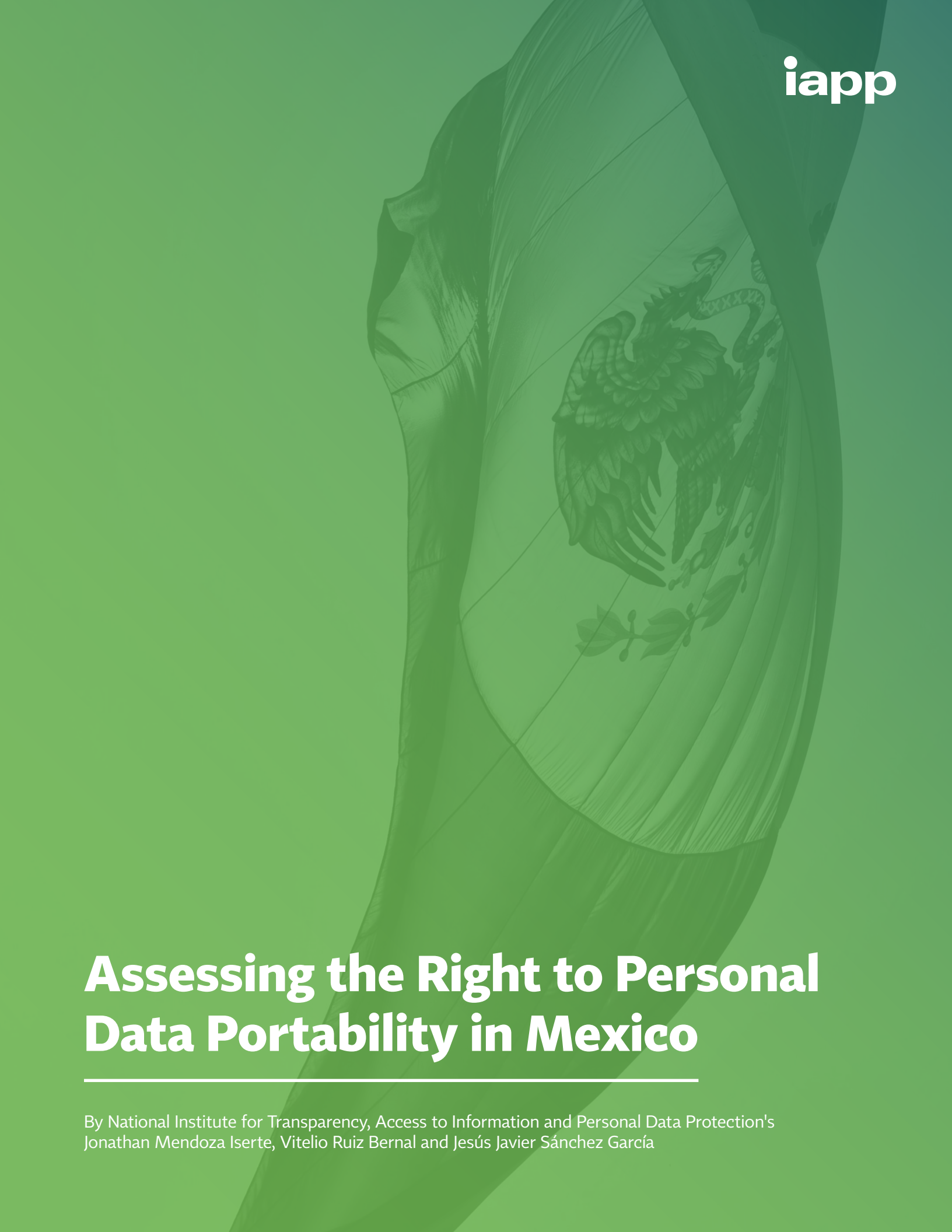

Assessing the Right to Personal Data Portability in Mexico

By National Institute for Transparency, Access to Information and Personal Data Protection's Jonathan Mendoza Iserte, Vitelio Ruiz Bernal and Jesús Javier Sánchez García

Assessing the Right to Personal Data Portability in Mexico

By National Institute for Transparency, Access to Information and Personal Data Protection's Jonathan Mendoza Iserte, Vitelio Ruiz Bernal and Jesús Javier Sánchez García

The right to personal data portability arises as a new complementary modality to the right of access to personal data that had its origin in the EU General Data Protection Regulation. Mexico, by enacting the personal data protection regulations in the public sector in January 2017, adopted this figure, creating an asymmetry among the personal data protection regulations held by private parties. This research outlines in a simple way what the right to portability is, the similarities and differences between European and Mexican law regarding portability, and makes a brief analysis of the recent reform proposals to incorporate this right into Mexican regulations for personal data protection held by private parties.

