Comparing privacy laws: GDPR v. Personal Data Protection Act

OneTrust DataGuidance™
REGULATORY RESEARCH SOFTWARE

About the authors

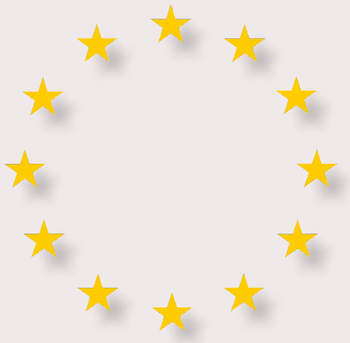
OneTrust DataGuidance™ provides a suite of privacy solutions designed to help organisations monitor regulatory developments, mitigate risk and achieve global compliance.

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

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

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

Table of contents



Introduction

The Personal Data Protection Act, Act No. 25.326 of 2000 ('the Act') sets forth the main principles and rules for the protection of personal data and has been followed by multiple decrees that detail requirements for the implementation of the Act. Three years after the passing of the Act, Argentina was recognised by the European Commission as providing an adequate level of protection for personal data.

The Argentinian data protection authority ('AAIP') regularly issues Resolutions which interpret the Act and guide compliance. These Resolutions have, among other things, defined 'security measures' and provided guidance on Binding Corporate Rules ('BCRs') for international data transfers. An important, recent Resolution, Resolution 4/2019 (only available in Spanish here) ('Resolution 4/2019'), specifies mandatory guidelines for the application of the Act, and addresses topics including video surveillance, automated data processing, consent, and biometric data. In addition, a significantly revised data protection bill (only available in Spanish here) ('the Bill') is currently being considered in the National Congress of Argentina ('the Congress'), which if passed would enable Argentina to have a more similar regime to that of the EU, as it would provide for requirements around the appointment of data protection officers as well as deadlines for the notification of data breaches.

The Act covers a similar set of topics as the General Data Protection Regulation (Regulation (EU) 2016/679) ('GDPR'), such as the rights of access, to inform, and to withdraw consent, among others. In addition, although Decree No. 1558/2001 Regulating Law No. 25.326 (only available in Spanish here) ('the Decree') supplements and addresses further topics alongside the Act, it does not clarify the processing of children's data, uses of pseudonymised data, or processing for research purposes and data protection officers.

This overview 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.

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.

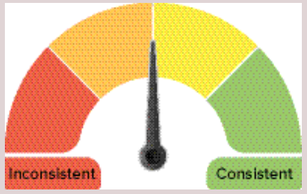
Key for giving the consistency rate

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

1.1. Personal scope

Fairly inconsistent

The Act employs similar core concepts as the GDPR, however, the terminology differs. In particular, the Act refers to 'person responsible for a database', which can be compared to the GDPR's 'data controller', and to 'data owner', which can be compared to the concept of 'data subject' under the GDPR. On the other hand, the Act does not include a definition for 'data processor'. Moreover, the Act does refer to the nationality and place of residence in regards to natural and legal persons having their data processed. Furthermore, the Act does not make reference to deceased individuals.

GDPR	The Act
Similarities	
Article 4(7): 'controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.	Section 2: Person responsible for a data file, register, bank or base: Physical person or legal entity, either public or private, owning a data file, register, bank or base.
Article 4(1): 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.	Section 2: 'data owner' is any physical person or legal entity having a legal domicile or local offices or branches in the country, whose data are subject to the processing referred to in the Act. Section 2: 'personal data' is information of any kind referring to certain or ascertainable physical persons or legal entities.
Article 4(7): 'controller' means the natural or legal person, public authority, agency or other body.	Section 2: 'data user' is any person, either public or private, performing in its, their discretion the processing of data contained in datafiles, registers, databases or databanks, owned by such persons or to which they may have access through a connection.
Differences	
Article 4(8): 'processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.	The Act does not expressly define the concept of data processors, however in Section 10(1) it states that 'those responsible for and all persons taking part in any stage of the processing of personal data have a professional secret duty in respect of the said data. Such duty shall subsist even after the relationship with the data file owner has expired'.

GDPR	The Act
Differences (cont'd)	
Recital 14: The protection afforded by this Regulation should apply to natural persons, whatever their nationality or place of residence, in relation to the processing of their personal data.	Section 2: 'Data owner' is any physical person or legal entity having a legal domicile or local offices or branches in the country, whose data are subject to the processing referred to in the Act.
Regarding the place of residence, see Recital 14, above.	See above.
Recital 27: This Regulation does not apply to the personal data of deceased persons. Member States may provide for rules regarding the processing of personal data of deceased persons.	The Act does not explicitly refer to deceased individuals' data.

1.2. Territorial scope

In general terms, and unlike the GDPR, the Act does not apply extraterritorially, nor does it explicitly regulate goods and services or monitoring from abroad. Moreover, the Act does not specify whether it applies to corporate bodies incorporated outside of Argentina.

GDPR	The Act
Similarities	
Article 3: This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not. Recital 22: Establishment implies the effective and real exercise of activity through stable arrangements.	Section 44: The provisions of the Act set forth in Chapters I, II, III, and IV, and Section 32 shall be of public order and be applicable, to the relevant extent, all over the national territory. Provinces are hereby encouraged to adhere to those provisions of the Act as may be of an exclusively national jurisdiction. The federal jurisdiction shall apply in respect of data registers, files, or banks interconnected via national or international interjurisdictional networks.
Differences	
See Article 3, above.	The Act does not refer to an extraterritorial scope.
Recital 23: In order to ensure that natural persons are not deprived of the protection to which they are entitled under this Regulation, the processing of personal data of data subjects who are in the Union by a controller, or a processor not established in the Union should be subject to this Regulation where the processing activities are related to offering goods or services to such data subjects irrespective of whether connected to a payment.	The Act does not refer to the offering of goods and services from abroad.
Recital 24: The processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union should also be subject to this Regulation when it is related to the monitoring of the behaviour of such data subjects in so far as their behaviour takes place within the Union.	The Act does not refer to monitoring from abroad.

1.3. Material scope

Fairly consistent

The Act and the GDPR provide definitions of personal data, special categories, or sensitive data, automated processing, as well as anonymised data. Whilst the Act does not use the term data processing, it refers to a similar operation as data treatment. The two pieces of legislation do, however, differ in terms of the exemptions and pseudonymised data.

GDPR	The Act
Similarities	
Article 4(1): 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.	Section 2: 'personal data' is information of any kind referred to certain or ascertainable physical persons or legal entities.
Article 4(2): 'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.	Section 2: 'data treatment' is any systematic operation or procedure, either electronic or otherwise, which enables the collection, integration, sorting, storage, change, relation, assessment, blocking, destruction, disclosure of data or transfer to third parties.
Article 9(1): Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.	Section 2: 'sensitive data' is personal data revealing racial and ethnic origin, political opinions, religious, philosophical or moral beliefs, labour union membership, and information concerning health conditions or sexual habits or behaviour.
Recital 26: The principles of data protection should not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable.	Section 2: 'data dissociation' is the treatment of personal data in such a way that the information obtained cannot be related to any certain or ascertainable person.

GDPR	The Act
Similarities (cont'd)	
Article 2(1): This Regulation applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.	Section 2: 'computerized data' is personal data subjected to electronic or automated treatment or processing.
Differences	
Article 4(5): 'pseudonymisation' means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.	The Act does not refer to pseudonymisation.
Article 2(2): This Regulation does not apply to the processing of personal data: (a) in the course of an activity which falls outside the scope of Union law; (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 (c) by a natural person in the course of a purely personal or household activity.	Section 1: In no case shall journalistic information sources or data bases be affected. Section 28: The regulations contained in the Act shall not apply to opinion polls, surveys or statistics collected pursuant to Law No. 17.622 (only available in Spanish here) ('Law No. 17.622'), market research works, scientific or medical research, and other similar activities, to the extent that the data collected cannot be attributed to a certain or ascertainable person.

