paragraph 1 shall not be required if any of the following conditions are met:<br><br>(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;<br><br>(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;<br><br>(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. | Section 20(f)(2) of the Act: The NPC may exempt a personal information controller from notification where, in its reasonable judgment, such notification would not be in the public interest or in the interests of the affected data subjects. |



## 4.6. Accountability



Fairly inconsistent

While both the GDPR and the Act establish accountability as a fundamental principle, the Act applies this principle in relation to the transfer of personal data. While the GDPR explicitly specifies where data processors may be held liable, the IRRs more generally provides that any natural or juridical person may be considered liable.

| GDPR | The Act / the IRRs |
|---|---|
| **Differences** | |
| Article 5(2) of the GDPR: 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.] | Sections 21 of the Act and 50 of the IRRs: Each personal information controller is responsible for personal information under its control or custody, including information that has been transferred to a third party for processing, whether domestically or internationally, subject to cross-border arrangement and cooperation.<br><br>(a) The personal information controller is accountable for complying with the requirements of the Act and shall use contractual or other reasonable means to provide a comparable level of protection while the information is being processed by a third party.<br><br>(b) The personal information controller shall designate an individual or individuals who are accountable for the organisation's compliance with the Act. The identity of the individual(s) so designated shall be made known to any data subject upon request. |
| Article 82(2) of the GDPR: Any controller involved in processing shall be liable for the damage caused by processing which infringes this Regulation. A processor shall be liable for the damage caused by processing only where it has not complied with obligations of this Regulation specifically directed to processors or where it has acted outside or contrary to lawful instructions of the controller. | Section 51(a) of the IRRs: Any natural or juridical person, or other body involved in the processing of personal data, who fails to comply with the Act, the IRRs, and other issuances of the NPC, shall be liable for such violation, and shall be subject to its corresponding sanction, penalty, or fine, without prejudice to any civil or criminal liability, as may be applicable. |

# 5. Rights

Fairly consistent

## 5.1. Right to erasure

The Act establishes, in a similar fashion as the GDPR, the right to erasure for data subjects and provides legal grounds for the exercise of this right including situations where personal data has been unlawfully processed, is inaccurate, or is no longer necessary in relation to the purpose for which they have been collected. The Act, however, does not specifically address the format and timeframe associated with a data subject's request for erasure, or the penalties associated with non-compliance.

Please note that more detail on the procedures for exercising data subject rights are set out in NPC Advisory No. 2021-01 on Data Subject Rights ('Advisory No. 2021-01'). See Philippines – Data Subject Rights for further information.

| GDPR | The Act / the IRRs |
|---|---|
| **Similarities** | |
| Article 17(1) of the GDPR: 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:<br><br>(a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;<br><br>(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;<br><br>(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);<br><br>(d) the personal data have been unlawfully processed;<br><br>(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;<br><br>(f) the personal data have been collected in relation to the offer of information society services referred to in Article 8(1). | Section 16(e) of the Act: The data subject is entitled to suspend, withdraw, or order the blocking, removal, or destruction of his or her personal information from the personal information controller's filing system upon discovery and substantial proof that the personal information is incomplete, outdated, false, unlawfully obtained, used for unauthorised purposes, or is no longer necessary for the purposes for which they were collected. In this case, the personal information controller may notify third parties who have previously received such processed personal information.<br><br>Section 34(e)(1) of the IRRs: This right to erasure may be exercised upon discovery and substantial proof of any of the following:<br><br>(a) The personal data is incomplete, outdated, false, or unlawfully obtained;<br><br>(b) The personal data is being used for purposes not authorised by the data subject;<br><br>(c) The personal data is no longer necessary for the purposes for which they were collected;<br><br>(d) The data subject withdraws consent or objects to the processing, and there is no other legal ground or overriding legitimate interest for the processing; |



| GDPR | The Act / the IRRs |
|---|---|
| **Similarities (cont'd)** | |
| | (e) The personal data concerns private information that is prejudicial to data subject, unless justified by freedom of speech, of expression, or of the press or otherwise authorised;<br><br>(f) The processing is unlawful;<br><br>(g) The personal information controller or personal information processor violated the rights of the data subject. |
| Article 12(1) of the GDPR: 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. | Section 16(b)(8) of the Act: The data subject is entitled to be furnished information regarding the existence of their rights, i.e. to access, correction, as well as the right to lodge a complaint before the NPC, before the entry of his or her personal information into the processing system of the personal information controller, or at the next practical opportunity. |
| **Differences** | |
| Article 12(5) of the GDPR: Information provided under Articles 13 and 14 and any communication and any actions taken under Articles 15 to 22 and 34 shall be provided free of charge. Where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character, the controller may either:<br><br>(a) charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested; or<br><br>(b) refuse to act on the request. The controller shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request. | Neither the Act nor the IRRs explicitly address fees for erasure requests. However, see Advisory No. 2021-01 for further information. |
| Article 12(3) of the GDPR: The controller shall provide information on action taken on a request under Articles 15 to 22 to the data subject without undue delay and in any event within one month of receipt of the request. That period may be extended by two further months where necessary, taking | Neither the Act nor the IRRs explicitly impose a timeframe for responding to erasure requests. However, see Advisory No. 2021-01 for further information. |