I. Background

The right to portability arises as a complementary modality to the right of access to personal data, although they are independent of each other, and became more relevant with the EU General Data Protection Regulation. This regulatory framework has become an international reference, considering seven rights, instead of four (access, correction, cancellation and opposition), as in our country, among them, the aforementioned right to personal data portability.

Although the GDPR does not define what portability is, the Article 29 Working Party (now European Data Protection Board)[1] defines it as the right that "allows for data subjects to

[1] This Working Group was created from Article 29 of Directive 95/46/EC. The article established the creation of a group for the protection of individuals with regard to the processing of their personal data. This group had an independent and consultative character. The group was composed of a representative of the supervisory authorities of each member state of the European Union and a representative of the European Commission. The group's mission was, among others: the application of the aforementioned directive within national legislations; issue a verdict on the adequate level of data protection within the EU and third countries; draw up opinions and recommendations on any matter related with the protection of individuals regarding the processing of their personal data.

Since the application of the GDPR (May 25, 2018), the WP29 was replaced by the European Data Protection Board, which has similar but broader functions conferred by the GDPR, some of them include: provide guidance (including guidelines, recommendations and good practices) to clarify the GDPR; advise the European Commission on any aspect related to the protection of personal data and the new legislation proposed in the European Union; adopt consistent results in cross-

receive personal data that were provided to a controller, in a structured, commonly used and machine-readable format, and to transmit those data to another data controller without impediments."[2]

The WP29 stated that individuals making use of the right of access to their personal data, under the repealed Data Protection Directive 95/46/EC,[3] were constrained by the format chosen by the data controller when providing the requested information. In this sense, they considered that the new right to data portability aims to empower data subjects regarding their personal data, as it facilitates their ability to move, copy or transmit personal data easily into an IT environment.[4]

Mexico is no stranger to this new regulatory scope. It was one of the first countries to adapt the right to data portability provided in the GDPR by incorporating it in the General Law on Protection of Personal Data held by Obligated Parties, which regulates government or public sector.[5] However, the above-mentioned generated an asymmetry since the Mexican legislation has not yet reformed the personal data regulations applicable to private parties.

In the Ibero-American region, the adoption of legislation that consider the right to data portability is a reality. Between 2016 and 2017, countries such as Argentina, Brazil and Chile, incorporated the innovations from the GDPR in their respective legislation, specifically regarding the right to data portability. For example, in Argentina, the preliminary draft reform to Law 25,326 of 2000, Article 33, provides for the right to data portability. Brazil recently approved its law No. 13,853 in July 2019, through which Law 13,709 of August 2018 was modified. Within these modifications, two mentions are made regarding the right to data portability, first, in Article 4, Section I and, second, in Articles 18, Section V, and 19 Numerals 3 and 4, in which it makes a reshipment to secondary legislation of the national authority, similar to Mexico and establishes the procedure for personal data portability.[6] Finally, in Chile, Article 9 of the preliminary draft bill presented in 2017 establishes the right to data portability and indicates the procedure to exercise this right.[7]

We must remember that this right is of European origin and is binding only for the private sector. The inclusion and effective implementation in the public sector is a problem with technical and economic edges that currently

---

border data protection cases; promote cooperation and the effective exchange of information and good practices among national authorities; draw up an annual activity report, which is published and sent to Parliament, the Council and the Commission.

[2] WP29 Guidelines on the right to data portability, Brussels, p. 4. Available for online consultation.

[3] Directive 95/46/EC was adopted by the Parliament and the Council of Europe on Oct. 24, 1995, on the protection of individuals to the processing of personal data and the free movement of such data. The adoption of this instrument occurred to specify and expand the general conditions established in Convention 108 of the Council of Europe regarding the automated processing of personal data.

With the entry into force of the GDPR, this directive was repealed to advance with this new regulatory framework, which will regulate the processing of personal data. Available for online consultation.

[4] Ibid.