2. Key definitions

2.1. Personal data

The GDPR and the Act set out similar understandings for the concepts of personal data and sensitive, or special categories of data. The two pieces of legislation differ in that the Act does not directly address online identifiers.

GDPR	The Act
Similarities	
Article 4(1): 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.	Section 2: 'personal data' is information of any kind referred to certain or ascertainable physical persons or legal entities.
Article 9(1): Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.	Section 2: 'sensitive data' is personal data revealing racial and ethnic origin, political opinions, religious, philosophical or moral beliefs, labour union membership, and information concerning health conditions or sexual habits or behaviour. According to Resolution 4/2019 of the AAIP, biometric data that identifies a person will also be considered sensitive data only when it can reveal additional data whose use may result in potential discrimination for its owner (e.g., biometric data that reveal ethnic origin or reference information to health).
Differences	
Recital 30: Natural persons may be associated with online identifiers provided by their devices, applications, tools and protocols, such as internet protocol addresses, cookie identifiers or other identifiers such as radio frequency identification tags. This may leave traces which, in particular when combined with unique identifiers and other information received by the servers, may be used to create profiles of the natural persons and identify them.	Although there is no direct reference to online identifiers, the definition of personal data under Section 2 of the Act provides for information of any kind referring to individuals or corporations, identified or identifiable.
Not applicable.	Data user: Any person, either public or private, performing in its, their discretion the treatment of data contained in datafiles, registers, databases or databanks, owned by such persons or to which they may have access through a connection.

2.2. Pseudonymisation

The Act only addresses anonymisation and not pseudonymisation, unlike the GDPR.

GDPR	The Act
Similarities	
Recital 26: 'anonymous information' is information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable.	Section 2: 'data dissociation' is the treatment of personal data in such a way that the information obtained cannot be related to any certain or ascertainable person.
Differences	
Article 4(5): 'pseudonymisation' means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.	The Act does not refer to pseudonymisation.

2.3. Controllers and processors

Fairly inconsistent

The Act and the GDPR provide a similar definition for data controllers, however data processors are not defined within the Act. The Act does include provisions on data treatment agreements, whilst the AAIP has issued a guide regarding Data Protection Impact Assessments ('DPIAs') ('the Guide'). Unlike the GDPR, however, the Act does not provide for data protection officer ('DPO') appointments.

GDPR	The Act
Similarities	
Article 4(7): 'controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.	Section 2: A 'person responsible for a data file' is a register, bank or base: physical person or legal entity, either public or private, owning a data file, register, bank or base.
Differences	
Article 4(8): 'processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.	Section 10(1): Those responsible for and all persons taking part in any stage of the treatment of personal data have a professional secret duty in respect of the said data. Such duty shall subsist even after the relationship with the data file owner has expired.
Article 28(3): 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 and rights of the controller. [Article 28 goes on to stipulate necessary information to be included in such a contract.]	Section 25(1): When personal data treatment services are provided for the account of third parties, such data cannot by applied or used with any purpose other than the one appearing on the corresponding contract for the provision of the service, nor can such data be communicated to other parties, even for storage purposes. Article 25 of the Decree: the contracts for the provision of services for the treatment of personal data must contain the security levels provided for in the Act, the Decree and the complementary rules issued by the National Directorate for the Protection of Personal Data, as well as the obligations that arise for the tenants in order to the confidentiality and reserve that they must maintain on the information obtained.

GDPR	The Act
Differences (cont'd)	
DPIA is not specifically defined, however Article 35 sets out requirements for DPIAs (see section 5.3. for further information).	Although the Act does not refer to DPIAs, page 5 of the Guide provides for a mandatory requirement to conduct a DPIA. Page 13 of the Guide sets out requirements for DPIAs (see section 4.3. for further information).
DPO is not specifically defined, however Article 37 sets out requirements related to DPOs (see section 5.4. for further information).	The Act does not provide for a requirement to appoint a DPO.

2.4. Children

Fairly inconsistent

Although the Act does not refer to children, Resolution 4/2019 does provide for the requirement to obtain consent when processing children's data.

GDPR	The Act
Similarities	
Article 8(2): The controller shall make reasonable efforts to verify in such cases that consent is given or authorised by the holder of parental responsibility over the child, taking into consideration available technology.	Resolution 4/2019 provides that in accordance with international regulation, the consent of children and adolescents must be granted for the processing of their data.
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.	The Act does not specifically define children.
Recital 58: Given that children merit specific protection, any information and communication, where processing is addressed to a child, should be in such a clear and plain language that the child can easily understand.	The Act does not refer to privacy notices in relation to children.

2.5. Research

Fairly Inconsistent

The Act refers to the processing for scientific or historical research purposes, although it does so in a more general way than the GDPR.

GDPR	The Act
Similarities	
Recital 159: Where personal data are processed for scientific research purposes, this Regulation should also apply to that processing. For the purposes of this Regulation, the processing of personal data for scientific research purposes should be interpreted in a broad manner including for example technological development and demonstration, fundamental research, applied research and privately funded research. Recital 160: Where personal data are processed for historical research purposes, this Regulation should also apply to that processing. This should also include historical research and research for genealogical purposes, bearing in mind that this Regulation should not apply to deceased persons.	SThe Act does not define scientific/historical research. Section 28(1): the regulations contained in the Act shall not apply to opinion polls, surveys or statistics collected pursuant to Law No. 17.622, market research works, scientific or medical research, and other similar activities, to the extent that the data collected cannot be attributed to a certain or ascertainable person.
Differences	
Article 5(1)(b): Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation').	The Act does not refer to the compatibility with the original purpose of collection.
Article 89(1): Processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, shall be subject to appropriate safeguards, in accordance with this Regulation, for the rights and freedoms of the 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.	The Act does not refer to the appropriate safeguards when processing for research purposes.

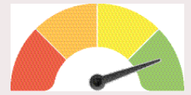
GDPR	The Act

Differences (cont'd)

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

Section 28(1): The regulations contained in the Act shall not apply to opinion polls, surveys or statistics collected pursuant to Law No. 17.622, market research works, scientific or medical research, and other similar activities, to the extent that the data collected cannot be attributed to a certain or ascertainable person.

3. Legal basis



Fairly consistent

Whilst the Act and the GDPR both set out legal bases for the processing for the processing of data, they differ slightly in terms of the available bases that may be relied upon.

GDPR	The Act

Similarities

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

(a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;

(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

(c) processing is necessary for compliance with a legal obligation to which the controller is subject;

(d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;

(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; or

(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

Section 5(1): The treatment of personal data is unlawful when the data owner has not given their express consent, which must be given in writing, or through any other similar means, depending on the circumstances. The consent above, given with other statements, must appear in a prominent and express manner, together with the warnings set forth in Section 6 of the Act.

Section 5(2): The consent above shall not be deemed necessary when:

(a) the data are secured from source of unrestricted public-access;

(b) are collected for the performance of the duties inherent in the powers of the State;

(c) consist of lists limited to name, national identity card number, taxing or social security identification, occupation, date of birth, domicile and telephone number;

(d) arise from a contractual relationship, either scientific or professional of data owner, and are necessary for its development or fulfilment. Refer to the transactions performed by financial entities, and arise from the information received from their customers in accordance with the provisions of Section 39 of Act No. 21.526.

GDPR	The Act

Similarities (cont'd)

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

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

Section 5(1): The processing of personal data is unlawful when the data owner has not given their express consent, which must be given in writing, or through any other similar means, depending on the circumstances. The consent above, given with other statements, must appear in a prominent and express manner, together with the warnings set forth in Section 6 of the Act.

