Comparing privacy laws:
GDPR v. Federal Law and Regulations

OneTrust DataGuidance™
REGULATORY RESEARCH SOFTWARE

About the authors

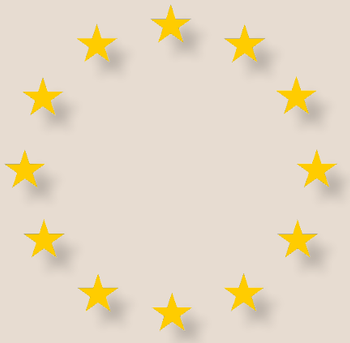
OneTrust DataGuidance™ provides a suite of privacy solutions designed to help organisations monitor regulatory developments, mitigate risk and achieve global compliance.

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 Federal Law/ 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 General Data Protection Regulation (Regulation (EU) 2016/679) ('GDPR') came into effect on 25 May 2018 and governs the protection of personal data in EU and EEA Member States. The Data Protection Federal Law/ Regulations (2021 Revision) ('the Federal Law/ Regulations') is the primary piece of data protection legislation in the Cayman Islands, which updated the Data Protection Law, 2017 (Law 33 of 2017). The Federal Law/ Regulations established the Office of the Ombudsman ('the Ombudsman') and is supplemented by the Data Protection Regulations, 2018 (SL 17 of 2019) ('the Regulations').

The Federal Law/ Regulations is based on eight principles, which provide a general framework for personal data protection that is similar to the GDPR. For instance, the Federal Law/ Regulations sets out requirements for data subject rights, breach notifications, data transfers, and sensitive data. Indeed, the Federal Law/ Regulations cites European adequacy decisions as a basis for enabling international data transfers. However, the GDPR and the Federal Law/ Regulations differ in areas such as data protection officer and impFederal Law/ Regulations assessment obligations, and the Federal Law/ Regulations combines rights to information and access.

This overview organises provisions from the GDPR and the Federal Law/ Regulations 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 Federal Law/ Regulations.

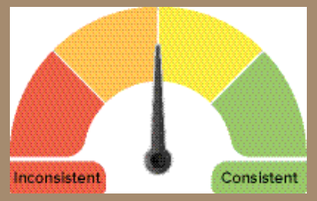
Key for giving the consistency rate

Consistent: The GDPR and the Federal Law/ Regulations bear a high degree of similarity in the rationale, core, scope, and the application of the provision considered.

Fairly consistent: The GDPR and the Federal Law/ Regulations 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 Federal Law/ Regulations 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 Federal Law/ Regulations 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 Federal Law/ Regulationsed upon without specific legal advice based on particular circumstances.

1. Scope

1.1. Personal scope

The Federal Law employs similar core concepts as the GDPR and refers to data controllers, data processors, and data subjects. The GDPR and the Federal Law differ, however, in that the latter does not refer to the nationality, place of residence of data subjects, public bodies, or make reference to deceased individuals.

GDPR	Federal Law/ Regulations
Data controller	
Article 4(7): 'controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.	Article 3(XIV) of the Federal Law: Individual or private legal entity that decides on the processing of personal data.
Data processor	
Article 4(8): 'processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.	Article 3(IX) of the Federal Law: The individual or legal entity that, alone or jointly with others, processes personal data on behalf of the data controller.
Data subject	
Article 4(1): 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more fFederal Law/ Regulationsors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.	Article 3(XVII) of the Federal Law: 'Data owner' means the individual to whom personal data relates.
Public bodies	
Article 4(7): 'controller' means the natural or legal person, public authority, agency or other body.	Neither the Federal Law nor the Regulations refer to the public bodies.

GDPR	Federal Law/ Regulations
Nationality of data subject	
Recital 14: The protection afforded by this Regulation should apply to natural persons, whatever their nationality or place of residence, in relation to the processing of their personal data.	Neither the Federal Law nor the Regulations refer to the nationality of data subjects.
Place of residence	
See Recital 14, above.	Neither the Federal Law nor the Regulations refer to the place of residence of data subjects.
Deceased individuals	
Recital 27: This Regulation does not apply to the personal data of deceased persons. Member States may provide for rules regarding the processing of personal data of deceased persons.	Neither the Federal Law nor the Regulations have provisions on deceased individuals.

1.2. Territorial scope

Fairly inconsistent

In general terms, and unlike the GDPR, the Federal Law does not apply extraterritorially, nor does it explicitly regulate goods and services or monitoring from abroad. The Federal Law does, however, specify that it applies to corporate bodies incorporated outside of Mexico.

GDPR	Federal Law/ Regulations
Establishment in jurisdiction	
Article 3: This Regulation applies to the processing of personal data in the context of the Federal Law/ Regulationsivities 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 Federal Law/ Regulationsivity through stable arrangements.	Article 4 of the Regulations: These Regulations will be obligatory for all processing when: (I) it is carried out in an establishment of the data controller located in Mexico; (II) it is carried out by a data processor, regardless of its location, on behalf of a data controller established in Mexico; (III) the data controller is not established in Mexico but is subject to Mexican laws as a consequence of entering into a contract or under international law; and (IV) the data controller is not established in Mexico and uses media located in Mexico, unless such media are used only for transit purposes that do not involve processing. For purposes of this subsection, the data controller shall provide the media necessary to comply with the obligations imposed by the Federal Law, its Regulations, and other applicable rules and regulations with respect to the processing of personal data. For this purpose, it shall designate a representative or implement the mechanism that it considers appropriate, provided that by means of this, it is ensured that the data controller will be able to effectively comply with the obligations that are imposed by law on individuals and corporate bodies that deal with personal data in Mexico. When the data controller is not located in Mexico, but the data processor is, the latter shall be subject to the provisions related to the security measures contained in Chapter III of the Regulations. In the case of individuals, the establishment shall mean the location of their main place of business or that used to perform their activities or their home. In case of corporate bodies, the establishment shall mean the location of the principal management of the business; in case of corporate bodies residing abroad, the location of the principal management of the business; in case of corporate bodies residing abroad, the location of the principal management of the business in Mexico, or in the absence thereof, that designated by them or any stable installation that allows actual or real performance of an activity.

GDPR	Federal Law/ Regulations
Extraterritorial	
See Article 3, above.	See Article 4 of the Regulations above.
Goods & servicies from abroad	
Recital 23: In order to ensure that natural persons are not deprived of the protection to which they are entitled under this Regulation, the processing of personal data of data subjects who are in the Union by a controller or a processor not established in the Union should be subject to this Regulation where the processing Federal Law/ Regulationsivities are related to offering goods or services to such data subjects irrespective of whether connected to a payment.	Neither the Federal Law nor the Regulations refer to goods and services from abroad.
Monitoring from abroad	
Recital 24: The processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union should also be subject to this Regulation when it is related to the monitoring of the behaviour of such data subjects in so far as their behaviour takes place within the Union.	Neither the Federal Law nor the Regulations refer to monitoring from abroad.

1.3. Material scope

Fairly consistent

The Federal Law and the GDPR provide definitions of personal data and data processing, as well as setting out specific requirements for special categories of, or sensitive, data. The two pieces of legislation differ, however, in terms of the general exemptions they stipulate, and in regard to anonymised and pseudonymised data.

GDPR	Federal Law/ Regulations
Personal data/ personal information	
Article 4(1): 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more fFederal Law/ Regulationsors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.	Article 3(V) of the Federal Law: 'personal data' means any information concerning an identified or identifiable individual.
Data processing	
Article 4(2): 'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.	Article 3(XVIII) of the Federal Law: 'processing' means the retrieval, use, disclosure or storage of personal data by any means. Use covers any action of access, management, exploitation, transfer or disposal of personal data.
Special categories of data	
Article 9(1): Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.	Article 3(VI) of the Federal Law: 'sensitive personal data' refers to personal data touching on the most private areas of the data subject's life, or whose misuse might lead to discrimination or involve a serious risk for said data subject. In particular, sensitive data is considered that which may reveal items such as racial or ethnic origin, present and future health status, genetic information, religious, philosophical and moral beliefs, union membership, political views, sexual preference.

GDPR	Federal Law/ Regulations

Anonymised data

Recital 26: The principles of data protection should not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable.	Neither the Federal Law nor the Regulations refer to anonymised data.

Pseudonymised data

Article 4(5): 'pseudonymisation' means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.	Neither the Federal Law nor the Regulations refer to pseudonymised data.