[5] Secondary legislation, issued in compliance with the transitional regime of the reform of Feb. 7, 2014, to the sixth constitutional article. Entry into force Jan. 27, 2017.

[6] Puccinelli, Oscar Raúl, El derecho a la portabilidad de los datos personales. Orígenes, sentido y alcances, Revista Pensamiento Constitucional, N° 22, 2017, pp. 203–228 available only in Spanish.

[7] Draft bill, initiated in a message from S. E. the President of the Republic, which regulates the protection and treatment of personal data and creates the Personal Data Protection Agency. Available for consultation only in Spanish.

creates a big challenge for governments. Of course, that it is not enough to regulate new rights, it is necessary to protect them effectively and guarantee them.

In this regard, it is specified that there are currently some reform initiatives in both chambers comprising the Mexican Congress concerning the Federal Law on Protection of Personal Data Held by Private Parties,[8] one of them specifically related to the incorporation of the right to data portability in the private sector.

> *Decree reform initiative that adds Article 35 BIS to the Federal Law on Protection of Personal Data Held by Private Parties, regarding Portability.*[9]
>
> - *Author: Senador Ricardo Monreal Ávila del Grupo Parlamentario de Morena.*
> - *Date: Feb. 13, 2020.*
> - *Chamber or origin: Senate of the Republic.*
> - *Available online only in Spanish.*

II. Concept and elements of the right to portability

From a systemic interpretation of the different national and international regulatory bodies, we can define the right to portability as the right of a data subject to receive their personal data provided to a data controller in a structured and commonly used format of which they may have a copy to continue using or transfer them to another data controller without being limited by the data controller that would have provided them.

According to the WP29, portability is made up of the following elements:[10]

A. Right to receive personal data that concerns an individual and were processed by the controller and stored for later use. In this sense, portability plays as a complement to the right of access since the owner can manage the data that is in a structured, commonly used and machine-readable format in its own way.[11]

[8] Reform Initiatives regarding the LFPDPPP:

DATE	HOUSE OF ORIGIN	AUTHOR	LINK (SPA)
May 12, 2019	Senate	Sen. Ricardo Monreal Ávila of the Parliamentary Group of Morena.	https://bit.ly/2KQ9Cva
Jan. 28, 2020	Deputies	Deputy Mario Martín Delgado Carrillo, of the Parliamentary Group of Morena.	https://bit.ly/34LoMLe
Feb. 11, 2020	Senate	Sen. Ricardo Monreal Ávila of the Parliamentary Group of Morena.	https://bit.ly/3aikbBt
Feb. 17, 2020	Senate	Sen. Miguel Ángel Mancera Espinosa, of the Party of the Democratic Revolution.	https://bit.ly/2yos773
Feb. 18, 2020	Senate	Sen. Juan Manuel Fócil Pérez, of the Parliamentary Group of the Democratic Revolution.	https://bit.ly/2VF9hjQ
Feb. 18, 2020	Deputies	Deputy Jorge Arturo Espadas Galván and members of the PAN Parliamentary Group.	https://bit.ly/2RHkFL1

[9] Turned to the Commission of Anticorruption, Transparency, and Citizen Participation and that is pending judgment.

[10] Op. Cit. p. 5.

[11] When referring to structured, commonly used and machine-readable format, we are referring to attributes or technical characteristics that the format or file or device in which the information is delivered or transmitted must have. In this sense, we can say that a mechanical reading refers to the fact that the file must be in a structured format that allows computer applications to easily identify, recognize and extract specific data, including factual statements and their internal

B. Right to transmit from one controller to another, which provides the possibility to reuse the data directly by another controller at the request of the owner of the data.[12]

Aside from these two elements, being a novel right, each regulatory body, jurisdiction and, when appropriate, data protection authority or control authority, may interpret portability differently so that the particularities and various manifestations of this right are yet to be defined.