Differences

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

Section 7(1): No person can be compelled to provide sensitive data.

Section 7(2): Sensitive data can be collected and subjected to treatment only in case there exist circumstances of general interest authorised by law, or with statistical or scientific purposes provided data owners cannot be identified.

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

Section 1: In no case shall journalistic information sources or data bases be affected by the provisions of the Act.

4. Controller and processor obligations

4.1. Data transfers

Both the GDPR and the Act provide requirements and restrictions for data transfers outside the EU/EEA and Argentina respectively. Both pieces of legislation place an obligation on parties to have certain mechanisms in place, such as BCRs and standard contractual clauses, among others.

GDPR	The Act

Similarities

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

Section 12(1): The transfer of any type of personal information to countries or international or supranational entities which do not provide adequate levels of protection, is prohibited.

The Decree highlights that the National Directorate of Personal Data Protection is empowered to evaluate, ex officio or at the request of an interested party, the level of protection provided by the norms of a State or international organisation. If it reaches the conclusion that a State or body does not adequately protect personal data, it will submit a draft decree to the National Executive Power to issue such a declaration.

The Decree further provides that the adequate nature of the level of protection offered by a country or international organisation will be evaluated taking into account all the circumstances that occur in a transfer or in a category of data transfers. In particular, the nature of the data, the purpose and duration of the treatment or of the planned treatments, the final destination, the general or sectoral rules of law in force in the country in question will be taken into consideration, as well as the professional standards, codes of conduct and security measures in force in said places, or that are applicable to international or supranational organisations.

The Decree further notes that it is understood that a State or international body provides an adequate level of protection when said protection derives directly from the current legal system, or from self-regulation systems, or from the protection established by the contractual clauses that provide for the protection of personal data.

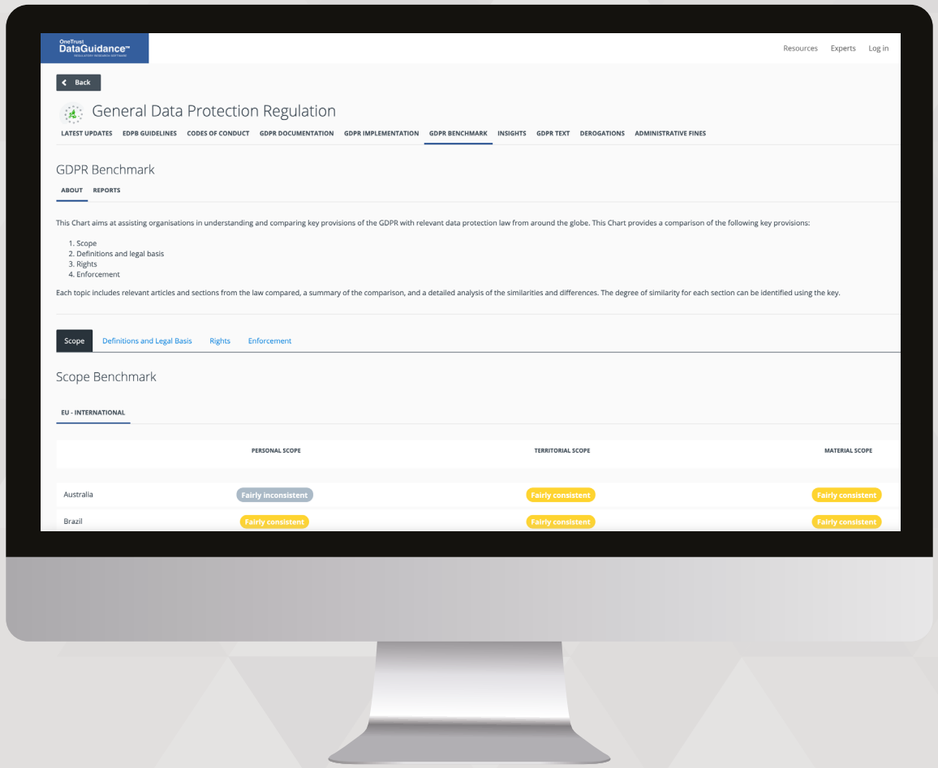
GDPR	The Act
Similarities (cont'd)	
Article 46(1): In the absence of a decision pursuant to Article 45(3), a controller or processor may transfer personal data to a third country or an international organisation only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available. (2) The appropriate safeguards referred to in paragraph 1 may be provided for, without requiring any specific authorisation from a supervisory authority, by: (a) a legally binding and enforceable instrument between public authorities or bodies; (b) binding corporate rules in accordance with Article 47; (c) standard data protection clauses adopted by the Commission in accordance with the examination procedure referred to in Article 93(2); (d) standard data protection clauses adopted by a supervisory authority and approved by the Commission pursuant to the examination procedure referred to in Article 93(2); (e) an approved code of conduct pursuant to Article 40 together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights; or (f) an approved certification mechanism pursuant to Article 42 together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights. (3) Subject to the authorisation from the competent supervisory authority, the appropriate safeguards referred to in paragraph 1 may also be provided for, in particular, by: (a) 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	Section 12(2): Restrictions on the international transfers of personal data do not apply to the following areas: international judicial collaboration; certain cases in regard to medical treatments; banking or stock exchange transactions conducted in accordance with applicable laws and regulations; transfer of data under international treaties; and data transfer between government intelligence agencies for the prevention of organised crime, terrorism, and drug trafficking. Section 12 of the Decree outlines that the Act prohibits the cross-border transfer of personal data from Argentina to other countries if these countries do not provide an adequate level of protection, unless: the data subject has consented to such international transfer; adequate level of protections arise from: (a) contractual clauses; or (b) mechanisms of self-regulations by establishing BCRs.

GDPR	The Act
Similarities (cont'd)	
(b) provisions to be inserted into administrative arrangements between public authorities or bodies which include enforceable and effective data subject rights.	

Global Regulatory Research Software

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

Monitor regulatory developments, mitigate risk, and achieve global compliance



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

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

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

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

- Scope
- Rights
- Definitions and legal basis
- Enforcement

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

OneTrust
DataGuidance™
REGULATORY RESEARCH SOFTWARE

Start your free trial at
www.dataguidance.com

4.2. Data processing records

Fairly inconsistent

The Act, unlike the GDPR does not provide for record keeping requirements. However, the Act does provide data processing notification requirements. In addition, the AAIP's Resolution No. 47/2018 (only available in Spanish here) ('the Recommended Security Measures') does provide recommendations on record keeping similar to that of the GDPR.