Automated processing

Article 2(1): This Regulation applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.	Article 14 of the Regulations: When the data controller uses remote or local electronic, optical or other technological means of communication mechanisms that allow personal data to be obtained automatically and simultaneously at the time the data subject has contact with the mechanisms, at the same time the data subject must be informed of the use of such technology, that through these mechanisms personal data will be obtained, and of the manner in which this can be disabled.

General exemptions

Article 2(2): This Regulation does not apply to the processing of personal data: (a) in the course of an Federal Law/ Regulationsivity which falls outside the scope of Union law; (b) by the Member States when carrying out Federal Law/ Regulationsivities 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 Federal Law/ Regulationsivity.	Article 2 of the Federal Law: The parties regulated under the Federal Law are private parties, whether individuals or private legal entities, that process personal data, with the exception of: (I) credit reporting companies under the Law Regulating Credit Reporting Companies and other applicable laws; and (II) persons carrying out the collection and storage of personal data that is exclusively for personal use, and without purposes of disclosure or commercial use.

2. Key definitions

Fairly consistent

2.1. Personal data

The GDPR and the Federal Law 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 Federal Law does not directly address online identifiers.

GDPR	Federal Law/ Regulations

Personal data/ personal information

Article 4(1): 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more fFederal Law/ Regulationsors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.	Article 3(V) of the Federal Law: 'personal data' means any information concerning an identified or identifiable individual.

Special categories of data

Article 9(1): Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.	Article 3(VI) of the Federal Law: 'sensitive personal data' refers to personal data touching on the most private areas of the data subject's life, or whose misuse might lead to discrimination or involve a serious risk for said data subject. In particular, sensitive data is considered that which may reveal items such as racial or ethnic origin, present and future health status, genetic information, religious, philosophical and moral beliefs, union membership, political views, sexual preference.

Online identifiers

Recital 30: Natural persons may be associated with online identifiers provided by their devices, applications, tools and protocols, such as internet protocol addresses, cookie identifiers or other identifiers such as radio frequency identification tags. This may leave traces which, in particular when combined with unique identifiers and other information received by the servers, may be used to create profiles of the natural persons and identify them.	Neither the Federal Law nor the Regulations refer to online identifiers.

2.2. Pseudonymisation

Unlike the GDPR, the Federal Law does not address anonymisation and pseudonymisation.

GDPR	Federal Law/ Regulations
Anonymisation	
Recital 26: 'anonymous information' is information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable.	Neither the Federal Law nor the Regulations define or refer to anonymisation.
Pseudonymisation	
Article 4(5): 'pseudonymisation' means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.	Neither the Federal Law nor the Regulations define or refer to pseudonymisation.

2.3. Controllers and processors

The Federal Law and the GDPR provide similar definitions for data controllers and data processors, as well as the requirements for agreements between these parties. Unlike the GDPR, however, the Federal Law does not explicitly refer to the appointment of a data protection officer ('DPO') or consider Data Protection Impact Assessments ('DPIAs').

GDPR	Federal Law/ Regulations
Data controller	
Article 4(7): 'controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.	Article 3(XIV) of the Federal Law: Individual or private legal entity that decides on the processing of personal data.
Data processor	
Article 4(8): 'processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.	Article 3(IX) of the Federal Law: The individual or legal entity that, alone or jointly with others, processes personal data on behalf of the data controller.
Controller and processor contrFederal Law/ Regulationss	
Article 28(3): Processing by a processor shall be governed by a contrFederal Law/ Regulations or other legal Federal Law/ Regulations 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 contrFederal Law/ Regulations.]	Article 51 of the Regulations: The relationship between the data controller and data processor must be established by contract or other legal instrument decided upon by the data controller and that permits its existence, scope, and contents to be proven.
Data Protection Impact Assessment ('DPIA')	
DPIA is not specifically defined, however Article 35 sets out requirements for DPIAs (see section 5.3. for further information).	Neither the Federal Law nor the Regulations address DPIAs.

GDPR	Federal Law/ Regulations
Data Protection Officer ('DPO')	
DPO is not specifically defined, however Article 37 sets out requirements related to DPOs (see section 5.4. for further information).	DPO is not specifically defined, however Article 30 of the Federal Law refers to the requirement that all data controllers must designate a personal data person or department who will process requests from data subject for the exercise of the rights referred to in the Federal Law.

2.4. Children

Unlike the GDPR, the Federal Law does not provide additional requirements for children's data.

GDPR	Federal Law/ Regulations
Children's definition	
The GDPR does not specifically define 'child'. However, Article 8(1) provides: Where point (a) of Article 6(1) applies, in relation to the offer of information society services directly to a child, the processing of the personal data of a child shall be lawful where the child is at least 16 years old. Where the child is below the age of 16 years, such processing shall be lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility over the child. Member States may provide by law for a lower age for those purposes provided that such lower age is not below 13 years.	Neither the Federal Law nor the Regulations define children's data.
Consent for processing children's data	
Article 8(2): The controller shall make reasonable efforts to verify in such cases that consent is given or authorised by the holder of parental responsibility over the child, taking into consideration available technology.	The Federal Law/ Regulations does not address consent for processing children's data.
Privacy notice (children)	
Recital 58: Given that children merit specific protection, any information and communication, where processing is addressed to a child, should be in such a clear and plain language that the child can easily understand.	The Federal Law does address children's data indirectly. Article 89 of the Regulations: ARCO rights may be exercised: [...] (II) By the representative of the data subject, after proving: a) the identity of the data subject; b) the identity of the representative, and c) the existence of the representation by means of a public instrument or simple power of attorney signed before two witnesses or by personal attendance by the data subject. For the exercise of ARCO rights by minors or by a person under interdiction or without legal capacity, the representation rules of the Federal Civil Code shall apply.

2.5. Research

Unlike the GDPR, the Federal Law does not address processing for scientific or historical research purposes.

GDPR	Federal Law/ Regulations

Scientific/ historical research definition

GDPR	Federal Law/ Regulations
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.	Neither the Federal Law nor the Regulations address processing for scientific or historical research purposes.

Compatibility with original purpose of collection

GDPR	Federal Law/ Regulations
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').	Neither the Federal Law nor the Regulations address processing for scientific or historical research purposes.

Appropriate safeguards

GDPR	Federal Law/ Regulations
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.	Neither the Federal Law nor the Regulations address processing for scientific or historical research purposes.

GDPR	Federal Law/ Regulations

Data subject rights (research)

GDPR	Federal Law/ Regulations
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.	Neither the Federal Law nor the Regulations address processing for scientific or historical research purposes.

3. Legal basis

Fairly inconsistent

The Federal Law sets out different grounds for the processing of personal data and does not address matters such as processing for journalistic/artistic purposes. However, the Federal Law provides similarities to the GPDR in terms of additional requirements for the processing of sensitive data and defining conditions for consent.

GDPR	Federal Law/ Regulations

Legal grounds

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

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

(b) processing is necessary for the performance of a contrFederal Law/ Regulations 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 contrFederal Law/ Regulations;

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

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

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

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

Article 8 of the Federal Law: All processing of personal data will be subject to the consent of the data subject except as otherwise provided by the Federal Law.

Article 10: Consent for processing of personal data will not be necessary where:

I. any Law so provides;

II. the data is contained in publicly available sources;

III. the personal data is subject to a prior dissociation procedure;

IV. it has the purpose of fulfilling obligations under a legal relationship between the data subject and the data controller;

V. there is an emergency situation that could potentially harm an individual in their person or property;

VI. it is essential for medical attention, prevention, diagnosis, health care delivery, medical treatment or health services management, where the data subject is unable to give consent in the terms established by the General Health Law and other applicable laws, and said processing of data is carried out by a person subject to a duty of professional secrecy or an equivalent obligation; or

VII. a resolution is issued by a competent authority.

Article 40 of the Regulations: Personal data may be processed only to comply with the purpose or purposes set out in the privacy notice.

GDPR	Federal Law/ Regulations

Sensitive data (legal basis)

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

Article 15(III) of the Federal Law: The data controller must obtain the express consent of the data subject in the case of sensitive data.

Conditions for consent

Article 7(3): The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent.
Article 4: (11) 'consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative Federal Law/ Regulationsion, signifies agreement to the processing of personal data relating to him or her.