III. Regulation of the right to portability

a. Portability in Regulation (EU) 2016/679 of the European Parliament and of the Council.[13]

The GDPR establishes in Article 20 the right to data portability, as follows:

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

   (a) the processing is based on consent pursuant to point (a) of Article 6(1) or point (a) of Article 9(2) or on a contract pursuant to point (b) of Article 6(1); and

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

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.*

3. *The exercise of the right referred to in paragraph 1 of this Article shall be without prejudice to Article 17. That right shall not apply to processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. The right referred to in*

structure. Similarly, structured means that the machine or its user can identify, recognize and extract the information, which, in other words, means that the information is ordered or cataloged in containers that allow it to be identified and searched for. Common use means that data controllers must provide personal data using commonly used open formats (e.g., XML, JSON, CSV), along with useful metadata with the best possible level of granularity while maintaining a high degree of abstraction. Thus, appropriate metadata must be used to accurately describe the meaning of the information exchanged. Such metadata must be sufficient to make it possible to work with the data and reuse it through the use of accessible and easy-to-read formats regardless of the computer equipment and without the need for the use and utilization of tools or licenses that imply a cost for the data subject (guidelines on the right to data portability).

[12] The importance consists in the data subject's right to transmit or receive their personal data and should not oblige the data controller to adopt or maintain treatment systems that are technically compatible. Portability aims to produce interoperable systems, not compatible systems (considering Article 68 of the GDPR). Therefore, those responsible must try to design mechanisms for common use that allow them to directly and securely transmit this data in the formats that we already mentioned or to have a download tool that allows the owner of the personal data or the other controller access and download all or part of a set of personal data, without the above implying an overload on the person responsible (guidelines on the right to data portability).

[13] Regulation (EU) 2016/679 of the European Parliament and of the Council, Official Journal of the European Union, May 4, 2016, available here.

paragraph 1 shall not adversely affect the rights and freedoms of others."[14]

From this normative article, we can deduce the two elements mentioned in Section II of this analysis: the right to access personal data by the data subject or the interested party and the transmission of data between the controllers. In the same sense, it mentions some conditions for this modality of the right of access to operate and they are: processing is based on consent; or processing is based on a contract.

In addition, the processing was carried out by automated means,[15] the right cannot contravene the right to suppression or to the processing of personal data that is necessary for the public interest or in the exercise of powers.

These conditioning factors or limitations do not seem like many, although there are an endless number of situations that require a more detailed study for a more adequate application of this right.[16]

b. Portability in the General Law on Protection of Personal Data held by Obligated Parties

Mexico, at the dawn of an initiative to enact regulations for the protection of personal data in the public sector, seems to have considered the adoption of the GDPR. Adopting this new modality of the right of access, due to its novelty, the legislation seeking not to overload the regulatory body, instead empowered the guarantor bodies so that, through the National System of Transparency and Personal Data Protection, they will regulate their peculiarities. In this sense, we find this right regulated in the following way:

> *"...*
> *Chapter III*
> *Data Portability*
>
> *Article 57. Where personal data are processed via electronic means in a commonly used structured format, the data owner will be entitled to obtain from the data controller a copy of the processed data in a commonly used structured electronic format allowing him/her their continuous use.*
>
> *Where the data owner has provided personal data and processing is based on consent or contract, he/she will be entitled to transmit such personal data and any other information he/she may have provided, which is kept in an automated processing system, to another system in a commonly used electronic format, no impediment being placed by the processing data controller that is being subjected to removal of the personal data.*
>
> *The National System will establish guidelines providing for the parameters to be taken into consideration to determine the hypotheses under*

[14] European Parliament and of the Council, Regulation (eu) 2016/679, May 4, 2016, Official Journal of the European Union, available here.
[15] What is the absence of human intervention in an action or operation of the processing by the controller.
[16] The WP29, prior to the entry into force of the General Regulation on the Protection of Personal Data (which also marks its transformation) issued the guidelines on the right to data portability in December 2016 available here.

> *which the presence of a commonly used structured format is presumed to be present, as well as for the technical standards, modalities and procedures for the transfer of personal data…"*[17]

From the analysis of the previous article, we can appreciate the clear influence of the GDPR, denoting that although it was a matter of making adaptations, some concepts or references were inherited, which even when they do not make this right inapplicable, they can lead you to different interpretations

In the same way, we can find the two basic elements of portability (receiving and transmitting from controller to another controller), as well as technical elements, such as providing personal data in structured and commonly used formats.

On the other hand, the National System of Transparency, Access to Information and Personal Data Protection complied with its legal mandate, and on Feb. 12, 2018, it published in the Official Gazette of the Federation the "Agreement that approve the Guidelines that establish the Parameters, Modalities and Procedures for the Personal Data Portability," in which the details for the implementation of this right are established, such as the deadlines and ways in which the compliance for the substantiation of requests thereof, as well as the legal means of defense that data subject has.