GDPR	The Act
Differences	
Article 30(1): 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: (a) the name and contact details of the controller and, where applicable, the joint controller, the controller's representative and the data protection officer; (b) the purposes of the processing; (c) a description of the categories of data subjects and of the categories of personal data; (d) the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organisations; (e) where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards; (f) where possible, the envisaged time limits for erasure of the different categories of data; and (g) where possible, a general description of the technical and organisational security measures referred to in Article 32(1).	The Act does not refer to data controller obligations in regards to record-keeping requirements. Though not mandatory, the Recommended Security Measures include certain data processing records such as: • an inventory of computer assets that store or manage personal data; • a record of access to the systems; • a record of system use; • a record of physical accesses (identifying day, time, entrants, and reason); • a record of the verifications and/or tests carried out to ensure the integrity, availability, and confidentiality of the data; • a record of recovery tests carried out identifying: type of information recovered, place and date where recovery tests were carried out, result of the recovery tests, person responsible for carrying out the recovery tests, personnel involved in the recovery tests, and notification to the data manager; and • an inventory identifying the backups, their actual location, and the physical medium.
Article 30(2): 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:	The Act does not refer to data processor obligations in regards to record-keeping requirements. Though not mandatory, the Recommended Security Measures include certain data processing records such as:

GDPR	The Act
Differences (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; (b) the categories of processing carried out on behalf of each controller; (c) where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards; and (d) where possible, a general description of the technical and organisational security measures referred to in Article 32(1).	• an inventory of computer assets that store or manage personal data; • a record of access to the systems; • a record of system use; • a record of physical accesses (identifying day, time, entrants, and reason); • a record of the verifications and/or tests carried out to ensure the integrity, availability, and confidentiality of the data; • a record of recovery tests carried out identifying: type of information recovered, place and date where recovery tests were carried out, result of the recovery tests, person responsible for carrying out the recovery tests, personnel involved in the recovery tests, and notification to the data manager; and • an inventory identifying the backups, their actual location, and the physical medium.
Article 30(3): The records referred to in paragraphs 1 and 2 shall be in writing, including in electronic form.	The Act does not refer to the format of records.
Article 30(4): The controller or the processor and, where applicable, the controller's or the processor's representative, shall make the record available to the supervisory authority on request.	The Act does not refer requirements to make records available in relation to record keeping.
Article 30(5): The obligations referred to in paragraphs 1 and 2 shall not apply to an enterprise or an organisation employing fewer than 250 persons unless the processing it carries out is likely to result in a risk to the rights and freedoms of data subjects, the processing is not occasional, or the processing includes special categories of data as referred to in Article 9(1) or personal data relating to criminal convictions and offences referred to in Article 10.	The Act does not refer to exemptions for record-keeping requirements.
Not applicable.	The Act provides for data processing notification requirements. For further information please refer to the following OneTrust DataGuidance Guidance Note Argentina - Data Processing Notification.

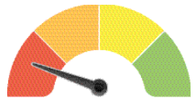
4.3. Data protection impact assessment

The Act does not provide for a requirement to conduct a DPIA unlike the GPDR. However, the Guide provides for such a requirement with similar requirements to that of the GDPR.

GDPR	The Act
Differences	
Article 35(1): Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks.	There is a mandatory requirement to undertake a DPIA under page 5 of the Guide. Pages 13 to 15 of the Guide provide examples of factors where if one or more of these concur, it can be inferred that the project or activity under analysis poses significant risks to people's rights and therefore require a DPIA.
[...] (3) A data protection impact assessment referred to in paragraph 1 shall in particular be required in the case of: (a) a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person; (b) processing on a large scale of special categories of data referred to in Article 9(1), or of personal data relating to criminal convictions and offences referred to in Article 10; or (c) a systematic monitoring of a publicly accessible area on a large scale.	
Article 35(7): The assessment shall contain at least: (a) a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller; (b) an assessment of the necessity and proportionality of the processing operations in relation to the purposes; (c) an assessment of the risks to the rights and freedoms of data subjects referred to in paragraph 1; and	The Act does not refer to the content of a DPIA.

GDPR	The Act
Differences (cont'd)	
(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].	The Act does not refer to requirements to consult with the authority regarding DPIAs.

4.4. Data protection officer appointment



Unlike the GDPR, there is no requirement to appoint a DPO under the Act.

GDPR	The Act
Differences	
Article 39(1): The data protection officer shall have at least the following tasks: (a) to inform and advise the controller or the processor and the employees who carry out processing of their obligations pursuant to this Regulation and to other Union or Member State data protection provisions; (b) to monitor compliance with this Regulation, with other Union or Member State data protection provisions and with the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits; (c) to provide advice where requested as regards the data protection impact assessment and monitor its performance pursuant to Article 35; (d) to cooperate with the supervisory authority; and (e) to 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.	There is no requirement to appoint a DPO under the Act or the Decree.
Article 37(1): The controller and the processor shall designate a data protection officer in any case where: (a) the processing is carried out by a public authority or body, except for courts acting in their judicial capacity; (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	The Act does not refer to when a DPO is required.

GDPR	The Act
Differences (cont'd)	
(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(2): A group of undertakings may appoint a single data protection officer provided that a data protection officer is easily accessible from each establishment.	The Act does not refer to group appointments.
Article 37(7): The controller or the processor shall publish the contact details of the data protection officer and communicate them to the supervisory authority.	The Act does not refer to notification of a DPO.
Article 37(5): The data protection officer shall be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfil the tasks referred to in Article 39.	The Act does not refer to the qualifications of a DPO.

4.5. Data security and data breaches

Fairly consistent

There is no general obligation under the Act to notify a data breach or incident that has involved personal data, unlike the GDPR. However, the Recommended Security Measures provides for similar breach notification requirements to the GDPR.

GDPR	The Act

Similarities

GDPR	The Act
Article 32(1): Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate: (a) the pseudonymisation and encryption of personal data; (b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; (c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; (d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.	Section 9: The person responsible for or the user of data files must take such technical and organisational measures as are necessary to guarantee the security and confidentiality of personal data, in order to avoid their alteration, loss, unauthorised consultation or treatment, and which allow for the detection of any intentional or unintentional distortion of such information, whether the risks arise from human conduct or the technical means used. It is prohibited to record personal data in files, registers or banks that do not meet the requirements of technical integrity and security. Annexes I and II of the Regulation provide further information regarding security measures needed when processing computerised and non-computerised personal data.
Article 33(1): In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.	There is no general obligation under the Act to notify a data breach or incident that has involved personal data. However, Annex II(E) of the Regulation states that data security incidents will have to be notified to the AAIP.

GDPR	The Act

Differences

GDPR	The Act
See Article 33(1) above.	Neither the Act, nor the Regulation provide for a timeframe for notification.
Article 34(1): When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay.	Neither the Act nor the Regulation provide for the notification to data subjects.
Article 33(2): The processor shall notify the controller without undue delay after becoming aware of a personal data breach.	The Act or the Regulation do not provide information on processors being required to notify controllers in the event of a breach.
Article 34(3): The communication to the data subject referred to in paragraph 1 shall not be required if any of the following conditions are met: (a) the controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption; (b) the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects referred to in paragraph 1 is no longer likely to materialise; (c) it would involve disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.	The Act nor the Regulation provide for exceptions in regard to data breach notification.

4.6. Accountability

Fairly consistent

Unlike the GDPR, the Act does not refer to the principle of accountability directly. However, both the Act and Disposition No. 60-E/2016 provide for the liability of data controllers and processors similar to that of the GDPR in terms of compliance with the relevant legal and regulatory obligations.

GDPR	The Act

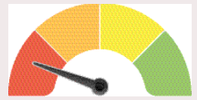
Similarities

GDPR	The Act
Article 82(2): Any controller involved in processing shall be liable for the damage caused by processing which infringes this Regulation. A processor shall be liable for the damage caused by processing only where it has not complied with obligations of this Regulation specifically directed to processors or where it has acted outside or contrary to lawful instructions of the controller.	Section 11 of the Act and Disposition No. 60-E/2016 provide that the controller and the processor will respond jointly and severally for the observance of the legal and regulatory obligations before the AAIP and the owner of the data. However, the processor may be totally or partially exempt from liability if it proves that the cause of damage cannot be attributed to them.

Differences

GDPR	The Act
Article 5(2): The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability'). [Paragraph 1 details principles of: lawfulness, fairness and transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity and confidentiality.]	The Act does not directly refer to the principle of accountability.

5. Rights



Inconsistent

5.1. Right to erasure

The Act does not explicitly refer to the right to erasure, unlike the GDPR.