Article 8 of the Federal Law: All processing of personal data will be subject to the consent of the data subject except as otherwise provided by the Federal Law.
Consent will be express when such is communicated verbally, in writing, by electronic or optical means or via any other technology, or by unmistakable indications.
It will be understood that the data subject tacitly consents to the processing of their data when, once the privacy notice has been made available to them, and they do not express objection.

Financial or asset data will require the express consent of the data subject, except as provided in Articles 10 and 37 of the Federal Law. Consent may be revoked at any time without retroactive effects being attributed thereto. For revocation of consent, the data controller must, in the privacy notice, establish the mechanisms and procedures for such action.

Article 12 of the Regulations: Obtaining consent, tacitly or explicitly, shall be:

(I) Free: without error, bad faith, violence or fraud that may affect the expression of the will of the data subject:

(II) Specific: refer to one or several specific purposes that justify the processing; and

(III) Informed: the data subject must previously know from the privacy notice, the processing to be done with their personal data and the consequences of granting their consent.

Express consent must also be unequivocal, in other words, that there are elements that unquestionably demonstrate that it was given.

GDPR	Federal Law/ Regulations
Journalism/artistic purposes	
Article 85(1): Member States shall by law reconcile the right to the protection of personal data pursuant to this Regulation with the right to freedom of expression and information, including processing for journalistic purposes and the purposes of academic, artistic or literary expression.	Neither the Federal Law nor the Regulations address processing for journalistic or artistic purposes.

4. Controller and processor obligations

4.1. Data transfers

The Federal Law does not outline alternative mechanisms for data transfers such as binding corporate rules. Instead, the Federal Law sets out that data transfers need to be mentioned in a privacy notice and imposes the same obligations on a receiver of the data as the data controller. The Regulations further enable the free flow of data between data controllers and data processors.

GDPR	Federal Law/ Regulations
Adequate protection	
Article 45(1): A transfer of personal data to a third country or an international organisation may take place where the Commission has decided that the third country, a territory or one or more specified sectors within that third country, or the international organisation in question ensures an adequate level of protection. Such a transfer shall not require any specific authorisation.	Not applicable.
Other mechanisms for data transfers	
Article 46(1): In the absence of a decision pursuant to Article 45(3), a controller or processor may transfer personal data to a third country or an international organisation only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available. (2) The appropriate safeguards referred to in paragraph 1 may be provided for, without requiring any specific authorisation from a supervisory authority, by: (a) a legally binding and enforceable instrument between public authorities or bodies; (b) binding corporate rules in accordance with Article 47; (c) standard data protection clauses adopted by the Commission in accordance with the examination procedure referred to in Article 93(2); (d) standard data protection clauses adopted by a supervisory authority and approved by the Commission pursuant to the examination procedure referred to in Article 93(2);	Article 36 of the Federal Law: Where the data controller intends to transfer personal data to domestic or foreign third parties other than the data processor, it must provide them with the privacy notice and the purposes to which the data subject has limited data processing. Data processing will be done as agreed in the privacy notice, which shall contain a clause indicating whether or not the data subject agrees to the transfer of his data; moreover, the third party receiver will assume the same obligations as the data controller that has transferred the data. Article 53 of the Regulations: National and international transmissions of personal data between a data controller and a data processor need not be informed to the data subject or their consent obtained. The data processor shall be considered as a data controller, together with its own obligations, when it: (I) uses the personal data for a purpose different from that authorised by the data controller; or

GDPR	Federal Law/ Regulations
Other mechanisms for data transfers	
(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) contrFederal Law/ Regulationsual clauses between the controller or processor and the controller, processor or the recipient of the personal data in the third country or international organisation; or (b) provisions to be inserted into administrative arrangements between public authorities or bodies which include enforceable and effective data subject rights.	(II) makes a transfer without complying with the instructions of the data controller. The data processor will not be held responsible when, at the express indication of the data controller, it transmits the personal data to another data processor designated by the latter, to which it had entrusted the performance of a service, or transfers the personal data to another data controller pursuant to the Regulations.
Data localisation	
Not applicable.	Not applicable.

4.2. Data processing records

While the GDPR requires both data controllers and data processors to maintain data processing records, the Federal Law does not directly provide such an obligation. Instead, the Federal Law and the Regulations outline more general concepts of security requirements, some of which may overlap with expectations for record-keeping.

GDPR	Federal Law/ Regulations
Data controller obligation	
Article 30(1): Each controller and, where applicable, the controller's representative, shall maintain a record of processing Federal Law/ Regulationsivities under its responsibility. That record shall contain all of the following information: (a) the name and contFederal Law/ Regulations 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 Federal Law does not directly address record-keeping requirements. Certain articles may, however, be considered relevant, including: Article 14 of the Federal Law: The data controller shall ensure compliance with the personal data protection principles established by the Federal Law, and shall adopt all necessary measures for their application. The foregoing will apply even when this data has been processed by a third party at the request of the data controller. Article 19 of the Federal Law: All responsible parties that process personal data must establish and maintain physical and technical administrative security measures designed to protect personal data from damage, loss, alteration, destruction, or unauthorised use, access, or processing. Data controllers will not adopt security measures inferior to those they keep to manage their own information. Moreover, the risk involved, potential consequences for the data subjects, sensitivity of the data, and technological development will be taken into account.

GDPR	Federal Law/ Regulations

Data processor obligation

GDPR	Federal Law/ Regulations
Article 30(2): Each processor and, where applicable, the processor's representative shall maintain a record of all categories of processing Federal Law/ Regulationsivities carried out on behalf of a controller, containing: (a) the name and contFederal Law/ Regulations details of the processor or processors and of each controller on behalf of which the processor is Federal Law/ Regulationsing, and, where applicable, of the controller's or the processor's representative, and the data protection officer; (b) the categories of processing carried out on behalf of each controller; (c) where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards; and (d) where possible, a general description of the technical and organisational security measures referred to in Article 32(1).	Article 50 of the Regulations: The data processor shall have the following obligations with respect to the processing carried out on behalf of the data controller: [...] (III) Implement the security measures required by the Federal Law, the Regulations, and other applicable laws and regulations.

Records format

Article 30(3): The records referred to in paragraphs 1 and 2 shall be in writing, including in electronic form.	Neither the Federal Law nor the Regulations address the format for data processing records.

Required to make available

Article 30(4): The controller or the processor and, where applicable, the controller's or the processor's representative, shall make the record available to the supervisory authority on request.	Neither the Federal Law nor the Regulations provide specific requirements to make data processing record available.

Exemptions

Article 30(5): The obligations referred to in paragraphs 1 and 2 shall not apply to an enterprise or an organisation employing fewer than 250 persons unless the processing it carries out is likely to result in a risk to the rights and freedoms of data subjects, the processing is not occasional, or the processing includes special categories of data as referred to in Article 9(1) or personal data relating to criminal convictions and offences referred to in Article 10.	Neither the Federal Law nor the Regulations provide specific exemptions from data processing record requirements.

GDPR	Federal Law/ Regulations

General Data Processing Notification ('DPN')

Not applicable.	Neither the Federal Law nor the Regulations provide DPN requirements.

4.3. Data protection impFederal Law/ Regulations assessment

Unlike the GDPR, the Federal Law does not provide requirements for DPIAs.

GDPR	Federal Law/ Regulations

When is a DPIA required

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

Neither the Federal Law nor the Regulations provide requirements for DPIAs for data controllers or processors.

However, Article 48(V) of the Regulations expands on the minimum obligations imposed upon data controllers to ensure the proper processing of personal data which includes a requirement to implement a procedure to deal with the risk to the protection of personal data by the implementation of new products, services, technologies, and business models, as well as to mitigate them.

Article 39(X) of the Federal Law places an obligation on the National Institute for Transparency, Access to Information and Personal Data Protection ('INAI') to carry out studies of the impact on privacy prior to the implementation of new types of processing of personal data or material modification of existing types of processing.

DPIA content requirements

Article 35(7): The assessment shall contain at least:
(a) a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller;
(b) an assessment of the necessity and proportionality of the processing operations in relation to the purposes;
(c) an assessment of the risks to the rights and freedoms of data subjects referred to in paragraph 1; and
(d) the measures envisaged to address the risks, including

Neither the Federal Law nor the Regulations provide content requirements for DPIAs.