These guidelines take up or coincide in multiple concepts and interpretations with those made by the WP29 in its guidelines on data portability, among which we can find the following:[18]

GUIDELINES National System for Transparency, Access to Information and Personal Data Protection	**GUIDELINES** WP29
Objective Article 1. These guidelines are intended to establish the parameters to be considered to determine the cases in which you are in the presence of a structured and commonly used format that contains personal data, as well as the technical standards, modalities and procedures for transmission, to guarantee the personal data portability referred to in the General Law on Protection of Personal Data held by Obligated Parties.	**Objective** It aims at discussing the right to data portability and its scope. It clarifies the conditions under which this new right applies taking into account the legal basis of the data processing (either the data subject's consent or the necessity to perform a contract) and the fact that this right is limited to personal data provided by the data subject. The opinion also provides concrete examples and criteria to explain the circumstances in which this right applies.

[17] The General Law on Protection of Protection. Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, 26 de enero de 2017, Diario Oficial de la Federación, disponible aquí.
[18] Available online.

GUIDELINES National System for Transparency, Access to Information and Personal Data Protection	GUIDELINES WP29
Chapter II. Of the object and scope of the portability of personal data. **Criteria for determining a commonly used and structured format.** Article 6. For the purposes of these guidelines, it will be understood that a format acquires the quality of structured and commonly used, regardless of the computer system used for its generation and reproduction, when all the following assumptions are met: 1. It is an electronic format accessible and readable by automated means, so that they can identify, recognize, extract, exploit or carry out any other operation with specific personal data; 2. The format allows the reuse and/or use of personal data. 3. The format is interoperable with other computer systems, in accordance with the provisions of Article 2, Section I of these guidelines.	**I. How do the general rules governing the exercise of data subject rights apply to data portability?** **What is the expected data format?** The GDPR places requirements on data controllers to provide the personal data requested by the individual in a format, which supports reuse. Specifically, Article 20(1) of the GDPR states that the personal data must be provided "in a structured, commonly used and machine-readable format." The terms "structured," "commonly used" and "machine-readable" are a set of minimal requirements that should facilitate the interoperability of the data format provided by the data controller.
Chapter II. Of the object and scope of the personal data portability. **Purpose of portability.** Article 7. The purpose of the personal data portability is for the owner to request: 1. A copy of your personal data that you have provided directly to the controller, in a structured and commonly used format, that allows you to continue using them and, where appropriate, deliver them to another controller for reuse and use in a new treatment, without This is prevented by the controller to whom the owner has provided the personal data. 2. The transmission of your personal data to a controller receiver, if it is technically possible, the owner has directly provided your personal data.	**II. What are the main elements of data portability?** **A right to receive personal data** Firstly, data portability is a right of the data subject to receive a subset of the personal data processed by a data controller concerning them and to store those data for further personal use. Such storage can be on a private device or on a private cloud without necessarily transmitting the data to another data controller. **A right to transmit personal data from one data controller to another data controller** Secondly, Article 20(1) provides data subjects with the right to transmit personal data from one data controller to another data controller "without hindrance." Data can also be transmitted directly from one data controller to another on request of the data subject and where it is technically feasible (Article 20(2)). In this respect, Recital 68 encourages data controllers to develop interoperable formats that enable data portability but without creating an obligation for controllers to adopt or maintain processing systems which are technically compatible. The GDPR does, however, prohibit controllers from establishing barriers to the transmission.