| GDPR | The Act / the IRRs |
| --- | --- |
| **Differences (cont'd)** | |
| into account the complexity and number of the requests. The controller shall inform the data subject of any such extension within one month of receipt of the request, together with the reasons for the delay. Where the data subject makes the request by electronic form means, the information shall be provided by electronic means where possible, unless otherwise requested by the data subject. | |
| Article 12(1) of the GDPR: 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. | Neither the Act nor the IRRs explicitly impose a format of response to erasure requests. However, see Advisory No. 2021-01 for further information. |
| Article 17(2) of the GDPR: 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. | Neither the Act nor the IRRs explicitly address publicly available data. |
| Article 17(3) of the GDPR: Paragraphs 1 and 2 shall not apply to the extent that processing is necessary:<br><br>(a) for exercising the right of freedom of expression and information;<br><br>(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;<br><br>(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);<br><br>(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 | Section 19 of the Act: The sections providing the rights of the data subject are not applicable if the processed personal information is used only for the needs of scientific and statistical research and, on the basis of such, no activities are carried out and no decisions are taken regarding the data subject, provided that the personal information shall be held under strict confidentiality and shall be used only for the declared purpose. Likewise, such sections are not applicable to processing of personal information gathered for the purpose of investigations in relation to any criminal, administrative, or tax liabilities of a data subject.<br><br>[Note: Section 37 of the IRRs provides a similar provision as Section 19 of the Act, while also emphasising that any limitations on the rights of the data subject shall only be to the minimum extent necessary to achieve the purpose of said research.<br><br>Furthermore, Section 34(2)(b) of the IRRs notes that the data subject shall be notified and furnished with certain information before the entry of his or her personal data into the processing |



| GDPR | The Act / the IRRs |
| --- | --- |
| **Differences (cont'd)** | |
| (e) for the establishment, exercise or defence of legal claims.<br><br>Article 12(5): Information provided under Articles 13 and 14 and any communication and any actions taken under Articles 15 to 22 and 34 shall be provided free of charge. Where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character, the controller may either:<br><br>(a) charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested; or<br><br>(b) refuse to act on the request. The controller shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request. | system of the personal information controller, or at the next practical opportunity, including the purposes for which they are being or will be processed, including processing for direct marketing, profiling or historical, statistical, or scientific purpose.] |

# 5.2. Right to be informed

Fairly consistent

The right to be informed, under the Act, follows similar requirements as those found under the GDPR. The Act, however, does not explicitly distinguish when personal data originates from third parties.

Please note that more detail on the procedures for exercising data subject rights are set out in Advisory No. 2021-01. See Philippines – Data Subject Rights for further information.

| GDPR | The Act / the IRRs |
| --- | --- |
| **Similarities** | |
| Article 13(1) of the GDPR: 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:<br><br>(a) the identity and the contact details of the controller and, where applicable, of the controller's representative;<br><br>(b) the contact details of the data protection officer, where applicable;<br><br>(c) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;<br><br>(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;<br><br>(e) the recipients or categories of recipients of the personal data, if any;<br><br>(f) where applicable, the fact that the controller intends to transfer personal data to a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1), reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available.<br><br>(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: | Sections 16(1) of the Act and 34(a) of the IRRs: The data subject is entitled to:<br><br>(a) Be informed whether personal information pertaining to him or her shall be, are being, or have been processed; and<br><br>(b) Be furnished the information indicated hereunder before the entry of his or her personal information into the processing system of the personal information controller, or at the next practical opportunity:<br><br>(1) Description of the personal information to be entered into the system;<br><br>(2) Purposes for which they are being or are to be processed;<br><br>(3) Scope and method of the personal information processing;<br><br>(4) The recipients or classes of recipients to whom they are or may be disclosed;<br><br>(5) Methods utilised for automated access, if the same is allowed by the data subject, and the extent to which such access is authorised;<br><br>(6) The identity and contact details of the personal information controller or its representative;<br><br>(7) The period for which the information will be stored; and<br><br>(8) The existence of their rights, i.e. to access, correction, as well as the right to lodge a complaint before the NPC. |





| GDPR | The Act / the IRRs |
| --- | --- |
| **Similarities (cont'd)** | |
| (a) the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;<br><br>(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;<br><br>(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;<br><br>(d) the right to lodge a complaint with a supervisory authority;<br><br>(e) whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data; (f) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject. | Section 34(a)(1) of the IRRs: The data subject has a right to be informed whether personal data pertaining to him or her shall be, is being or has been processed, including the existence of automated decision-making and profiling. |
| See Article 13(1) and (2) of the GDPR above. | See Sections 16(1)(a) and 16(1)(b) of the Act above. |
| **Differences** | |
| In addition to the information required under Article 13, Article 14(2) of the GDPR 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. | Neither the Act nor the IRRs specifically address the right to be informed when data is obtained from a third party. |