GDPR	Federal Law/ Regulations

DPIA content requirements

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

Consultation with authority

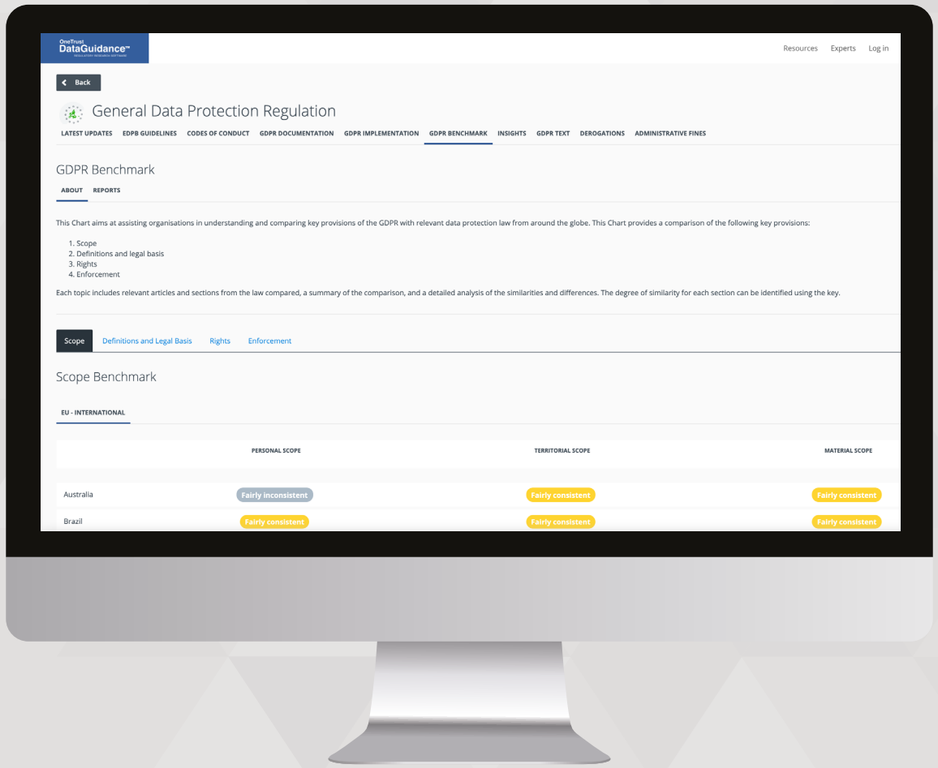
Article 36(1): The controller shall consult the supervisory authority prior to processing where a data protection impFederal Law/ Regulations assessment under Article 35 indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk.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

See Article 39(X) of the Federal Law above.

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

4.4. Data protection officer appointment

Although the Federal Law does not provide for the appointment of a data protection officer ('DPO'), INAI has released Recommendations for the Designation of the Person or Department Responsible for Data Protection (August 2016) (only available in Spanish here) ('the Recommendations'). The Federal Law and the Recommendations present some similarities with the GDPR in relation to the tasks of a DPO. Unlike the GDPR, however, neither the Federal Law nor the Recommendations provide for group appointments or notification of a DPO appointment.

GDPR	Federal Law/ Regulations

DPO tasks

GDPR	Federal Law/ Regulations
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 impFederal Law/ Regulations assessment and monitor its performance pursuant to Article 35; (d) to cooperate with the supervisory authority; and (e) to Federal Law/ Regulations as the contFederal Law/ Regulations point for the supervisory authority on issues relating to processing, including the prior consultation referred to in Article 36, and to consult, where appropriate, with regard to any other matter.	Article 30 of the Federal Law: All data controllers must designate a personal data person or department who will process requests from data subjects for the exercise of the rights referred to in the Federal Law. In addition, data controllers must promote the protection of personal data within their organisations.

When is a DPO required

GDPR	Federal Law/ Regulations
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 Federal Law/ Regulationsing in their judicial capacity; (b) the core Federal Law/ Regulationsivities 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	See Article 30 of the Federal Law above.

GDPR	Federal Law/ Regulations

When is a DPO required (cont'd)

GDPR	Federal Law/ Regulations
(c) the core Federal Law/ Regulationsivities 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.	

Group appointments

GDPR	Federal Law/ Regulations
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.	Neither the Federal Law nor the Regulations provide group appointment requirements for data protection officers.

Notification of DPO

GDPR	Federal Law/ Regulations
Article 37(7): The controller or the processor shall publish the contFederal Law/ Regulations details of the data protection officer and communicate them to the supervisory authority.	Neither the Federal Law nor the Regulations provide notification requirements for data protection officers.

Qualifications

GDPR	Federal Law/ Regulations
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 prFederal Law/ Regulationsices and the ability to fulfil the tasks referred to in Article 39.	There is no requirement under the Federal Law for DPOs or departments to have specific qualifications. However, the INAI advises that the DPO or persons appointed within the data protection department should satisfy the following requirements (the Recommendations): (I) have experience dealing with data protection issues or similar areas (such as compliance and auditing); (II) be knowledgeable of data protection and data security regulations and issues; and (III) have organisational, communicational and leadership skills.

4.5. Data security and data breaches

While the Federal Law provides for the use of technical security measures, it does not specify breach notification requirements to INAI. However, the Federal Law provides some similarities with the GDPR in terms of notifying data subjects of security incidents.

GDPR	Federal Law/ Regulations

Security measures defined

GDPR	Federal Law/ Regulations
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.	The Federal Law does not define security measures. Article 2(VII) of the Regulations: 'Technical security measures' is defined as a combination of activities, controls, and mechanisms with measurable results that use technology to ensure that: a) access to logical databases or to information in logical format is by identified and authorised users; b) the access referred to in the previous paragraph is only so that the user may carry out the activities required by their position; c) actions to acquire, operate, develop, and maintain secure systems are included; and d) the management of communications and computerised resources used in the processing of personal data is carried out.

Data breach notification to authority

GDPR	Federal Law/ Regulations
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.	Neither the Federal Law nor the Regulations directly address breach notifications to authorities.

Timeframe for breach notification

GDPR	Federal Law/ Regulations
See Article 33(1) above.	Article 64 of the Regulations: The data controller must inform the data subject, without delay, of breaches that significantly prejudice the property or nonpecuniary rights of the data subjects upon confirming the breach and having taken action to trigger an exhaustive review of the magnitude of the breach so that the prejudiced data subjects may take the appropriate measures.

GDPR	Federal Law/ Regulations

Notifying data subjects of data breach

GDPR	Federal Law/ Regulations
Article 34(1): When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay.	Article 20 of the Federal Law: Security breaches occurring at any stage of processing that materially affect the property or moral rights of data subjects will be reported immediately by the data controller to the data subject, so that the latter can take appropriate action to defend its rights. In addition, see Article 64 of the Regulations above.

Data processor notification of data breach

GDPR	Federal Law/ Regulations
Article 33(2): The processor shall notify the controller without undue delay after becoming aware of a personal data breach.	The Federal Law does not provide requirements for data processor notification of data breaches.

Exceptions

GDPR	Federal Law/ Regulations
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.	Not applicable.

4.6. Accountability

Farily consisntent

While the Regulations explicitly addresses a concept of accountability, neither the Federal Law nor the Regulations define the liabilities of data processors. The Federal Law, though, specifies that data controllers are liable for violations of its principles.

GDPR	Federal Law/ Regulations

Principle of accountability

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

The Federal Law does not provide a definition for the principle of accountability.

Article 47 of the Regulations: Pursuant to Articles 6 and 14 of the Federal Law, the data controller has the obligation to protect and be responsible for the processing of personal data found in its custody or in its possession or for those it communicated to a data processor, whether or not the latter is located in Mexico.

To comply with this obligation, the data controller may use standards, best international practices, corporate policies, self-regulation arrangements, or any other mechanism that it determines is adequate for such purpose.

In addition, Article 48 of the Regulations sets out measures for the principle of accountability, pursuant to Article 14 of the Federal Law, that the data controller must adopt measures to guarantee the proper processing of personal data, giving priority to the interests of the data subject and the reasonable expectation of privacy.