GDPR	The Act

Differences

GDPR	The Act
Article 17(1): The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies: (a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed; (b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing; (c) the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2); (d) the personal data have been unlawfully processed; (e) the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject; (f) the personal data have been collected in relation to the offer of information society services referred to in Article 8(1).	The Act does not explicitly refer to the right to erasure.

GDPR	The Act
Differences (cont'd)	
Article 12(1): The controller shall take appropriate measures to provide any information referred to in Articles 13 and 14 and any communication under Articles 15 to 22 and 34 relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child. The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means.	The Act does not explicitly refer to the requirement of informing data subjects of the right to erasure.
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: (a) charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested; or (b) refuse to act on the request. The controller shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request.	The Act does not explicitly refer to fees for the right to erasure.
Article 12(3): The controller shall provide information on action taken on a request under Articles 15 to 22 to the data subject without undue delay and in any event within one month of receipt of the request. That period may be extended by two further months where necessary, taking into account the complexity and number of the requests. The controller shall inform the data subject of any such extension within one month of receipt of the request, together with the reasons for the delay. Where the data subject makes the request by electronic form means, the information shall be provided by electronic means where possible, unless otherwise requested by the data subject.	The Act does not explicitly refer to response timeframes for the right to erasure.

GDPR	The Act
Differences (cont'd)	
Article 12(1): The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means.	The Act does not explicitly refer to the format of the request to the right to erasure.
Article 17(2): Where the controller has made the personal data public and is obliged pursuant to paragraph 1 to erase the personal data, the controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data.	Section 16(4): In the event of a data communication or transfer the person responsible for or the user of the data bank must notify the recipient of such rectification or suppression within five business days of the data treatment being affected.
Article 17(3): Paragraphs 1 and 2 shall not apply to the extent that processing is necessary: (a) for exercising the right of freedom of expression and information; (b) for compliance with a legal obligation which requires processing by Union or Member State law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; (c) for reasons of public interest in the area of public health in accordance with points (h) and (i) of Article 9(2) as well as Article 9(3); (d) for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) in so far as the right referred to in paragraph 1 is likely to render impossible or seriously impair the achievement of the objectives of that processing; or (e) for the establishment, exercise or defence of legal claims.	The Act does not explicitly refer to the exceptions to the right to erasure.
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	

GDPR	The Act

Differences (cont'd)

or excessive, in particular because of their repetitive character, the controller may either:

(a) charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested; or

(b) refuse to act on the request. The controller shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request.

5.2. Right to be informed

Fairly consistent

The Act provides for a right to be informed, similar to that of the GDPR in terms of timeframe, intelligibility requirements, content and format. However, unlike the GDPR, the Act does not refer to information from third parties or exceptions.

GDPR	The Act

Similarities

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

(a) the identity and the contact details of the controller and, where applicable, of the controller's representative;

(b) the contact details of the data protection officer, where applicable;

(c) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;

(d) where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller or by a third party;

(e) the recipients or categories of recipients of the personal data, if any;

(f) where applicable, the fact that the controller intends to transfer personal data to a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1), reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available.

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

(a) the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;

Section 6: Whenever personal data is collected, data subjects shall be previously notified.

Section 13: Any person may request information from the AAIP regarding the existence of data files, registers, bases, or banks containing personal data, their purposes and the identity of the persons responsible therefor. The register kept for such purpose can be publicly consulted, free of charge.

GDPR	The Act

Similarities (cont'd)

(b) the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability;

(c) where the processing is based on point (a) of Article 6(1) or point (a) of Article 9(2), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;

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

(e) whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data; (f) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

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

Section 6(a) to (e): The following information needs to be provided:

- the purpose for which the data shall be treated, and who their addressees or type of addressees may be;
- the existence of the relevant data file, register or bank, whether electronic or otherwise, and the identity and domicile of the person responsible therefor;
- the compulsory or discretionary character of the answers to the questionnaire the person is presented with, particularly, in relation to the data connected with in Section 7 of the Act;
- the consequences of providing the data, of refusing to provide such data or of their inaccuracy;
- the possibility the party concerned has to exercise the right of data access, rectification, and suppression.

GDPR | The Act

Similarities (cont'd)

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

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

See Article 12(1) above.

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

The requirements of Article 14 do not apply where:

(a) the data subject already has the information;

(b) the provision of such information proves impossible or would involve a disproportionate effort, in particular for processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to the conditions and safeguards referred to in Article 89(1) or in so far as the obligation referred to in paragraph 1 of this Article is likely to render impossible or seriously impair the achievement of the objectives of that processing. In such cases the controller shall take appropriate measures to protect the data subject's rights and freedoms and legitimate interests, including making the information publicly available;

The Act does not explicitly refer to requirements for the right to be informed when personal data is not obtained directly from the data subject.

Section 6: Whenever personal data are requested, data owners shall be previously notified in an express and clear manner.

Section 6: Whenever personal data are requested, data owners shall be previously notified in an express and clear manner.

Section 17(2): The information about personal data may also be denied by the persons responsible for or users of public data banks when such information could hinder pending judicial or administrative proceedings relating to the compliance with tax or social security obligations, the performance of health and environment control functions, the investigation of crimes and the verification of administrative violations. The resolution so providing must be justified and notice thereof be given to the party concerned.

GDPR	The Act

Similarities (cont'd)

(c) obtaining or disclosure is expressly laid down by Union or Member State law to which the controller is subject and which provides appropriate measures to protect the data subject's legitimate interests; or

(d) where the personal data must remain confidential subject to an obligation of professional secrecy regulated by Union or Member State law, including a statutory obligation of secrecy.

Section 17(2): The information about personal data may also be denied by the persons responsible for or users of public data banks when such information could hinder pending judicial or administrative proceedings relating to the compliance with tax or social security obligations, the performance of health and environment control functions, the investigation of crimes and the verification of administrative violations. The resolution so providing must be justified and notice thereof be given to the party concerned.

5.3. Right to object

The Act does not explicitly refer to a general right to object, unlike the GDPR. However, the Act does provide for the right of data subjects to withdraw their consent as well as to restrict the processing of their data similar to that of the GDPR.

GDPR	The Act

Similarities

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

Article 5 of the Decree notes that data subjects can withdraw their consent which was previously given for the processing of personal data at any time.

Article 18(1): The data subject shall have the right to obtain from the controller restriction of processing where one of the following applies:

(a) the accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy of the personal data;

(b) the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead;

(c) the controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims;

(d) the data subject has objected to processing pursuant to Article 21(1) pending the verification whether the legitimate grounds of the controller override those of the data subject.

Section 16(1): Every person has the right to suppress and keep confidential their personal data included in a data bank.

Section 16(4): Where data is being transferred or shared the person responsible for or the user of the data bank must notify the third party of such suppression within five business days of the data processing being affected.

Section 16(5): Such restriction must not be affected in the event it could cause harm to the rights or legitimate interests of third parties, or there existed a legal obligation to preserve such data.

GDPR	The Act
Differences	
Article 21(3): Where the data subject objects to processing for direct marketing purposes, the personal data shall no longer be processed for such purposes.	The Act does not explicitly refer to the objection of direct marketing.
See Article 12(1) in section 6.1. 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.	The Act does not explicitly refer to the requirements to inform the data subject of the right to object.
See Article 12(5) in section 5.1. above.	The Act does not explicitly refer to the fees for right to object.
See Article 12(3) in section 5.1. above.	The Act does not explicitly refer to timeframes under the right to object.
See Article 12(1) in section 5.1. above.	The Act does not explicitly refer to the format requirements under right to object.
See Article 12(5) in section 5.1. above.	The Act does not explicitly refer to the exceptions for refusing a request under the right to object.