| GDPR | The Act / the IRRs |
|---|---|
| **Differences (cont'd)** | |
| Article 12(1) of the GDPR: 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. | Section 18(a) of the IRRs: The data subject must be aware of the nature, purpose, and extent of the processing of his or her personal data, including the risks and safeguards involved, the identity of the personal information controller, his or her rights as a data subject, and how these can be exercised. Any information and communication relating to the processing of personal data should be easy to access and understand, using clear and plain language. |
| See Article 12(1) of the GDPR above. | See Section 18(a) of the IRRs above. |
| The requirements of Article 13 do not apply where the data subject already has the information.<br><br>The requirements of Article 14 do not apply where:<br><br>(a) the data subject already has the information;<br><br>(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;<br><br>(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<br><br>(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. | Section 16(b) of the Act: The notification under Section 16(b) of the Act shall not apply should the personal information be needed pursuant to a subpoena or when the collection and processing are for obvious purposes, including when it is necessary for the performance of or in relation to a contract or service or when necessary or desirable in the context of an employer-employee relationship, between the collector and the data subject, or when the information is being collected and processed as a result of legal obligation.<br><br>Section 19 of the Act: The sections providing the rights of the data subject are not applicable if the processed personal information is used only for the needs of scientific and statistical research and, on the basis of such, no activities are carried out and no decisions are taken regarding the data subject, provided that the personal information shall be held under strict confidentiality and shall be used only for the declared purpose. Likewise, such preceding sections are not applicable to processing of personal information gathered for the purpose of investigations in relation to any criminal, administrative, or tax liabilities of a data subject.<br><br>[Note: Section 37 of the IRRs provides a similar provision as Section 19 of the Act, while also emphasising that any limitations on the rights of the data subject shall only be to the minimum extent necessary to achieve the purpose of said research.<br><br>Furthermore, Section 34(2)(b) of the IRRs notes that the data subject shall be notified and furnished with certain information before the entry of his or her personal data into the processing system of the personal information controller, or at the next practical opportunity, including the purposes for which they are being or will be processed, including processing for direct marketing, profiling or historical, statistical, or scientific purpose.] |




GDPR | The Act / the IRRs
Differences (cont'd)

## 5.3. Right to object

Fairly consistent

The GDPR and the Act and the IRRs establish a right to object to processing in certain circumstances, such as where processing is for the purposes of direct marketing. Both legislative frameworks also provide for the ability to withdraw consent and restrict processing.

Please note that more detail on the procedures for exercising data subject rights are set out in Advisory No. 2021-01. See Philippines – Data Subject Rights for further information.

| GDPR | The Act / the IRRs |
| --- | --- |
| **Similarities** | |
| Article 21(1) of the GDPR: 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. | Section 16(1)(e) of the Act: The data subject is entitled to suspend, withdraw, or order the blocking, removal, or destruction of his or her personal information from the personal information controller's filing system upon discovery and substantial proof that the personal information is incomplete, outdated, false, unlawfully obtained, used for unauthorised purposes, or is no longer necessary for the purposes for which they were collected. In this case, the personal information controller may notify third parties who have previously received such processed personal information.<br><br>Section 34(b) of the IRRs: The data subject shall have the right to object to the processing of his or her personal data, including processing for direct marketing, automated processing, or profiling. The data subject shall also be notified and given an opportunity to withhold consent to the processing in case of changes or any amendment to the information supplied or declared to the data subject in the preceding paragraph. When a data subject objects or withholds consent, the personal information controller shall no longer process the personal data, unless:<br><br>(1) The personal data is needed pursuant to a subpoena;<br><br>(2) The collection and processing are for obvious purposes, including, when it is necessary for the performance of or in relation to a contract or service to which the data subject is a party, or when necessary or desirable in the context of an employer-employee relationship between the collector and the data subject; or<br><br>(3) The information is being collected and processed as a result of a legal obligation. |

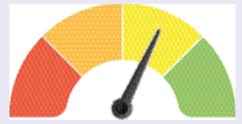




| GDPR | The Act / the IRRs |
| --- | --- |
| **Similarities (cont'd)** | |
| Article 7(3) of the GDPR: The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent. | See Section 34(b) of the IRRs above. |
| Article 18(1): The data subject shall have the right to obtain from the controller restriction of processing where one of the following applies:<br><br>(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;<br><br>(b) the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead;<br><br>(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;<br><br>(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. | See Section 16(1)(e) of the Act above. |
| Article 21(3) of the GDPR: Where the data subject objects to processing for direct marketing purposes, the personal data shall no longer be processed for such purposes. | See Section 16(1)(e) of the Act above. |
| See Article 12(1) of the GDPR 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. | Section 16(b)(8) of the Act: The data subject is entitled to be furnished information regarding the existence of their rights, i.e. to access, correction, as well as the right to lodge a complaint before the NPC, before the entry of his or her personal information into the processing system of the personal information controller, or at the next practical opportunity. |

| GDPR | The Act / the IRRs |
|---|---|
| **Differences** | |
| See Article 12(5) of the GDPR in section 5.1. above. | Neither the Act nor the IRRs explicitly address fees related to requests from data subjects. However, see Advisory No. 2021-01 for further information. |
| See Article 12(3) of the GDPR in section 5.1. above. | Neither the Act nor the IRRs explicitly address timeframe for responses. However, see Advisory No. 2021-01 for further information. |
| See Article 12(1) of the GDPR in section 5.1. above. | Neither the Act nor the IRRs explicitly impose a format of response to objection requests. However, see Advisory No. 2021-01 for further information. |
| See Article 12(5) of the GDPR in section 5.1. above. | Section 19 of the Act: The sections providing the rights of the data subject are not applicable if the processed personal information is used only for the needs of scientific and statistical research and, on the basis of such, no activities are carried out and no decisions are taken regarding the data subject, provided that the personal information shall be held under strict confidentiality and shall be used only for the declared purpose. Likewise, such sections are not applicable to processing of personal information gathered for the purpose of investigations in relation to any criminal, administrative, or tax liabilities of a data subject.<br><br>[Note: Section 37 of the IRRs provides a similar provision as Section 19 of the Act, while also emphasising that any limitations on the rights of the data subject shall only be to the minimum extent necessary to achieve the purpose of said research.<br><br>Furthermore, Section 34(2)(b) of the IRRs notes that the data subject shall be notified and furnished with certain information before the entry of his or her personal data into the processing system of the personal information controller, or at the next practical opportunity, including the purposes for which they are being or will be processed, including processing for direct marketing, profiling or historical, statistical, or scientific purpose.] |