GUIDELINES National System for Transparency, Access to Information and Personal Data Protection	GUIDELINES WP29
Chapter II. Purpose and scope of the portability of personal data. **Purpose of portability.** Article 8. Provenance of the portability of personal data. For the purposes of these guidelines, when the personal data are in a structured and commonly used format, the portability of the personal data will proceed if each of the following conditions are met: 1. The treatment is carried out by automated or electronic means in a structured and commonly used format referred to in Article 6 of these guidelines. 2. The personal data of the data subject is in the possession of the controller or its processor. 3. The personal data concerns the data object or individuals linked to a deceased who have a legal interest. 4. The data subject has provided the controller directly, in an active and conscious way, which includes the personal data obtained in the context it is use, the provision of a service or the completion of a procedure, or those provided by the data subject through a technological device. 5. The portability of personal data does not affect the rights and freedoms of third parties.	**III. When does data portability apply? Which processing operations are covered by the right to data portability?** Compliance with the GDPR requires data controllers to have a clear legal basis for the processing of personal data. **What personal data must be included?** Pursuant to Article 20(1), to be within the scope of the right to data portability, data must be: • Personal data concerning them. • Which they have provided to a data controller. With this right shall not adversely affect the rights and freedoms of others. First condition: Personal data concerning the data subject. Second condition: Data provided by the data subject. Third condition: The right to data portability shall not adversely affect the rights and freedoms of others.
Chapter III. Of the specific rules for the exercise of the portability of personal data. **General framework applicable to the exercise of personal data portability.** Article 14. For the exercise of the portability of personal data, the controller must observe the requirements, terms, conditions and procedures established in Title Three of Chapter II of the General Law or those that correspond to local state legislation on the matter and the provisions that may be applicable in the matter, as well as the provisions aforementioned in this chapter.	**IV. How do the general rules governing the exercise of data subject rights apply to data portability?** **What prior information should be provided to the data subject?** To comply with the new right to data portability, data controllers must inform data subjects of the existence of the new right to portability. Where the personal data concerned are directly collected from the data subject, this must happen "at the time where personal data are obtained." In addition, the WP29 recommends that data controllers always include information about the right to data portability before data subjects close any account they may have. This allows users to take stock of their personal data and easily transmit the data to their own device or another provider before a contract is terminated.

GUIDELINES National System for Transparency, Access to Information and Personal Data Protection	GUIDELINES WP29
Request for the portability of personal data Article 15. Without prejudice to provisions of Article 52 of the General Law or those that correspond to state legislation in the matter, in the request for portability of personal data, no greater requirements may be imposed than the following: 1. The request of a copy of your personal data in a structured and commonly used format, or to transmit your personal data to the controller receiver. 2. The general explanation of the emergency situation in which the data subject is, so that the response times on the proceeding or inadmissibility of his request and, and where appropriate, to make the portability of his personal data effective, in shorter terms, if applicable as established in the provisions of Articles 19 and 21 of these guidelines. 3. The business name of the controller receiver and the document that proves the legal relationship between the controller and the data subject; compliance with a legal provision or the right it intends to exercise, in the event that the data subject requests the transmission of his personal data referred to in Article 7, Section II of these guidelines. If the data subject requests from the controller a copy of their personal data in a structured format and commonly use.	**How can the data controller identify the data subject before answering his request?** There are no prescriptive requirements to be found in the GDPR on how to authenticate the data subject. Nevertheless, Article 12(2) of the GDPR states that the data controller shall not refuse to act on request of a data subject for exercising his or her rights, including the right to data portability, unless it is processing personal data for a purpose that does not require the identification of a data subject and it can demonstrate that it is not able to identify the data subject. **What is the time limit imposed to answer a portability request?** Article 12(3) requires that the data controller provides "information on action taken" to the data subject "without undue delay" and in any event "within one month of receipt of the request."

We are facing a new modality of the right of access to personal data and, as such, data subjects must exercise their right, which will necessarily generate criteria and knowledge for both the controller, and the authorities guaranteeing the right to data protection and even for the data subjects themselves.

There are pending questions that we understand are not part of the data susceptible to portability, which in the case of Mexican law finds a limit regarding the data inferred and/or created by the controller, the pseudonyms and the data subject to dissociation processes.

Finally, regarding EU law, it allows a broad interpretation regarding what data may be subject to portability, which means the data provided by the data subject must concern them and which they have provided to a data controller even when it tends to leave out the data created by the data controller or inferred from raw data provided by the data subjects or interested party or data obtained from other sources. The truth is that it allows data processing even from third parties but that concern the interested party (e.g., conversations in messaging applications) or that were provided by the data subject not necessarily

> ***We are facing a new modality of the right of access to personal data and, as such, data subjects must exercise their right, which will necessarily generate criteria and knowledge for both the controller, and the authorities guaranteeing the right to data protection and even for the data subjects themselves.***

consciously, but that it gives by the virtue of the use of a service (e.g., those that are delivered when searching for purchases that result in subsequent offers of related services).

c. Standards for Personal Data Protection for Ibero-American States

The Ibero-American Data Protection Network (RIPD, in Spanish), arises on the occasion of the agreement reached at the Ibero-American Data Protection Meeting held in La Antigua, Guatemala, in June 2003. It is currently made up of 12 data protection authorities from eight countries and more than 15 authorities of the matter are observers.[19]