5.4. Right of access

Like the GDPR, the Act provides for the right of access for data subjects with a similar process in terms of content, identity verification informing the data subject of said right among others. However, the Act only allows specific types of information to be accessed unlike the GDPR which grants access to more categories of information.

GDPR	The Act
Similarities	
Article 15(1): The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed.	Section 4(6): The data must be stored in such a way that enables the data subject to exercise their right of access. Section 13: Data subjects may request information regarding the existence of data files, registers, bases or banks containing personal data, their purposes and the identity of the persons responsible therefore.
Article 15(1): The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information: (a) the purposes of the processing; (b) the categories of personal data concerned; (c) the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations; (d) where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period; (e) the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing; (f) the right to lodge a complaint with a supervisory authority; (g) where the personal data are not collected from the data subject, any available information as to their source; and	Section 14(1): A data subject can access their personal data included in public data registers or banks, or in private registers or banks intended for the provision of reports. Article 14 of the Decree outlines that the right of access will allow the data subject to: know whether or not the data subject is in the file, registry, database or database; know all the data relating to them that appears in the file; request information about the sources and means through which your data was obtained; request the purposes for which they were collected; know the intended destination for personal data; and know if the file is registered in accordance with the requirements of the Act.

GDPR	The Act
Similarities (cont'd)	
See Article 12(1) in section 5.1.	Section 6(e): A data subject must be informed of their right of access. Section 14(3): The right of access dealt with in this Section may only be exercised free of charge within intervals no shorter than six months, unless a legitimate interest to do otherwise is shown.
Recital 64: The controller should use all reasonable measures to verify the identity of a data subject who requests access, in particular in the context of online services and online identifiers. A controller should not retain personal data for the sole purpose of being able to react to potential requests.	Section 14(1): Data subjects, once they have duly evidenced their identity, have the right to request and obtain information.
See Article 12(3) in section 5.1. above.	Section 14(2): The data controller shall provide the requested information within ten calendar days from the date of the request of access.
See Article 12(1) in section 5.1. above.	Section 15(1): The information must be provided clearly, without any codes and, where applicable, enclosing an explanation of the terms used, in a language that is understood by a citizen with an average degree of education. Section 15(2): The information must be extensive and deal with the full record corresponding to the data subject, even in case the request submitted refers to only one item of personal data. In no case shall the report disclose information corresponding to third parties, even if such third parties are related to the requesting party. Section 15(3): The information may, at the data subject's request, be provided in writing, by email, telephonic, visual, or other adequate means for such purpose.
See Article 12(5) in section 6.1. above.	Section 17(1): The persons responsible for, or the users of public data banks, by means of a well-grounded decision may deny the access to such data, based on national defence, public order, and safety grounds or the protection of rights and interests of third parties.

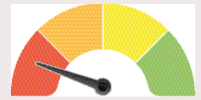
GDPR	The Act
Similarities (cont'd)	
	Section 17(2): The information about personal data may also be denied by the persons responsible for or users of public data banks when such information could hinder pending judicial or administrative proceedings relating to the compliance with tax or social security obligations, the performance of health and environment control functions, the investigation of crimes and the verification of administrative violations. The resolution so providing must be justified and notice thereof be given to the party concerned. Section 17(3): Notwithstanding the above provisions, access to the relevant records must be given at the time the affected party is to exercise their defence rights.

5.5. Right not to be subject to discrimination

The Act does not define the right not to be subject to discrimination. However, the Act does provide data subjects with the right to not be subject to judicial decisions or administrative acts that involve an appreciation or assessment that has its only basis the result of computerised treatment of personal data providing a definition of the profile or personality of the party concerned, a concept similar to the GDPR's right to not be subject to automated decision-making.

GDPR	The Act
Similarities	
Article 22(1): The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her. [Article 22 goes on to detail this right, including exceptions]	Section 20(1): Judicial decisions or administrative acts involving an assessment of human behaviour shall not have as their only basis the result of the automated processing of personal data providing a definition of the profile or personality of the party concerned.
Differences	
The GDPR only implies this right and does not provide an explicit definition for it.	The Act does not define the right not to be subject to discrimination.

5.6. Right to data portability



Unlike the GDPR, the Act does not address the right to data portability.

GDPR	The Act
Differences	
Article 20(1): The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, where: (a) the processing is based on consent pursuant to point (a) of Article 6(1) or point (a) of Article 9(2) or on a contract pursuant to point (b) of Article 6(1); and (b) the processing is carried out by automated means.	The Act does not explicitly refer to right to data portability.
See Article 12(1) in section 5.1.	The Act does not explicitly refer to the requirements to inform the data subject of the right to data portability.
See Article 12(5) in section 5.1. above.	The Act does not explicitly refer to fees for the right to data portability.
See Article 12(3) in section 5.1. above.	The Act does not explicitly refer to the timeframes for the right to data portability.
See Article 20(1) above.	The Act does not explicitly refer to format requirements for the right to data portability.
Article 20(2): In exercising his or her right to data portability pursuant to paragraph 1, the data subject shall have the right to have the personal data transmitted directly from one controller to another, where technically feasible.	The Act does not explicitly refer to the portability requirements for controller to controller transfers.
See Article 20(2) above.	The Act does not explicitly refer to the technical feasibility of transfers.
See Article 12(5) in section 6.1. above.	The Act does not explicitly refer to exceptions for the right to data portability.

6. Enforcement

Fairly consistent

6.1. Monetary penalties

The Act does provide for monetary penalties for violations of its provisions, however, said penalties are not of a similar nature to that of the GDPR as they are significantly lower in comparison. Both the Act and GDPR do provide for a set of mitigating factors when a penalty is being decided.

GDPR	The Act

Similarities

GDPR	The Act
The GDPR provides for monetary penalties.	The Act and Resolution No. 7/2005, as modified by Resolution No. 9/2015 and Provision 71 - E/2016 ('the Provision') provide for monetary penalties.
Article 58(2) Each supervisory authority shall have all of the following corrective powers:	Section 31: The AIPP may apply sanctions consisting of a warning, suspension, or a fine.
[...] (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 31(1): a fine ranging between ARS 1,000 (approx. €8) and ARS 100,000 (approx. €880).
Article 83(5): infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher:	Moreover, Article 1 of the Provision, outlines that for minor infractions the maximum fine is ARS 1 million (approx. €8,800), for serious infractions the maximum is ARS 3 million (approx. €26,400) and for very serious infractions the maximum fine is ARS 5 million (approx. €43,960).
(a) the basic principles for processing, including conditions for consent, pursuant to Articles 5, 6, 7 and 9;	
(b) the data subjects' rights pursuant to Articles 12 to 22;	
(c) the transfers of personal data to a recipient in a third country or an international organisation pursuant to Articles 44 to 49;	
(d) any obligations pursuant to Member State law adopted under Chapter IX;	
(e) non-compliance with an order or a temporary or definitive limitation on processing or the suspension of data flows by the supervisory authority pursuant to Article 58(2) or failure to provide access in violation of Article 58(1).	