Fairly consistent

## 5.4. Right of access

The Act and GDPR provide similar grounds for the right of access, including what information may be accessed by the data subject. However, the Act does not address fees, format, or timeframe for a response.

Please note that more detail on the procedures for exercising data subject rights are set out in Advisory No. 2021-01. See Philippines – Data Subject Rights for further information.

| GDPR | The Act / the IRRs |
|---|---|
| **Similarities** | |
| Article 15(1) of the GDPR: 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. | Sections 16(c) of the Act and 34(c) of the IRRs: The data subject is entitled to reasonable access to, upon demand, the following:<br><br>(1) Contents of his or her personal information that were processed;<br><br>(2) Sources from which personal information was obtained;<br><br>(3) Names and addresses of recipients of the personal information;<br><br>(4) Manner by which such data were processed;<br><br>(5) Reasons for the disclosure of the personal information to recipients;<br><br>(6) Information on automated processes where the data will or likely to be made as the sole basis for any decision significantly affecting or will affect the data subject;<br><br>(7) Date when his or her personal information concerning the data subject was last accessed and modified; and<br><br>(8) The designation, or name or identity and address of the personal information controller. |
| Article 15(1) of the GDPR: 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:<br><br>(a) the purposes of the processing; | See Section 16(c) of the Act above. |

| GDPR | The Act / the IRRs |
|---|---|
| **Similarities (cont'd)** | |
| (b) the categories of personal data concerned;<br><br>(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;<br><br>(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;<br><br>(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;<br><br>(f) the right to lodge a complaint with a supervisory authority;<br><br>(g) where the personal data are not collected from the data subject, any available information as to their source; and<br><br>(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. | |
| See Article 12(1) of the GDPR in section 5.1. above. | Section 16(b)(8) of the Act: The data subject is entitled to be furnished the information regarding the existence of their rights, i.e. to access, correction, as well as the right to lodge a complaint before the NPC, before the entry of his or her personal information into the processing system of the personal information controller, or at the next practical opportunity. |



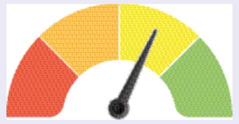
OneTrust DataGuidance™
REGULATORY RESEARCH SOFTWARE

| GDPR | The Act / the IRRs |
|---|---|
| **Differences** | |
| See Article 12(5) of the GDPR in section 5.1. above. | Neither the Act nor the IRRs address fees related to access requests. However, see Advisory No. 2021-01 for further information. |
| Recital 64 of the GDPR: The controller should use all reasonable measures to verify the identity of a data subject who requests access, in particular in the context of online services and online identifiers. A controller should not retain personal data for the sole purpose of being able to react to potential requests. | Neither the Act nor the IRRs address verification requirements for access requests. However, see Advisory No. 2021-01 for further information. |
| See Article 12(3) of the GDPR in section 5.1. above. | Neither the Act nor the IRRs establish a timeframe for response to access requests. However, see Advisory No. 2021-01 for further information. |
| See Article 12(1) of the GDPR in section 5.1. above. | Section 18(a) of the IRRs: The data subject must be aware of the nature, purpose, and extent of the processing of his or her personal data, including the risks and safeguards involved, the identity of the personal information controller, his or her rights as a data subject, and how these can be exercised. Any information and communication relating to the processing of personal data should be easy to access and understand, using clear and plain language. |
| See Article 12(5) of the GDPR in section 5.1. above. | Section 19 of the Act: The sections providing the rights of the data subject are not applicable if the processed personal information is used only for the needs of scientific and statistical research and, on the basis of such, no activities are carried out and no decisions are taken regarding the data subject, provided that the personal information shall be held under strict confidentiality and shall be used only for the declared purpose. Likewise, such sections are not applicable to processing of personal information gathered for the purpose of investigations in relation to any criminal, administrative, or tax liabilities of a data subject.<br><br>[Note: Section 37 of the IRRs provides a similar provision as Section 19 of the Act, while also emphasising that any limitations on the rights of the data subject shall only be to the minimum extent necessary to achieve the purpose of said research. |

| GDPR | The Act / the IRRs |
|---|---|
| **Differences (cont'd)** | |
| | Furthermore, Section 34(2)(b) of the IRRs notes that the data subject shall be notified and furnished with certain information before the entry of his or her personal data into the processing system of the personal information controller, or at the next practical opportunity, including the purposes for which they are being or will be processed, including processing for direct marketing, profiling or historical, statistical, or scientific purpose.] |



## 5.5. Right not to be subject to discrimination




Both the GDPR and the Act establish the right and grounds for the right to portability of personal information. The Act, however, does not specify additional requirements such as format, technical standards, modalities, and procedures for such data portability, although the NPC is provided with the power to issue further information on these requirements.