The RIPD at the Ibero-American Meeting on the Protection of Personal Data, held in 2007 in Lisbon, approved the Guidelines for the Harmonization of Data Protection in the Ibero-American Community to establish guiding criteria for the development of legislative initiatives to be adopted in these countries and with the perspective of its usefulness as a frame of reference for other countries in other geographical areas.[20]

Following the trend and with the evolution of the work carried out by the RIPD at the meeting held in Colombia in 2016, the National Institute of Transparency, Access to Information and Protection of Personal Data was commissioned to write the Personal Data Protection Standards for the Ibero-American States, which were approved at the meeting held in 2017, in Santiago de Chile. Its objective was the homogenization of rules, principles, rights and duties, derived from the application of the criteria included therein; seeking that they are incorporated into the respective national laws and through which new levels of international cooperation can be achieved, facilitate cross-border data flows and ensure effective protection of the right to the protection of personal data.[21]

In these standards, it is proposed to regulate data portability in the following way:

> *"...*
>
> ***30. Right to Portability of Personal Data***
>
> ***30.1.*** *In the case of personal data by telephone or automated means, holder shall have the right to obtain a copy of the personal data that it had provided to the person responsible, or that are subject to treatment, in a structured electronic format, of common use and mechanical reading, that allows it to keep using them and transfer them to another person responsible, in case it requires so.*

[19] Ibero-American Data Protection Network, available here.
[20] Ibero-American Data Protection Network, "Lisbon Declaration 2007 V Ibero-American Data Protection Meeting," November 2007, Available here.
[21] Iberoamerican Data Protection Network, "Declaration of the XV Meeting of the Iberoamerican Data Protection Network, June 2017, available here.

> ***30.2.*** *Holder may request that its personal data are transferred directly from person responsible to person responsible when technically possible.*
>
> ***30.3.*** *The right to portability of personal data shall not affect negatively the rights and freedoms of others.*
>
> ***30.4.*** *Without prejudice to holder's rights, the right to portability of personal data shall not be admissible in the case of inferred, derived, created or generated information, or information obtained from the analysis or treatment performed by the person responsible, based on the personal data provided by holder, such as personal data that had been subject to a personalization, recommendation, categorization or profile creation process.*
>
> *…."

As we can see, the standards are essentially aligned to the GDPR, and it is not the exception regarding portability among its particularities that data portability is not restricted to the data provided by the data subject, but also includes those that are subject to treatment, which could include data obtained by the data controller indirectly.

IV. Initiatives to reform the right to portability in the private sector (Mexico)

As we have already decreed, the mismatch between the enactment of the laws for the protection of personal data in the public and private sectors led to a series of asymmetries between the two regulations, as in many of the cases, they have their point of influence in the European norms. On the one hand, the Federal Law on the Protection of Personal Data Held by Individuals and its Regulations, mainly, had a starting point in the repealed 95/46/EC Directive of the European Council, and on the other, the General Law of Protection of Personal Data in Possession of Obligated Subjects influenced by the GDPR.

We do not know whether, aware of the above, some legislators have proposed various reform initiatives to the LFPDPPP. Out of the eight reform initiatives that are in the legislative process, one that incorporates the right to portability for the private sector is distinguished, a proposal presented by Sen. Ricardo Monreal Ávila, coordinator of the Parliamentary Group Morena, called "Initiative with a draft decree amending, adding an Article 35 bis to the LFPDPPP, regarding portability."

The explanatory memorandum of this initiative states that Mexican legislation provides greater protection to data subjects in the public sector and becomes more lax in the private sector for it considers that it is necessary to recognize new rights or instruments that facilitate to data subjects of the data the circulation of the same, within the fundamental challenges, the recognition of the right to portability stands out.

In this sense, the initiative proposes the incorporation of Article 35 bis, as follows:

> *"…*
>
> *When personal data is processed via an electronic database, the holder shall have the right to obtain from the responsible a copy of the data object of the treatment in a structured and commonly used electronic format that allows him to continue using them.*

> *When the holder has provided the personal data and the treatment is based on consent or a contract, he will have the right to transmit said personal data and any other information that he has provided and that is kept in an automated treatment system to another system in a commonly used electronic format, without impediments by the responsible of the treatment from whom the personal data is withdrawn.*
>
> *The Institute will establish through guidelines the parameters to consider to determine the assumptions in which you are in the presence of a structured and commonly used format, as well as the technical standards, modalities and procedures for the transfer of personal data.*
>
> *…."*[22]

From the wording of the article itself, which is still a proposal for a reform initiative, we can see that it is almost identical to the wording of the LGPDPPSO.