GDPR	The Act

Similarities (cont'd)

GDPR	The Act
(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.	
Article 83(2): When deciding whether to impose an administrative fine and deciding on the amount of the administrative fine in each individual case due regard shall be given to the following:	Section 31(2): the applicable regulations shall determine the conditions and procedures for the application of the above mentioned sanctions, which shall be graded in proportion to the seriousness and extent of the violation and the damages arising from such violations, guaranteeing the due process of law.
(a) the nature, gravity and duration of the infringement taking into account the nature scope or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them;	
(b) the intentional or negligent character of the infringement;	
(c) any action taken by the controller or processor to mitigate the damage suffered by data subjects;	
(d) the degree of responsibility of the controller or processor taking into account technical and organisational measures implemented by them pursuant to Articles 25 and 32;	
(e) any relevant previous infringements by the controller or processor;	
(f) the degree of cooperation with the supervisory authority, in order to remedy the infringement and mitigate the possible adverse effects of the infringement;	
(g) the categories of personal data affected by the infringement;	
(h) the manner in which the infringement became known to the supervisory authority, in particular whether, and if so to what extent, the controller or processor notified the infringement;	
(i) where measures referred to in Article 58(2) have previously been ordered against the controller or processor concerned with regard to the same subject-matter, compliance with those measures;	

GDPR	The Act

Similarities (cont'd)

(j) adherence to approved codes of conduct pursuant to Article 40 or approved certification mechanisms pursuant to Article 42; and	
(k) any other aggravating or mitigating factor applicable to the circumstances of the case, such as financial benefits gained, or losses avoided, directly or indirectly, from the infringement.	

Differences

Under Article 83(4), (5), and (6), fines may be issued that equate to 2% or 4% of the total worldwide annual turnover of the preceding financial year.	Neither the Act nor Resolution No. 7/2005 provide for fines to be issued that equate to a percentage of turnover.
Not applicable.	Section 32(1): The following provision shall be included in the No. 11.179 for the Argentine Criminal Code (only available in Spanish here) ('the Criminal Code') as Section 117 bis: 1º. A penalty of imprisonment for the term of one month to two years shall correspond to anyone who knowingly inserts or has false information inserted in a personal data file. 2º. The penalty shall be of six months to three years to anyone who knowingly provides a third party with false information contained in a personal data file. 3º. The punishment scale shall be increased in one half of the minimum and the maximum penalties when a person is harmed as the result of the above mentioned action. 4º. When the offender or the person responsible for the offense is a public official in exercise of his duties, an accessory penalty consisting in the disqualification to occupy public offices for a term which shall double the one of the criminal penalty shall be applied. Section 32(2): The following provision shall be included in the Criminal Code as Section 157 bis: A penalty of six months to three years of imprisonment shall be applied to anyone who: 1º. Knowingly and unlawfully, or violating data confidentiality and security data systems, breaks in any way into a personal data bank;

GDPR	The Act

Differences (cont'd)

	2º. Discloses to third parties information registered in a personal data bank which should be kept secret by provision of law. When the offender is a public officer, an accessory penalty consisting in a special disqualification for a term from one to four years shall be applied.

6.2. Supervisory authority

Fairly consistent

The Act provides for the role of the AAIP but the primary legislation in regards to the functions of the AAIP is the Right of Access to Public Information Law No. 27,275 ('the Right of Access Law'), as amended by Article 11 of Decree No. 746/2017. The Right of Access Law provides that the AAIP is the supervisory authority with similar powers of investigation and enforcement to that of supervisory authorities of the GDPR.

GDPR	The Act
Similarities	
Article 51(1): Each Member State shall provide for one or more independent public authorities to be responsible for monitoring the application of this Regulation, in order to protect the fundamental rights and freedoms of natural persons in relation to processing and to facilitate the free flow of personal data within the Union ('supervisory authority').	Article 19 of the Right of Access Law, as amended by Article 11 of Decree No. 746/2017, provides that the AAIP is the main supervisory authority of both the Act and relevant regulations.
Article 58(1): Each supervisory authority shall have all of the following investigative powers: (a) to order the controller and the processor, and, where applicable, the controller's or the processor's representative to provide any information it requires for the performance of its tasks; (b) to carry out investigations in the form of data protection audits; (c) to carry out a review on certifications issued pursuant to Article 42(7); (d) to notify the controller or the processor of an alleged infringement of this Regulation; (e) to obtain, from the controller and the processor, access to all personal data and to all information necessary for the performance of its tasks; (f) to obtain access to any premises of the controller and the processor, including to any data processing equipment and means, in accordance with Union or Member State procedural law.	Section 29(1): The controlling Agency shall take all actions necessary to the compliance with the objectives and other provisions of the Act. To such purposes, it will have the following functions and powers: (a) give any requesting party assistance and advise on the scope of the Act and the legal means available for the defence of the rights guaranteed by the same; (b) pronounce the rules and regulations to be observed in the development of the activities covered by the Act; (c) do a census of data files, registers or banks covered by the Act and keep a permanent record thereof; (d) control compliance with the norms on data integrity and security by datafiles, registers, databases or databanks; to such purpose it shall be entitled to request the corresponding judicial authorisation to access data treatment premises, equipment or software in order to verify violations of the Act; (e) request information from public and private entities, which shall furnish the background, documents, software or other elements relating to personal data that such entities may be required; in these cases, the authorities shall guarantee the security and confidentiality of the information and elements supplied;

GDPR	The Act
Similarities (cont'd)	
	(f) enforce the administrative sanctions that may apply for the violation of the norms set forth in the Act and the regulations passed as a consequence thereof; (g) assume the role of accuser in criminal actions brought for violations of the Act; and (h) control fulfilment of requirements and guarantees to be met by private files or banks which provide reports to obtain the corresponding registration with the Register created by the Act. The Director of the AAIP shall exclusively devote to their functions, shall be subject to the incompatibility provisions set forth by law for public officers and may be removed from office by the Executive Branch on account of wrong fulfilment of their duties.
Article 58(2): Each supervisory authority shall have all of the following corrective powers: (a) to issue warnings to a controller or processor that intended processing operations are likely to infringe provisions of this Regulation; (b) to issue reprimands to a controller or a processor where processing operations have infringed provisions of this Regulation; (c) to order the controller or the processor to comply with the data subject's requests to exercise his or her rights pursuant to this Regulation; (d) to order the controller or processor to bring processing operations into compliance with the provisions of this Regulation, where appropriate, in a specified manner and within a specified period; (e) to order the controller to communicate a personal data breach to the data subject; (f) to impose a temporary or definitive limitation including a ban on processing;	Section 29(1)(f): Enforce the administrative sanctions that may apply for the violation of the norms set forth in the Act and the regulations passed as a consequence thereof; (g) assume the role of accuser in criminal actions brought for violations of the Act. Section 31(1): The maximum fine that can be applied is ARS 100,000 (approx. €880).

GDPR	The Act

Similarities (cont'd)

(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;	
(h) to withdraw a certification or to order the certification body to withdraw a certification issued pursuant to Articles 42 and 43, or to order the certification body not to issue certification if the requirements for the certification are not or are no longer met;	
(i) to impose an administrative fine pursuant to Article 83, in addition to, or instead of measures referred to in this paragraph, depending on the circumstances of each individual case;	
(j) to order the suspension of data flows to a recipient in a third country or to an international organisation.	
Article 58(3): Each supervisory authority shall have all of the following authorisation and advisory powers:	Section 29(1)(b): Pronounce the rules and regulations to be observed in the development of the activities covered by the Act;
(a) to advise the controller in accordance with the prior consultation procedure referred to in Article 36;	(d) Control compliance with the norms on data integrity and security by datafiles, registers, databases or databanks. To such purpose it shall be entitled to request the corresponding judicial authorisation to access data treatment premises, equipment or software in order to verify violations of the Act.
(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;	(e) Request information from public and private entities, which shall furnish the background, documents, software, or other elements relating to personal data that such entities may be required. In these cases, the authorities shall guarantee the security and confidentiality of the information and elements supplied.
(c) to authorise processing referred to in Article 36(5), if the law of the Member State requires such prior authorisation;	(f) Enforce the administrative sanctions that may apply for the violation of the norms set forth in the Act and the regulations passed as a consequence thereof.
(d) to issue an opinion and approve draft codes of conduct pursuant to Article 40(5);	(h) Control fulfilment of requirements and guarantees to be met by private files or banks which provide reports to obtain the corresponding registration with the Register created by the Act.
(e) to accredit certification bodies pursuant to Article 43;	
(f) to issue certifications and approve criteria of certification in accordance with Article 42(5);	
(g) to adopt standard data protection clauses referred to in Article 28(8) and in point (d) of Article 46(2);	