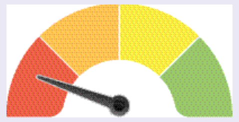
Please note that more detail on the procedures for exercising data subject rights are set out in Advisory No. 2021-01. See Philippines – Data Subject Rights for further information.

| GDPR | The Act / the IRRs |
|---|---|
| **Differences** | |
| The GDPR only implies this right and does not provide an explicit definition for it. | Neither the Act nor the IRRs address the right not to be subject to discrimination, although it does require that processing should be fair and lawful (Section 11(b) of the Act). |
| Article 22(1) of the GDPR: 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] | Section 48(b) of the IRRs: No decision with legal effects concerning a data subject shall be made solely on the basis of automated processing without the consent of the data subject.<br><br>Section 16(c)(6) of the Act: The data subject is entitled to reasonable access to, upon demand, information on automated processes where the data will or likely to be made as the sole basis for any decision significantly affecting or will affect the data subject.<br><br>Section 19(a)(2) of the IRRs: The data subject must be provided specific information regarding the purpose and extent of processing, including, where applicable, the automated processing of his or her personal data for profiling, or processing for direct marketing, and data sharing.<br><br>Section 34(a)(1) of the IRRs: The data subject has a right to be informed whether personal data pertaining to him or her shall be, are being, or have been processed, including the existence of automated decision-making and profiling.<br><br>Section 34(b) of the IRRs: The data subject shall have the right to object to the processing of his or her personal data, including processing for direct marketing, automated processing, or profiling. The data subject shall also be notified and given an opportunity to withhold consent to the processing in case of changes or any amendment to the information supplied or declared to the data subject in the preceding paragraph. |

| GDPR | The Act / the IRRs |
| --- | --- |
| **Differences (cont'd)** | |
| | [Note: Sections 47 and 48 of the IRRs detail notification requirements for automated processing. See section 5.2. above.] |







## 5.6. Right to data portability

Both the GDPR and the Act establish the right and grounds for the right to portability of personal information. The Act, however, does not specify additional requirements such as format, technical standards, modalities, and procedures for such data portability, although the NPC is provided with the power to issue further information on these requirements.

Please note that more detail on the procedures for exercising data subject rights are set out in Advisory No. 2021-01. See Philippines – Data Subject Rights for further information.

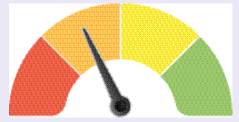
| GDPR | The Act / the IRRs |
| --- | --- |
| **Similarities** | |
| Article 20(1) of the GDPR: The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, where:<br><br>(a) the processing is based on consent pursuant to point (a) of Article 6(1) or point (a) of Article 9(2) or on a contract pursuant to point (b) of Article 6(1); and<br><br>(b) the processing is carried out by automated means. | Sections 18 of the Act and 36 of the IRRs: The data subject shall have the right, where personal information is processed by electronic means and in a structured and commonly used format, to obtain from the personal information controller a copy of data undergoing processing in an electronic or structured format, which is commonly used and allows for further use by the data subject. The NPC may specify the electronic format referred to above, as well as the technical standards, modalities, and procedures for their transfer. |
| See Article 12(1) of the GDPR in section 5.1. above. | Section 16(1)(8) of the Act: The data subject is entitled to be furnished information regarding the existence of their rights, i.e. to access, correction, as well as the right to lodge a complaint before the NPC, before the entry of his or her personal information into the processing system of the personal information controller, or at the next practical opportunity. |
| **Differences** | |
| See Article 12(5) of the GDPR in section 5.1. above. | Neither the Act nor the IRRs establish fees related to portability requests. However, see Advisory No. 2021-01 for further information. |
| See Article 12(3) of the GDPR in section 5.1. above. | Neither the Act nor the IRRs establish a timeframe for response to portability requests. However, see Advisory No. 2021-01 for further information. |
| See Article 20(1) of the GDPR above. | Neither the Act nor the IRRs establish a format for response to portability requests. However, see Advisory No. 2021-01 for further information. |

| GDPR | The Act / the IRRs |
|---|---|
| **Differences (cont'd)** | |
| Article 20(2) of the GDPR: 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. | Neither the Act nor the IRRs address data portability from controller to controller. |
| See Article 20(2) of the GDPR above. | Neither the Act nor the IRRs address technical feasibility. |
| See Article 12(5) of the GDPR in section 6.1. above. | Section 19 of the Act: The sections providing the rights of the data subject are not applicable if the processed personal information is used only for the needs of scientific and statistical research and, on the basis of such, no activities are carried out and no decisions are taken regarding the data subject, provided that the personal information shall be held under strict confidentiality and shall be used only for the declared purpose. Likewise, such sections are not applicable to processing of personal information gathered for the purpose of investigations in relation to any criminal, administrative, or tax liabilities of a data subject.<br><br>[Note: Section 37 of the IRRs provides a similar provision as Section 19 of the Act, while also emphasising that any limitations on the rights of the data subject shall only be to the minimum extent necessary to achieve the purpose of said research.<br><br>Furthermore, Section 34(2)(b) of the IRRs notes that the data subject shall be notified and furnished with certain information before the entry of his or her personal data into the processing system of the personal information controller, or at the next practical opportunity, including the purposes for which they are being or will be processed, including processing for direct marketing, profiling or historical, statistical, or scientific purpose.] |





# 6. Enforcement



Fairly inconsistent

## 6.1. Monetary penalties

Unlike the GDPR, the Act establishes individual offences and penalties for specific acts and violations of the Act and the IRRs. Additionally, the Act does not prescribe fines relating to the annual turnover of a company or explicitly state mitigating factors when considering fines. Instead, the Act establishes a definition of a 'large-scale' factor of breaches under the Act.