These measures include at least the following:

(I) prepare privacy policies and programs that are binding and enforceable within the organisation of the data controller;

(II) implement a program of training, updating, and raising the awareness of personnel about obligations in matters of protection of personal data;

(III) establish an internal supervision and monitoring system, as well as external inspections or audits to verify compliance with privacy policies;

(IV) dedicate resources for the implementation of privacy programs and policies;

(V) implement a procedure to deal with the risk to the protection of personal data by the implementation of new products, services, technologies, and business models, as well as to mitigate them;

(VI) periodically review the security policies and programs to determine modifications required;

(VII) establish procedures to receive and respond to the questions and complaints of data subjects;

GDPR	Federal Law/ Regulations

Principle of accountability (cont'd)

(VIII) have mechanisms to comply with privacy policies and programs, as well as sanctions for a breach thereof;

(IX) establish measures to protect personal data, in other words, a group of technical and administrative actions that will allow the data controller to ensure compliance with the principles and obligations established by the Federal Law and the Regulations; or

(X) establish measures to trace personal data, in other words, actions, measures, and technical procedures that will allow the tracing of personal data while being processed.

Liability of data controllers and data processors

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

Article 63(IV) of the Federal Law: Data controllers are in violation of the Federal Law where they are processing personal data in violation of the principles established in the Federal Law.

5. Rights

5.1. Right to erasure

Both the GDPR and the Federal Law provide that data subjects may request the cancelation or erasure of their data in certain circumstances and for legitimate reasons. In addition, both pieces of legislation set out requirements governing the process of the exercise of this right.

GDPR	Federal Law/ Regulations

Grounds for erasure

Article 17(1): The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:
(a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
(b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing;
(c) the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2);
(d) the personal data have been unlawfully processed;
(e) the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject;
(f) the personal data have been collected in relation to the offer of information society services referred to in Article 8(1).

Article 25 of the Federal Law: The data subject will at all times have the right to cancel their personal data. Cancellation of personal data will lead to a blocking period following which the data will be erased. The data controller may retain data exclusively for purposes pertaining to responsibilities arising from processing. The blocking period will be equal to the limitation period for actions arising from the legal relationship governing processing pursuant to applicable law. Once the data is cancelled, the data subject will be notified. Where personal data has been transmitted prior to the date of rectification or cancellation and continues to be processed by third parties, the data controller must notify them of the request for rectification or cancellation, so that such third parties also carry it out.
Article 105 of the Regulations: Pursuant to Article 25 of the Federal Law, cancellation means stopping the processing of personal data by the data controller, starting from their blockage and subsequent suppression.
Article 106 of the Regulations: The data subject may request, at any time, that the data controller cancel the personal data when they considers that it is not being processed in accordance with the principles and duties established by the Federal Law and the Regulations. The cancellation shall proceed with respect to all personal data of the data subject contained in a database, or only part thereof, as requested.

Inform data subject of right

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

Article 16 of the Federal Law: The privacy notice must contain at least the following information: [...] (IV) the means for exercising rights of access, rectification, cancellation or objection, in accordance with the provisions of the Federal Law.

GDPR	Federal Law/ Regulations

Inform data subject of right

by electronic means. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means.
Article 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.

Fees

Article 12(5): Information provided under Articles 13 and 14 and any communication and any Federal Law/ Regulationsions 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 charFederal Law/ Regulationser, the controller may either:
(a) charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the Federal Law/ Regulationsion requested; or
(b) refuse to Federal Law/ Regulations on the request.
The controller shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request.

Article 35 of the Federal Law: The action of providing personal data will be free, and the data subject must only pay justified expenses of shipping or the cost of copying or providing data in other formats. This right will be exercised by the data subject free of charge, upon proof of their identity to the data controller. However, if the same person repeats their request within a period of 12 months, costs will not be greater than three days of the General Current Minimum Wage in Mexico City, unless there are material changes to the privacy notice that prompt new queries. The data subject may file a data protection request due to the response received or lack of response from the data controller, in accordance with the provisions of Chapter VI of the Federal Law.

Response timeframe

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

Article 32 of the Federal Law: The data controller will notify the data subject, within a maximum of 20 days counted from the date of receipt of the request for access, rectification, cancellation, or objection, of the determination made, so that, where appropriate, same will become effective within 15 days from the date on which the notice is provided. For personal data access requests, delivery will be made upon proof of identity of the requesting party or legal representative.

The aforementioned time periods may be extended a single time by a period of equal length, provided that such action is justified by the circumstances of the case

GDPR	Federal Law/ Regulations

Format of response

Article 12(1): The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means.	The Federal Law does not explicitly refer to the format of the response to a right to erasure request. [Note: Article 29 of the Federal Law details requirements for the data subject's request to exercise rights.]

Publicly available data

Article 17(2): Where the controller has made the personal data public and is obliged pursuant to paragraph 1 to erase the personal data, the controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data.	Article 10(II) of the Federal Law: Consent for processing of personal data will not be necessary where, among other things, the data is contained in publicly available sources.

Exceptions

Article 17(3): Paragraphs 1 and 2 shall not apply to the extent that processing is necessary: (a) for exercising the right of freedom of expression and information; (b) for compliance with a legal obligation which requires processing by Union or Member State law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; (c) for reasons of public interest in the area of public health in accordance with points (h) and (i) of Article 9(2) as well as Article 9(3); (d) for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) in so far as the right referred to in paragraph 1 is likely to render impossible or seriously impair the achievement of the objectives of that processing; or (e) for the establishment, exercise or defence of legal claims. Article 12(5): Information provided under Articles 13 and 14 and any communication and any Federal Law/ Regulationsions 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 charFederal Law/ Regulationser, the controller may either:	Article 26 of the Federal Law: The data controller will not be obligated to cancel personal data when: (I) it relates to the parties of a private or administrative contract or partnership agreement and is necessary for its performance and enforcement; (II) the law requires that it be processed; (III) such action hinders judicial or administrative proceedings relating to tax obligations, investigation and prosecution of crimes, or updating of administrative sanctions; (IV) it is necessary to protect the legally protected interests of the data subject; (V) it is necessary to carry out an action in the public interest; (VI) it is necessary to fulfil an obligation legally undertaken by the subject, and (VII) it is subject to processing for medical diagnosis or prevention or health services management, provided such processing is done by a health professional subject to a duty of secrecy. Article 34 of the Federal Law: The data controller may deny access to personal data or refuse the rectification, cancellation, or objection with relation thereto in the following cases: (I) where the requesting party is not the subject of the personal data, or the legal representative is not duly accredited for such purposes;

GDPR	Federal Law/ Regulations

Exceptions (cont'd)

(a) charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the Federal Law/ Regulationsion requested; or (b) refuse to Federal Law/ Regulations on the request. The controller shall bear the burden of demonstrating the manifestly unfounded or excessive charFederal Law/ Regulationser of the request. The The Federal Law/ Regulations does not provide specific exceptions to a right to erasure.	(II) where the requesting party's personal data is not found in the data controller's database; (III) where the rights of a third party are adversely affected; (IV) where there is any legal impediment, or decision of a competent authority, restricting access to the personal data or not allowing the rectification, cancellation, or objection with relation thereto, and (V) where the rectification, cancellation, or objection has been previously performed. The refusal referred to in Article 34 of. theFederal Law may be partial, in which case the data controller will carry out the access, rectification, cancellation, or objection requested by the data subject. In all of the aforementioned cases, the data controller must notify the data subject, or, as appropriate, their legal representative, of its decision and the reason for such decision, within the periods established for such purposes, via the same means by which the request was made, attaching, where appropriate, any relevant evidence.

5.2. Right to be informed

Fairly consistent

The Federal Law and the GDPR stipulate generally similar requirements for information that should be provided to data subjects. However, the provisions on exceptions to this right are stipulated in secondary guidance from INAI rather than in either the Federal Law or the Regulations themselves.

GDPR	Federal Law/ Regulations

Informed prior to/ at collection

Article 13(1): Where personal data relating to a data subject are collected from the data subject, the controller shall, at the time when personal data are obtained, provide the data subject with all of the following information:
(a) the identity and the contFederal Law/ Regulations details of the controller and, where applicable, of the controller's representative;
(b) the contFederal Law/ Regulations 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 fFederal Law/ Regulations that the controller intends to transfer personal data to a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1), reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available.
(2) In addition to the information referred to in paragraph 1, the controller shall, at the time when personal data are obtained, provide the data subject with the following further information necessary to ensure fair and transparent processing:
(a) the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;
(b) the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability;
(c) where the processing is based on point (a) of Article 6(1) or point (a) of Article 9(2), the existence of the right to

See Articles 15 and 16 of the Federal Law in section 6.1. above.