GDPR | The Act

Similarities (cont'd)

(h) to authorise contractual clauses referred to in point (a) of Article 46(3);	
(i) to authorise administrative arrangements referred to in point (b) of Article 46(3);	
(j) to approve binding corporate rules pursuant to Article 47.	
Article 57(1): Without prejudice to other tasks set out under this Regulation, each supervisory authority shall on its territory:	Section 29(1): The controlling Agency shall take all actions necessary to the compliance with the objectives and other provisions of the Act. To such purposes, it will have the following functions and powers:
(a) monitor and enforce the application of this Regulation;	
(b) promote public awareness and understanding of the risks, rules, safeguards and rights in relation to processing. Activities addressed specifically to children shall receive specific attention;	a) give any requesting party assistance and advise on the scope of the Act and the legal means available for the defence of the rights guaranteed by the same;
(c) advise, in accordance with Member State law, the national parliament, the government, and other institutions and bodies on legislative and administrative measures relating to the protection of natural persons' rights and freedoms with regard to processing;	b) pronounce the rules and regulations to be observed in the development of the activities covered by the Act;
(d) promote the awareness of controllers and processors of their obligations under this Regulation;	c) do a census of data files, registers or banks covered by the Act and keep a permanent record thereof;
(e) upon request, provide information to any data subject concerning the exercise of their rights under this Regulation and, if appropriate, cooperate with the supervisory authorities in other Member States to that end;	d) control compliance with the norms on data integrity and security by datafiles, registers, databases or databanks; to such purpose it shall be entitled to request the corresponding judicial authorisation to access data treatment premises, equipment or software in order to verify violations of the Act;
(f) handle complaints lodged by a data subject, or by a body, organisation or association in accordance with Article 80, and investigate, to the extent appropriate, the subject matter of the complaint and inform the complainant of the progress and the outcome of the investigation within a reasonable period, in particular if further investigation or coordination with another supervisory authority is necessary;	e) request information from public and private entities, which shall furnish the background, documents, software, or other elements relating to personal data that such entities may be required; in these cases, the authorities shall guarantee the security and confidentiality of the information and elements supplied;
(g) cooperate with, including sharing information and provide mutual assistance to, other supervisory authorities with a view to ensuring the consistency of application and enforcement of this Regulation;	f) enforce the administrative sanctions that may apply for the violation of the norms set forth in the Act and the regulations passed as a consequence thereof;
	g) assume the role of accuser in criminal actions brought for violations of the Act; and

GDPR	The Act

Similarities (cont'd)

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

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

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

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

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

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

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

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

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

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

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

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

The Director of the AAIP shall exclusively devote to their functions, shall be subject to the incompatibility provisions set forth by law for public officers and may be removed from office by the Executive Branch on account of wrong fulfilment of their duties.

Article 19 of the Right of Access Law provides that the AAIP must ensure compliance with the principles and procedures established in this law, guarantee the effective exercise of the right of access to public information and promote active transparency measures.

Moreover, Article 24 of the Right of Access Law provides the tasks of the AAIP as follows:

- design its organic operating structure and appoint its staff of agents;
- prepare their annual budget;
- draft and approve the Regulation of Access to Public Information applicable to all obligated subjects;
- implement a technological platform for the management of information requests and their corresponding responses;
- require the obliged subjects to modify or adapt their organisation, procedures, customer service systems and receipt of correspondence to the applicable regulations in order to comply with the purpose of this law;
- provide a channel of communication with citizens in order to provide advice on requests for public information and, in particular, collaborating in directing the request and refining the search;
- coordinate the work of those responsible for access to public information designated by each of the obligated subjects, in the terms of the provisions of Article 30 of the Right of Access Law;
- prepare and publish periodic statistics on applicants, requested public information, number of denials and any other matter that allows citizen control as established by the Right of Access Law;
- periodically publish an index and list of frequently required public information that enables inquiries and requests for information to be answered through the official website of the AAIP;
- publish an annual management accountability report;

GDPR | The Act

Similarities (cont'd)

(t) contribute to the activities of the Board;

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

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

- to elaborate guiding criteria and indicators of best practices destined to the obligated subjects;
- prepare and present before the Congress legislative reform proposals regarding its area of competence;
- request to the obliged subjects files, reports, documents, antecedents and any other element necessary for the purposes of exercising their work;
- disseminate the training that is carried out in order to know the scope of this law;
- receive and resolve administrative claims filed by applicants for public information according to the provisions of this law with respect to all obligated parties, with the exception of those provided for in Article 7(b) and (f) of the Right of Access Law, and publish the resolutions issued in that framework;
- promote the corresponding legal actions, for which the AAIP has active procedural legitimacy within the framework of its competence;
- promote the pertinent administrative sanctions before the corresponding competent authorities in cases of non-compliance with the provisions of this law;
- enter into cooperation agreements and contracts with public or private organisations, national or foreign, within the scope of its competence, for the fulfilment of its functions; and
- publish the reserved information indexes prepared by the obligated subjects.

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

Article 24(j) of the Right of Access Law provides that the AAIP is required to publish an annual management accountability report.

6.3. Civil remedies for individuals

Fairly consistent

Both the GDPR and the Act allow for individuals to pursue civil remedies. The Act provides that these may be filed under the notion of habeas data, with reference to material and non-material damage as well as permitting actions to be brought on behalf of the data subject.

GDPR	The Act
Similarities	
Article 79: Without prejudice to any available administrative or non-judicial remedy, including the right to lodge a complaint with a supervisory authority pursuant to Article 77, each data subject shall have the right to an effective judicial remedy where he or she considers that his or her rights under this Regulation have been infringed as a result of the processing of his or her personal data in non-compliance with this Regulation.	Section 33: (1) The action for the protection of personal data or of habeas data shall be applicable: (a) to acquire knowledge of personal data stored in public or private data files, registers or banks intended for the provision of reports, as well as purposes thereof; (b) to those cases in which the falsehood, inaccuracy or outdating of the relevant information is presumed, and the treatment of such data whose registration is prohibited by the Act, in order to demand their suppression, rectification, confidentiality or updating.
Article 82(1): Any person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered.	Section 38(2): The plaintiff shall state the reasons why they understand that the identified data file, register or bank contains information about them; the reasons why they consider that such information about them is discriminatory, false or inaccurate, and evidence of compliance with the corresponding provisions so that the rights protected by the Act could be protected.
Article 80(1): The data subject shall have the right to mandate a not-for-profit body, organisation or association which has been properly constituted in accordance with the law of a Member State, has statutory objectives which are in the public interest, and is 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.	Section 34: An action be brought by the affected party, guardian or curator thereof, and the successors of physical persons, whether they are direct or collateral descendants of such persons up to the second degree, be it by him or herself or through an attorney. When the action is brought by legal entities, it must be brought by the legal representatives or agents appointed by them to such purpose.
Article 82(2): Any controller involved in processing shall be liable for the damage caused by processing which infringes this Regulation. A processor shall be liable for	Section 35: The action shall apply in respect of public or private data banks users and persons responsible therefor.

GDPR	The Act
Differences	
the damage caused by processing only where it has not complied with obligations of this Regulation specifically directed to processors or where it has acted outside or contrary to lawful instructions of the controller. Article 82(3): A controller or processor shall be exempt from liability under paragraph 2 if it proves that it is not in any way responsible for the event giving rise to the damage.	The Act does not refer to exceptions in relation to civil remedies for individuals.