Please note that NPC is in the process of adopting draft Guidelines on Administrative Fines, which provides additional penalties as separate from the criminal penalties and fines already provided under the Act and the IRRs.

| GDPR | The Act / the IRRs |
|---|---|
| **Similarities** | |
| The GDPR provides for monetary penalties. | The Act provides for monetary penalties. |
| Article 58(2) of the GDPR: Each supervisory authority shall have all of the following corrective powers:<br><br>[...] (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. | Section 65 of the IRRs: Violations of the Act, the IRRs, other issuances and orders of the NPC, shall, upon notice and hearing, be subject to compliance and enforcement orders, cease and desist orders, temporary or permanent ban on the processing of personal data, or payment of fines, in accordance with a schedule to be published by the NPC. |
| **Differences** | |
| Article 83(5) of the GDPR: 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:<br><br>(a) the basic principles for processing, including conditions for consent, pursuant to Articles 5, 6, 7 and 9;<br><br>(b) the data subjects' rights pursuant to Articles 12 to 22;<br><br>(c) the transfers of personal data to a recipient in a third country or an international organisation pursuant to Articles 44 to 49;<br><br>(d) any obligations pursuant to Member State law adopted under Chapter IX; | Neither the Act nor the IRRs prescribe a maximum for fines that may be imposed.<br><br>Notwithstanding the above, according to Sections 33 of the Act and 60 of the IRRs, any combination or series of acts as defined in Sections 25 to 32 of the Act shall make the person subject to imprisonment ranging from three years to six years and a fine of not less than PHP 1 million (approx. €17,230) but not more than PHP 5 million (approx. €86,170). |

| GDPR | The Act / the IRRs |
|---|---|

## Differences (cont'd)

| | |
|---|---|
| (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).<br><br>(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. | |
| Under Article 83(4), (5), and (6) of the GDPR, fines may be issued that equate to 2% or 4% of the total worldwide annual turnover of the preceding financial year. | Neither the Act nor the IRRs impose fines in terms of percentage of turnover. |
| Article 83(2) of the GDPR: 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:<br><br>(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;<br><br>(b) the intentional or negligent character of the infringement;<br><br>(c) any action taken by the controller or processor to mitigate the damage suffered by data subjects;<br><br>(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;<br><br>(e) any relevant previous infringements by the controller or processor;<br><br>(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 Act does not expressly provide mitigating factors.<br><br>However, Sections 35 of the Act and 60 of the IRRs define a 'large-scale' factor to be considered in the imposition of penalties, whereby the maximum penalty in the scale of penalties respectively provided for the preceding offences shall be imposed when the personal information of at least 100 persons are harmed, affected, or involved as the result of the above-mentioned actions. |





| GDPR | The Act / the IRRs |
|---|---|

## Differences (cont'd)

| | |
|---|---|
| (g) the categories of personal data affected by the infringement;<br><br>(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;<br><br>(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;<br><br>(j) adherence to approved codes of conduct pursuant to Article 40 or approved certification mechanisms pursuant to Article 42; and<br><br>(k) any other aggravating or mitigating factor applicable to the circumstances of the case, such as financial benefits gained, or losses avoided, directly or indirectly, from the infringement. | |
| Not applicable. | Sections 25 to 33 of the Act and 52 to 60 of the IRRs establishes offences for specific acts or violations of the Act and the IRRs, including imprisonment. |
| Not applicable. | Sections 34 of the Act and 61 of the IRRs: If the offender is a corporation, partnership or any juridical person, the penalty shall be imposed upon the responsible officers, as the case may be, who participated in, or by their gross negligence, allowed the commission of the crime. If the offender is a juridical person, the court may suspend or revoke any of its rights under the Act. If the offender is an alien, he or she shall, in addition to the penalties herein prescribed, be deported without further proceedings after serving the penalties prescribed. If the offender is a public official or employee and lie or she is found guilty of acts penalised under Sections 27 and 28 of the Act, he or she shall, in addition to the penalties prescribed herein, suffer perpetual or temporary absolute disqualification from office, as the case may be. |

# 6.2. Supervisory authority


Fairly consistent

The Act establishes generally similar powers and tasks for the supervisory authority of the Philippines, the NPC, as the GDPR provides to EU Member State data protection authorities. There are, though, differences in the nuances in terms of powers and expected functions.