Informed prior to/ at collection (cont'd)

withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;
(d) the right to lodge a complaint with a supervisory authority;
(e) whether the provision of personal data is a statutory or contrFederal Law/ Regulationsual requirement, or a requirement necessary to enter into a contrFederal Law/ Regulations, 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.

What information is to be provided

See Article 13(1) and (2) above

See Articles 15 and 16 of the Federal Law in section 6.1. above.

When data is from third party

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

Article 18 of the Federal Law: Where data has not been obtained directly from the data subject, the data controller must notify them of the change in the privacy notice. The provisions of the preceding paragraph are not applicable where processing is done for historical, statistical, or scientific purposes. Where it is impossible to provide the privacy notice to the data subject or where disproportionate effort is involved considering the number of data subjects, or the age of the data, with the authorisation of the INAI, the data controller may implement compensatory measures in the terms of the Regulations for the Federal Law.

Intelligibility requirements

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

Article 17 of the Federal Law: The privacy notice must be made available to data subjects through print, digital, visual, or audio formats or any other technology, as follows:

(I) where personal data has been obtained personally from the data subject, the privacy notice must be provided at the time the data is collected, clearly and unequivocally, through the format by which collection is carried out, unless the notice has been provided prior; and

GDPR	Federal Law/ Regulations

Intelligibility requirements

GDPR	Federal Law/ Regulations
the information may be provided orally, provided that the identity of the data subject is proven by other means.	(II) where personal data are obtained directly from the data subject by any electronic, optical, audio, or visual means, or through any other technology, the data controller must immediately provide the data subject with at least the information referred to in Article 16(I) and (II) of the Federal Law, as well as provide the mechanisms for the data subject to obtain the full text of the privacy notice.

Format

GDPR	Federal Law/ Regulations
See Article 12(1) above.	See Article 17 of the Federal Law above.

Exceptions

GDPR	Federal Law/ Regulations
The requirements of Article 13 do not apply where the data subject already has the information. The requirements of Article 14 do not apply where: (a) the data subject already has the information; (b) the provision of such information proves impossible or would involve a disproportionate effort, in particular for processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to the conditions and safeguards referred to in Article 89(1) or in so far as the obligation referred to in paragraph 1 of this Article is likely to render impossible or seriously impair the achievement of the objectives of that processing. In such cases the controller shall take appropriate measures to protect the data subject's rights and freedoms and legitimate interests, including making the information publicly available; (c) obtaining or disclosure is expressly laid down by Union or Member State law to which the controller is subject and which provides appropriate measures to protect the data subject's legitimate interests; or (d) where the personal data must remain confidential subject to an obligation of professional secrecy regulated by Union or Member State law, including a statutory obligation of secrecy.	The Federal Law and the Regulations do not include exceptions on the right to inform. INAI has issued guidance on exceptions in its Guidelines on Privacy Notices (only available in Spanish here).

5.3. Right to object

Fairly consistent

Both the GDPR and the Federal Law provide that data subjects may object to processing on certain, legitimate grounds; however, the laws are not entirely aligned on what these grounds are.

GDPR	Federal Law/ Regulations

Grounds for right to object/ opt out

GDPR	Federal Law/ Regulations
Article 21(1): The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her which is based on point (e) or (f) of Article 6(1), including profiling based on those provisions. The controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.	Article 27 of the Federal Law: Data subjects will, at all times and for any legitimate reason, have the right to object to the processing of their data. Where appropriate, the data controller may not process such data subject's data. Article 109 of the Regulations: Pursuant to Article 27 of the Federal Law, the data subject may, at any time, object to the processing of their personal data or require it to stop when: (I) there is a legitimate reason for doing so and their specific situation so requires, in which case, they must justify the fact that, even though the processing is lawful, it must stop in order to avoid its continuation causing prejudice to the data subject; or (II) the data subject needs to state their objection to the processing of their data in order to avoid processing for specific purposes. The exercise of the right to object may not be exercised in those cases where the processing is necessary to comply with a legal obligation imposed on the data controller.

Withdraw consent

GDPR	Federal Law/ Regulations
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 8 of the Federal Law: Consent may be revoked at any time without retroactive effects being attributed thereto. For revocation of consent, the data controller must, in the privacy notice, establish the mechanisms and procedures for such action.

Restrict processing

GDPR	Federal Law/ Regulations
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;	Article 23 of the Regulations: At any time, the data subject may revoke their consent for the processing of their personal data and the data controller shall establish simple and free-of-charge mechanisms to permit the data subject to revoke their consent using at least the same media that they used to provide it, provided that the law does not prevent this. The mechanisms or procedure established by the data controller to deal with consent revocation requests may not exceed the period contemplated in Article 32 of the Federal Law.

GDPR	Federal Law/ Regulations

Restrict processing

Article 18(1): The data subject shall have the right to obtain from the controller restriction of processing where one of the following applies: (a) the accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy of the personal data; (b) the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead;	When the data subject requests confirmation that the processing of their personal data has stopped, the data controller shall expressly respond to such request. If the personal data has been transmitted prior to the date of the revocation of consent and continues to be processed by the data processor, the data controller shall bring the revocation to the attention of the data processor so that the processor takes the necessary steps to deal with the request.

Object to direct marketing

Article 21(3): Where the data subject objects to processing for direct marketing purposes, the personal data shall no longer be processed for such purposes.	Article 16(II) of the Federal Law: The privacy notice must contain, among other things, the purposes of the data processing. Article 30 of the Regulations: Among the purposes of processing referred to in Article 16(II) of the Federal Law, as applicable, there must be included those concerning processing for marketing, advertising, or commercial exploration. The above is without prejudice to current law which regulates the processing for the purposes set out in Article 29(II) of the Regulations when this contemplates higher protection for the data subject than that provided in the Federal Law and the Regulations.

Inform data subject of right

See Article 12(1) in section 5.1. above. In addition, Article 21(4) provides: At the latest at the time of the first communication with the data subject, the right referred to in paragraphs 1 and 2 shall be explicitly brought to the attention of the data subject and shall be presented clearly and separately from any other information.	See Articles 15 and 16 of the Federal Law in section 6.1. above.

Fees

See Article 12(5) in section 5.1. above.	See Article 35 of the Federal Law in section 6.1. above.

GDPR	Federal Law/ Regulations

Response timeframe

See Article 12(3) in section 6.1. above.	See Article 32 of the Federal Law in section 6.1. above.

Format of response

See Article 12(1) in section 5.1. above.	Neither the Federal Law nor the Regulations explicitly refer to the format of the response to a right to object. [Note: Article 29 of the Federal Law details requirements for the data subject's request to exercise rights.]

Exceptions

See Article 12(5) in section 5.1. above.	See Article 34 of the Federal Law in section 6.1. above.

5.4. Right of access

Both the GDPR and the Federal Law establish a right of access and outline information that must be provided. However, the GDPR provides significantly more detail in terms of information to be accessed.

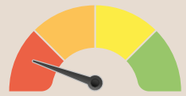
GDPR	Federal Law/ Regulations
Grounds for right of access	
Article 15(1): The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed.	Article 23 of the Federal Law: Data subjects will have the right to access their personal data held by the data controller as well as to be informed of the privacy notice to which processing is subject. Article 101 of the Regulations: Pursuant to Article 23 of the Law, the data subject has the right to obtain their personal data from the data controller, as well as information regarding the conditions and general features of the processing.
Information to be accessed	
Article 15(1): The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information: (a) the purposes of the processing; (b) the categories of personal data concerned; (c) the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations; (d) where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period; (e) the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing; (f) the right to lodge a complaint with a supervisory authority; (g) where the personal data are not collected from the data subject, any available information as to their source; and (h) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.	See Article 16 in section 6.1. above.
Inform data subject of right	
See Article 12(1) in section 5.1.	See Articles 15 and 16 of the Federal Law in section 6.1. above.
Fees	
See Article 12(5) in section 5.1. above.	See Article 35 of the Federal Law in section 6.1. above.
Verify data subject request	
Recital 64: The controller should use all reasonable measures to verify the identity of a data subject who requests access, in particular in the context of online services and online identifiers. A controller should not retain personal data for the sole purpose of being able to reFederal Law/ Regulations to potential requests.	Article 94 of the Regulations: For the purposes of Article 29(I) of the Federal Law, the request for access must show an address or some other means for notification of the response to the request. If this requirement is not complied with, the data controller shall deem the request not presented, and note this for the record.
Response timeframe	
See Article 12(3) in section 5.1. above.	See Article 32 of the Federal Law in section 6.1. above.
Format of response	
See Article 12(1) in section 5.1. above.	Article 102 of the Regulations: The obligation to give access will be considered as complied with when the data controller makes available to the data subject personal data on-site, respecting the period set out in Article 99 of the Regulations, or by issuing photocopies or using magnetic, optical, sound, visual, or holographic media, as well as other information technologies contemplated in the privacy notice. In all cases, access must be granted in formats that are readable and comprehensive to the data subject. When the data controller considers it appropriate, it may agree with the data subject upon reproduction media for the information different from that mentioned in the privacy notice.
Exceptions	
See Article 12(5) in section 5.1. above.	See Articles 26 and 34 of the Federal Law in section 6.1. above.