The substantial differences can be identified in two sections: In the first paragraph that modifies the wording "electronically" to "via electronic database"; the second difference addresses a question of competition, since the regulation of protection of personal data held by individuals is exclusive to the federation, while the regulation of the public sector is concurrent; and reasons why it is modified from the "National System" to the "Institute" in the third paragraph.

Regarding the third paragraph of Article 35 bis, it is highlighted that the legislation, on the one hand, recognizes the autonomy of authority in the matter, in this case the National Institute of Transparency, Access to Information and Protection of Personal Data, so that in the use of its powers it determines the secondary regulatory path (guidelines), the way in which the right to portability will be developed and made effective.

In case the proposed reform initiative is approved, the institute will bear the great responsibility of developing the secondary regulations that must be compatible or consistent with the guidelines that the National System issued, with the aim of making this right operational, its exercise equivalent, and that aspiring to a harmonized protection and implementation between the two regulatory bodies, thus ending part of the dissonance between them, as regards personal data portability in Mexico.

The second great challenge of this secondary regulation will be that the right to portability is interoperable between the regulation of individuals and that of obligated subjects, which in itself is a complicated task if we begin to take into account first the differences between the portability of each regulatory body, and secondly, the rest of the dissonances that remain between the regulations of the public sector with that of the private sector, which requires additional reforms to the one proposed.

V. Particularities and comments regarding the right to personal data portability

We can say of this new modality of the right of access, which is boundary, because although it gives access to information related

[22] Ibidem, p. 7.

to the interested party or data subject, not all the information that a controller has of an individual necessarily constitutes personal data. That is, it gives you the right of access to information, but this may lack the attribute for which personal data is considered as such and therefore would escape the scope of protection of the regulations on the matter. It may also be the case that the information object of the portability contains personal data or information related to third parties (constitutional exception).

Several experts on the subject, as well as the WP29, consider that portability is a mechanism that promotes free competition and freedom of contract with any provider. These are issues that are not related to personal data, but that are related to other rights and freedoms of the individuals who owns those personal data (complementary rights).

We are again faced with a scenario in which the right to personal data protection is not only informative self-determination, but also an enabling or key right that allows the protection or access to other human rights and liberties of individuals.

These evolutions or novelties that arise as part of the right to the protection of personal data imply an expansion in its scope and competence, allowing it to become more robust.

Among the new challenges of this modality we find what is related to the created data, generated or inferred by the controllers, the current regulations exclude them, since they could reveal industrial or commercial secrets and competitive advantages of the controller. However, it is still data concerning data subjects, so it is estimated that it should be delivered. In this sense, only the generated data should be delivered, not how the data was generated, leaving the safeguard for the controller that can provide proof with the delivery of said information it damages them directly.

> ***We are again faced with a scenario in which the right to personal data protection is not only informative self-determination, but also an enabling or key right that allows the protection or access to other human rights and liberties of individuals.***

The previous proposal becomes relevant if we take into account that the majority of service providers have planned and begin to use "big data"[23] and "data science"[24] and other techniques and algorithms to process massive amounts of data to discover and infer other data related to the data subject.

Only the experience resulting from the exercise of this new modality of access to personal data, as well as the evolution that occurs with its exercise, will be able to tell us if other information related to the data subjects would be incorporated in the future.

Let's see what happens and learn from it for future exercises.

[23] Big data: It is the set of technologies that allow massive amounts of data to be processed from disparate sources, among to be able to grant them a utility that provides value. This can be discovering patterns of behavior of an organization's customers to create much more effective targeted advertising, predicting economic trends or discovering previously unknown relationships between variables that can open doors to innovation (Gil Elena, Biga Data, Privacidad y Protección de Datos, 2016, own translation).

[24] Data science: It is an interdisciplinary field that uses scientific methods, processes, algorithms and systems to extract insights from many structured and unstructured data (Dhar V, Data science and prediction, 2013, traducción propia).