| GDPR | The Act / the IRRs |
|---|---|
| **Similarities** | |
| Article 51(1) of the GDPR: 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'). | Sections 7 of the Act and 8 of the IRRs: To administer and implement the provisions of the Act, and to monitor and ensure compliance of the country with international standards set for data protection, there is hereby created an independent body to be known as the NPC. |
| Article 58(1) of the GDPR: Each supervisory authority shall have all of the following investigative powers:<br><br>(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;<br><br>(b) to carry out investigations in the form of data protection audits;<br><br>(c) to carry out a review on certifications issued pursuant to Article 42(7);<br><br>(d) to notify the controller or the processor of an alleged infringement of this Regulation;<br><br>(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;<br><br>(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. | Section 7 of the Act: The NPC shall have the following functions:<br><br>(b) Receive complaints, institute investigations, facilitate or enable settlement of complaints through the use of alternative dispute resolution processes, adjudicate, award indemnity on matters affecting any personal information, prepare reports on disposition of complaints and resolution of any investigation it initiates, and, in cases it deems appropriate, publicise any such report, provided that in resolving any complaint or investigation (except where amicable settlement is reached by the parties), the NPC shall act as a collegial body. For this purpose, the NPC may be given access to personal information that is subject to any complaint and to collect the information necessary to perform its functions under the Act.<br><br>[Note: Section 9(e) of the IRRs further details the NPC's functions in relation to complaints and investigations.] |
| Article 58(2) of the GDPR: Each supervisory authority shall have all of the following corrective powers: | Section 7 of the Act: The NPC shall have the following functions: |





| GDPR | The Act / the IRRs |
|---|---|
| **Similarities (cont'd)** | |
| (a) to issue warnings to a controller or processor that intended processing operations are likely to infringe provisions of this Regulation;<br><br>(b) to issue reprimands to a controller or a processor where processing operations have infringed provisions of this Regulation;<br><br>(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;<br><br>(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;<br><br>(e) to order the controller to communicate a personal data breach to the data subject;<br><br>(f) to impose a temporary or definitive limitation including a ban on processing;<br><br>(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 actions to recipients to whom the personal data have been disclosed pursuant to Article 17(2) and Article 19;<br><br>(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;<br><br>(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;<br><br>(j) to order the suspension of data flows to a recipient in a third country or to an international organisation. | (c) Issue cease and desist orders, impose a temporary or permanent ban on the processing of personal information, upon finding that the processing will be detrimental to national security and public interest;<br><br>(d) Compel or petition any entity, government agency or instrumentality to abide by its orders or take action on a matter affecting data privacy.<br><br>(e) Monitor the compliance of other government agencies or instrumentalities on their security and technical measures and recommend the necessary action in order to meet minimum standards for protection of personal information pursuant to the Act.<br><br>[Note: Section 9(f) of the IRRs further details the NPC's functions in relation to enforcement.] |

| GDPR | The Act / the IRRs |
| --- | --- |
| **Similarities (cont'd)** | |
| Article 58(3) of the GDPR: Each supervisory authority shall have all of the following authorisation and advisory powers:<br><br>(a) to advise the controller in accordance with the prior consultation procedure referred to in Article 36;<br><br>(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;<br><br>(c) to authorise processing referred to in Article 36(5), if the law of the Member State requires such prior authorisation;<br><br>(d) to issue an opinion and approve draft codes of conduct pursuant to Article 40(5);<br><br>(e) to accredit certification bodies pursuant to Article 43;<br><br>(f) to issue certifications and approve criteria of certification in accordance with Article 42(5);<br><br>(g) to adopt standard data protection clauses referred to in Article 28(8) and in point (d) of Article 46(2);<br><br>(h) to authorise contractual clauses referred to in point (a) of Article 46(3);<br><br>(i) to authorise administrative arrangements referred to in point (b) of Article 46(3);<br><br>(j) to approve binding corporate rules pursuant to Article 47. | Section 7 of the Act: The NPC shall have the following functions:<br><br>(f) Coordinate with other government agencies and the private sector on efforts to formulate and implement plans and policies to strengthen the protection of personal information in the country;<br><br>(g) Publish on a regular basis a guide to all laws relating to data protection;<br><br>(i) Recommend to the Department of Justice the prosecution and imposition of penalties specified in Sections 25 to 29 of the Act;<br><br>(j) Review, approve, reject, or require modification of privacy codes voluntarily adhered to by personal information controllers, provided that the privacy codes shall adhere to the underlying data privacy principles embodied in this Act, provided, further, that such privacy codes may include private dispute resolution mechanisms for complaints against any participating personal information controller. For this purpose, the NPC shall consult with relevant regulatory agencies in the formulation and administration of privacy codes applying the standards set out in the Act, with respect to the persons, entities, business activities and business sectors that said regulatory bodies are authorised to principally regulate pursuant to the law, provided, finally, that the NPC may review such privacy codes and require changes thereto for purposes of complying with the Act.<br><br>(l) Comment on the implication on data privacy of proposed national or local statutes, regulations or procedures, issue advisory opinions, and interpret the provisions of this Act and other data privacy laws;<br><br>(m) Propose legislation, amendments, or modifications to Philippine laws on privacy or data protection as may be necessary.<br><br>[Note: Sections 9(b) and 9(c) of the IRRs further detail the NPC's functions in relation to advisory and public education.] |