5.5. Right not to be subject to discrimination

Unlike the GDPR, neither the Federal Law nor the Regulations contain provisions on a right to not be subject to discrimination nor do they imply such a right.

GDPR	Federal Law/ Regulations
Definition of right	
The GDPR only implies this right and does not provide an explicit definition for it.	Neither the Federal Law nor the Regulations provide for a right not to be subject to discrimination.
Automated processing	
Article 22(1): The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her. [Article 22 goes on to detail this right, including exceptions]	Neither the Federal Law nor the Regulations provide for a right not to be subject to decisions based solely on automated processing.

5.6. Right to data portability



Unlike the GDPR, neither the Federal Law nor the Regulations establish a right to data portability.

GDPR	Federal Law/ Regulations
Grounds for portability	
Article 20(1): The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, where: (a) the processing is based on consent pursuant to point (a) of Article 6(1) or point (a) of Article 9(2) or on a contrFederal Law/ Regulations pursuant to point (b) of Article 6(1); and (b) the processing is carried out by automated means.	Neither the Federal Law nor the Regulations provide for a right to data portability.
Inform data subject of right	
See Article 12(1) in section 5.1.	Neither the Federal Law nor the Regulations provide for a right to data portability.
Fees	
See Article 12(5) in section 5.1. above.	Neither the Federal Law nor the Regulations provide for a right to data portability.
Response timeframe	
See Article 12(3) in section 5.1. above.	The Federal Law/ Regulations does not provide for a right to data portability.
Format	
See Article 20(1) above.	Neither the Federal Law nor the Regulations provide for a right to data portability.
Controller to controller	
Article 20(2): In exercising his or her right to data portability pursuant to paragraph 1, the data subject shall have the right to have the personal data transmitted directly from one controller to another, where technically feasible.	Neither the Federal Law nor the Regulations provide for a right to data portability.

GDPR	Federal Law/ Regulations
Technically feasible	
See Article 20(2) above.	Neither the Federal Law nor the Regulations provide for a right to data portability.
Exceptions	
See Article 12(5) in section 5.1. above.	Neither the Federal Law nor the Regulations provide for a right to data portability.

6. Enforcement

Fairly consistent

6.1. Monetary penalties

Both the GDPR and the Federal Law provide that data protection authorities can issue monetary penalties, however, the potential sanctions under the Federal Law are significantly smaller. Additionally, the Federal Law imposes penalties of imprisonment.

GDPR	Federal Law/ Regulations
Provides for monetary penalties	
The GDPR provides for monetary penalties.	The Federal Law provides for monetary penalties and the possibility of imprisonment.
Issued by	
Article 58(2) Each supervisory authority shall have all of the following corrective powers: [...] (i): to impose an administrative fine pursuant to Article 83, in addition to, or instead of measures referred to in this paragraph, depending on the circumstances of each individual case.	Article 38 of the Federal Law: The INAI, for the purposes of the Federal Law, will have the purpose of disseminating information on the right to personal data protection in Mexico, promoting its exercise, and overseeing the due observance of the provisions of the Federal Law and those arising therefrom; particularly those related to the fulfilment of obligations by the parties regulated by the Federal Law.
Fine maximum	
Article 83(5): infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher: (a) the basic principles for processing, including conditions for consent, pursuant to Articles 5, 6, 7 and 9; (b) the data subjects' rights pursuant to Articles 12 to 22; (c) the transfers of personal data to a recipient in a third country or an international organisation pursuant to Articles 44 to 49; (d) any obligations pursuant to Member State law adopted under Chapter IX; (e) non-compliance with an order or a temporary or definitive limitation on processing or the suspension of data flows by the supervisory authority pursuant to Article 58(2) or failure to provide access in violation of Article 58(1). (6) Non-compliance with an order by the supervisory authority as referred to in Article 58(2) shall, in accordance with paragraph 2 of this Article, be subject to administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher.	Article 64 of the Federal Law: Violations of this Law will be punished by the INAI as follows: (I) a warning instructing the data controller to carry out the actions requested by the data subject, under the terms established by the Federal Law, in the cases described in Article 63(1) of the Federal Law; (II) a fine from 100 to 160,000 days of the Mexico City minimum wage (approx. €355 to €568,000), in the cases described in Article 63(II) to (VII) of the Federal Law; (III) a fine from 200 to 320,000 days of the Mexico City minimum wage (approx. €710 to €1,136,000), in the cases described in Article 63(VIII) to (XVIII); and (IV) in the event of repeated occurrences of the violations described in the preceding paragraphs, an additional fine will be imposed from 100 to 320,000 days of the current Mexico City minimum wage (approx. €355 to €1,136,000). With regard to violations committed in processing sensitive data, sanctions may be increased up to double the established amounts.

GDPR	Federal Law/ Regulations

Percentage of turnover

Under Article 83(4), (5), and (6), fines may be issued that equate to 2% or 4% of the total worldwide annual turnover of the preceding financial year.	Neither the Federal Law nor the Regulations provide for sanctions that equate to a percentage of turnover.

Mitigating factors

Article 83(2): When deciding whether to impose an administrative fine and deciding on the amount of the administrative fine in each individual case due regard shall be given to the following: (a) the nature, gravity and duration of the infringement taking into account the nature scope or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them; (b) the intentional or negligent charFederal Law/ Regulationser of the infringement; (c) any Federal Law/ Regulationsion taken by the controller or processor to mitigate the damage suffered by data subjects; (d) the degree of responsibility of the controller or processor taking into account technical and organisational measures implemented by them pursuant to Articles 25 and 32; (e) any relevant previous infringements by the controller or processor; (f) the degree of cooperation with the supervisory authority, in order to remedy the infringement and mitigate the possible adverse effects of the infringement; (g) the categories of personal data affected by the infringement; (h) the manner in which the infringement became known to the supervisory authority, in particular whether, and if so to what extent, the controller or processor notified the infringement; (i) where measures referred to in Article 58(2) have previously been ordered against the controller or processor concerned with regard to the same subject-matter, compliance with those measures; (j) adherence to approved codes of conduct pursuant to Article 40 or approved certification mechanisms pursuant to Article 42; and (k) any other aggravating or mitigating fFederal Law/ Regulationsor applicable to the circumstances of the case, such as financial benefits gained, or losses avoided, directly or indirectly, from the infringement.	Article 65 of the Federal Law: The INAI will ground its decisions in law and fact, considering: (I) the nature of the data; (II) the evident impropriety of the refusal of the data controller to perform the actions requested by the data subject in the terms of the Federal Law; (III) the intentional or unintentional nature of the action or omission constituting the violation; (IV) the financial position of the data controller, and (V) recurrence of the violation.

GDPR	Federal Law/ Regulations

Imprisonment

Not applicable.	Article 67 of the Federal Law: Three months to three years imprisonment will be imposed on any person who, authorised to process personal data, for profit, causes a security breach affecting the databases under their custody. Article 68 of the Federal Law: Six months to five years imprisonment will be imposed on any person who, with the aim of achieving unlawful profit, processes personal data deceitfully, taking advantage of an error of the data subject or the person authorised to transmit such data. Article 69 of the Federal Law: With regard to sensitive personal data, the penalties referred to in Chapter XI will be doubled.

DPO liability

Not applicable.	Not applicable

6.2. Supervisory authority

Fairly consistent

The role of INAI under the Federal Law is broadly similar to that of data protection authorities as envisioned by the GDPR. Both have advisory, investigatory, and corrective powers, although the details of these powers differ. In addition, the GDPR sets out the tasks and authority of the data protection authority in far more detail.