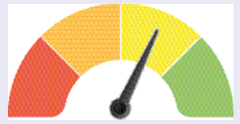


| GDPR | The Act / the IRRs |
| --- | --- |
| **Similarities (cont'd)** | |
| Article 59 of the GDPR: Each supervisory authority shall draw up an annual report on its activities, which may include a list of types of infringement notified and types of measures taken in accordance with Article 58(2). Those reports shall be transmitted to the national parliament, the government and other authorities as designated by Member State law. They shall be made available to the public, to the Commission and to the Board. | Sections 40 of the Act and 11 of the IRRs: The NPC shall annually report to the President and Congress on its activities in carrying out the provisions of the Act. The NPC shall undertake whatever efforts it may determine to be necessary or appropriate to inform and educate the public of data privacy, data protection, and fair information rights and responsibilities. |
| **Differences** | |
| Article 57(1) of the GDPR: Without prejudice to other tasks set out under this Regulation, each supervisory authority shall on its territory:<br><br>(a) monitor and enforce the application of this Regulation;<br><br>(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;<br><br>the development of information and communication technologies and commercial practices;<br><br>(j) adopt standard contractual clauses referred to in Article 28(8) and in point (d) of Article 46(2);<br><br>(k) establish and maintain a list in relation to the requirement for data protection impact assessment pursuant to Article 35(4);<br><br>(l) give advice on the processing operations referred to in Article 36(2);<br><br>(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);<br><br>(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); | In addition to above, Section 7 of the Act outlines the following further functions of the NPC:<br><br>(a) Ensure compliance of personal information controllers with the provisions of this Act;<br><br>(h) Publish a compilation of agency system of records and notices, including index and other finding aids;<br><br>(k) Provide assistance on matters relating to privacy or data protection at the request of a national or local agency, a private entity or any person;<br><br>(n) Ensure proper and effective coordination with data privacy regulators in other countries and private accountability agents, participate in international and regional initiatives for data privacy protection;<br><br>(o) Negotiate and contract with other data privacy authorities of other countries for cross-border application and implementation of respective privacy laws;<br><br>(p) Assist Philippine companies doing business abroad to respond to foreign privacy or data protection laws and regulations; and<br><br>(q) Generally perform such acts as may be necessary to facilitate cross-border enforcement of data privacy protection.<br><br>[Note: Sections 9(a), 9(d), and 10 of the IRRs further detail the NPC's functions in relation to rule-making, compliance and monitoring, and administrative issuances.] |

| GDPR | The Act / the IRRs |
|---|---|
| **Differences (cont'd)** | |
| (o) where applicable, carry out a periodic review of certifications issued in accordance with Article 42(7);<br><br>(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;<br><br>(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;<br><br>(r) authorise contractual clauses and provisions referred to in Article 46(3);<br><br>(s) approve binding corporate rules pursuant to Article 47;<br><br>(t) contribute to the activities of the Board;<br><br>(u) keep internal records of infringements of this Regulation and of measures taken in accordance with Article 58(2); and<br><br>(v) fulfil any other tasks related to the protection of personal data. | |



## 6.3. Other remedies



Fairly consistent

Both the Act and the IRRs allow data subjects to seek civil remedies for violations of the legislation, similar to the GDPR, and also allow for the lodging of complaints to the supervisory authority. The Act and IRRs do not, however, explicitly establish exemptions from the liability of civil remedies nor a mandate for representation to not-for-profit bodies, associations, or organisations.

| GDPR | The Act / the IRRs |
|---|---|
| **Similarities** | |
| Article 79 of the GDPR: 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. | Sections 16(f) of the Act and 34(f) of the IRRs: The data subject is entitled to be indemnified for any damages sustained due to such inaccurate, incomplete, outdated, false, unlawfully obtained, or unauthorised use of personal information.<br><br>Section 16(b)(8) of the Act: The data subject is entitled to be furnished information regarding the existence of their rights, i.e. to access, correction, as well as the right to lodge a complaint before the NPC, before the entry of his or her personal information into the processing system of the personal information controller, or at the next practical opportunity. |
| **Differences** | |
| Article 82(1) of the GDPR: 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. | Neither the Act nor the IRRs address material and non-material damage. See Section 34(f) of the IRRs above. |
| Article 80(1) of the GDPR: 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 active 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. | Neither the Act nor the IRRs provide for a mandate for representation. |
| Article 82(2) of the GDPR: Any controller involved in processing shall be liable for the damage caused by processing which infringes this Regulation. A processor shall be liable for the damage caused by processing only where it has not complied with obligations of this Regulation specifically directed to processors or where it has acted outside or contrary to lawful instructions of the controller. | Sections 21 and 50 of the IRRs: A personal information controller shall be responsible for any personal data under its control or custody, including information that has been outsourced or transferred to a personal information processor or a third party for processing, whether domestically or internationally, subject to cross-border arrangement and cooperation. |

| GDPR | The Act / the IRRs |
|---|---|
| **Differences (cont'd)** | |
| | (a) A personal information controller shall be accountable for complying with the requirements of the Act, the IRRs, and other issuances of the NPC. It shall use contractual or other reasonable means to provide a comparable level of protection to the personal data while it is being processed by a personal information processor or third party.<br><br>(b) A personal information controller shall designate an individual or individuals who are accountable for its compliance with the Act. The identity of the individual or individuals so designated shall be made known to a data subject upon request.<br><br>Section 45 of the IRRs: The personal information processor shall comply with the requirements of the Act, these Rules, other applicable laws, and other issuances of the NPC, in addition to obligations provided in a contract, or other legal act with a personal information controller. |
| 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. | Neither the Act nor the IRRs explicitly address exemption from liability of the abovementioned sections. |