GDPR	Federal Law/ Regulations
Provides for data protection authority	
Article 51(1): Each Member State shall provide for one or more independent public authorities to be responsible for monitoring the application of this Regulation, in order to protect the fundamental rights and freedoms of natural persons in relation to processing and to facilitate the free flow of personal data within the Union ('supervisory authority').	See section 7.1. above.
Investigatory powers	
Article 58(1): Each supervisory authority shall have all of the following investigative powers: (a) to order the controller and the processor, and, where applicable, the controller's or the processor's representative to provide any information it requires for the performance of its tasks; (b) to carry out investigations in the form of data protection audits; (c) to carry out a review on certifications issued pursuant to Article 42(7); (d) to notify the controller or the processor of an alleged infringement of this Regulation; (e) to obtain, from the controller and the processor, access to all personal data and to all information necessary for the performance of its tasks; (f) to obtain access to any premises of the controller and the processor, including to any data processing equipment and means, in accordance with Union or Member State procedural law.	Article 39 of the Federal Law: The INAI has the following responsibilities: (I) to oversee and verify compliance with the provisions of the Federal Law, within the scope of its competence, with the exceptions provided by the law; and (II) to interpret the Federal Law in the administrative system. [...]

GDPR	Federal Law/ Regulations
Corrective powers	
Article 58(2): Each supervisory authority shall have all of the following corrective powers: (a) to issue warnings to a controller or processor that intended processing operations are likely to infringe provisions of this Regulation; (b) to issue reprimands to a controller or a processor where processing operations have infringed provisions of this Regulation; (c) to order the controller or the processor to comply with the data subject's requests to exercise his or her rights pursuant to this Regulation; (d) to order the controller or processor to bring processing operations into compliance with the provisions of this Regulation, where appropriate, in a specified manner and within a specified period; (e) to order the controller to communicate a personal data breach to the data subject; (f) to impose a temporary or definitive limitation including a ban on processing; (g) to order the rectification or erasure of personal data or restriction of processing pursuant to Articles 16, 17 and 18 and the notification of such Federal Law/ Regulationsions 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 39 of the Federal Law: The INAI has the following responsibilities: [...] (VI) hear and issue decisions in rights protection and verification procedures as set forth in the Federal Law, and impose penalties as appropriate.

GDPR	Federal Law/ Regulations

Authorisation/ advisory powers

GDPR	Federal Law/ Regulations
Article 58(3): Each supervisory authority shall have all of the following authorisation and advisory powers: (a) to advise the controller in accordance with the prior consultation procedure referred to in Article 36; (b) to issue, on its own initiative or on request, opinions to the national parliament, the Member State government or, in accordance with Member State law, to other institutions and bodies as well as to the public on any issue related to the protection of personal data; (c) to authorise processing referred to in Article 36(5), if the law of the Member State requires such prior authorisation; (d) to issue an opinion and approve draft codes of conduct pursuant to Article 40(5); (e) to accredit certification bodies pursuant to Article 43; (f) to issue certifications and approve criteria of certification in accordance with Article 42(5); (g) to adopt standard data protection clauses referred to in Article 28(8) and in point (d) of Article 46(2); (h) to authorise contrFederal Law/ Regulationsual 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 39 of the Federal Law: The INAI has the following responsibilities: [...] (III) to provide technical support to the data controllers who so request for fulfilment of the obligations established by the Federal Law; (IV) to issue opinions and recommendations in accordance with the applicable provisions of the Federal Law, for purposes of its functions and operation; (V) to disseminate international best practices and standards for information security, in view of the nature of the data, the processing purposes, and the technical and financial capacity of the data controller; and (VI) hear and issue decisions in rights protection and verification procedures as set forth in the Federal Law, and impose penalties as appropriate.

Tasks of authority

GDPR	Federal Law/ Regulations
Article 57(1): Without prejudice to other tasks set out under this Regulation, each supervisory authority shall on its territory: (a) monitor and enforce the application of this Regulation; (b) promote public awareness and understanding of the risks, rules, safeguards and rights in relation to processing. Federal Law/ Regulationsivities addressed specifically to children shall receive specific attention; (c) advise, in accordance with Member State law, the national parliament, the government, and other institutions and bodies on legislative and administrative measures relating to the protection of natural persons' rights and freedoms with regard to processing; (d) promote the awareness of controllers and processors of their obligations under this Regulation;	Article 39 of the Federal Law: The INAI has the following responsibilities: [...] (VII) cooperate with other domestic and international bodies and supervisory authorities, in order to assist in the area of data protection; [...] (X) carry out studies of the impact on privacy prior to the implementation of new types of processing of personal data or material modification of existing types of processing; (XI) develop, promote, and disseminate analyses, studies, and research in the area of protection of personal data held by third parties and provide training to the obligated parties, and (XII) any other responsibilities under the Federal Law and other applicable laws. In addition, see the other provisions of Article 39 of the Federal Law above.

GDPR	Federal Law/ Regulations

Tasks of authority

GDPR	Federal Law/ Regulations
(e) upon request, provide information to any data subject concerning the exercise of their rights under this Regulation and, if appropriate, cooperate with the supervisory authorities in other Member States to that end; (f) handle complaints lodged by a data subject, or by a body, organisation or association in accordance with Article 80, and investigate, to the extent appropriate, the subject matter of the complaint and inform the complainant of the progress and the outcome of the investigation within a reasonable period, in particular if further investigation or coordination with another supervisory authority is necessary; (g) cooperate with, including sharing information and provide mutual assistance to, other supervisory authorities with a view to ensuring the consistency of application and enforcement of this Regulation; (h) conduct investigations on the application of this Regulation, including on the basis of information received from another supervisory authority or other public authority; (i) monitor relevant developments, insofar as they have an impFederal Law/ Regulations on the protection of personal data, in particular the development of information and communication technologies and commercial prFederal Law/ Regulationsices; (j) adopt standard contrFederal Law/ Regulationsual 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 impFederal Law/ Regulations 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;	

GDPR	Federal Law/ Regulations

Tasks of authority (cont'd)

(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 contrFederal Law/ Regulationsual clauses and provisions referred to in Article 46(3);
(s) approve binding corporate rules pursuant to Article 47;
(t) contribute to the Federal Law/ Regulationsivities of the Board;
(u) keep internal records of infringements of this Regulation and of measures taken in accordance with Article 58(2); and
(v) fulfil any other tasks related to the protection of personal data.

Annual report

Article 59: Each supervisory authority shall draw up an annual report on its Federal Law/ Regulationsivities, 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 39 of the Federal Law: The INAI has the following responsibilities: [...] (VIII) submit an annual activity report to the Mexican Congress.

6.3. Civil remedies for individuals

Fairly inconsistent

The GDPR provides for a much more extensive procedure for civil remedies for individuals compared to the Federal Law. While both the GDPR and the Federal Law enable data subjects to seek civil remedies for material, or patrimonial, and non-material, or non-patrimonial, damages, there are notable differences in processes.

GDPR	Federal Law/ Regulations

Provides for claims/ cause of Federal Law/ Regulationsion

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.

Neither the Federal Law nor the Regulations provide for private cause of actions.
.

Material and non-material damage

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

Article 58 of the Federal Law: Data subjects who feel they have suffered harm or damage to their property or rights as a result of a breach of the provisions of the Federal Law by the data controller or data processor, may exercise the rights they deem appropriate for purposes of any applicable indemnity, in the terms of the relevant law.

Mandate for representation

Article 80(1): The data subject shall have the right to mandate a not-for-profit body, organisation or association which has been properly constituted in accordance with the law of a Member State, has statutory objectives which are in the public interest, and is Federal Law/ Regulationsive 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.

Not applicable.

Specifies amount for damages

Not applicable.

Not applicable.

GDPR	Federal Law/ Regulations
Processor liability	
Article 82(2): Any controller involved in processing shall be liable for the damage caused by processing which infringes this Regulation. A processor shall be liable for the damage caused by processing only where it has not complied with obligations of this Regulation specifically directed to processors or where it has Federal Law/ Regulationsed outside or contrary to lawful instructions of the controller.	Not applicable.
Exceptions	
Article 82(3): A controller or processor shall be exempt from liability under paragraph 2 if it proves that it is not in any way responsible for the event giving rise to the damage.	Not applicable.