GRA
GIBRALTAR REGULATORY AUTHORITY

Guidance on the General Data Protection Regulation

(5) Data Portability

13th March 2018

Guidance Note IR05/17

FOREWORD

The General Data Protection Regulation (the "GDPR") will come into force on the 25th May 2018, replacing the existing data protection framework under the EU Data Protection Directive.

As an EU regulation, the GDPR will not generally require transposition (EU regulations have 'direct effect') and will automatically become law in Gibraltar. Therefore, organisations involved in the processing of personal data need to be aware of the obligations that the GDPR will impose on them. The GDPR emphasises transparency, security and accountability by data controllers, while at the same time standardising and strengthening the right of European citizens to data privacy.

The Gibraltar Regulatory Authority ("GRA"), as the Data Protection Commissioner, is aware of the increased obligations that the GDPR places on organisations. The GRA's aim is to alleviate some of the concerns for businesses and public-sector organisations, and facilitate a smooth transition to future data protection standards through the publishing of a number of Guidance Notes.

CONTENTS

1. INTRODUCTION

The General Data Protection Regulation (the "GDPR") will come into force on the 25th May 2018, replacing the existing data protection framework under the EU Data Protection Directive.

This is the fifth of a series of Guidance Notes that the Gibraltar Regulatory Authority ("GRA"), as the Data Protection Commissioner, will issue in the run up to the 25th May 2018.

This Guidance Note provides general advice on the GDPR's right of data portability.

The GDPR creates a new right of data portability, which is closely related to the right of access but different in many ways. This new right will allow for data subjects to receive the personal data that they have provided to a data controller, in a structured, commonly used and machine-readable format, and have it transferred to another data controller. Under this new right, the data subject will have more power and control over their own personal data.

Individuals making use of their right of access under the Data Protection Act 2004 were constrained by the format chosen by the data controller when providing the requested information. The new right to data portability aims to empower data subjects regarding their own personal data, as it facilitates their ability to move, copy or transmit personal data easily from one IT environment to another (whether to their own systems, the systems of trusted third parties or those of new data controllers).

Data portability will be an important tool that will support the free flow of personal data between data controllers and therefore, data controllers should start developing and implementing methods which will contribute to answering a data portability request.

The aim of this guidance note is to provide advice on the GDPR's requirement relating to data portability and assist data controllers to clearly understand their respective obligations. This guidance note includes recommendations on good practice and tools that support compliance with the right to data portability. It also aims to clarify the meaning of data portability in order to enable data subjects to efficiently use their new right.

2. THE RIGHT TO DATA PORTABILITY

2.1. A right to receive personal data

GDPR - Article 20

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

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

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

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.

4. The right referred to in paragraph 1 shall not adversely affect the rights and freedoms of others.

Data portability is a right of the data subject to receive a subset of the personal data processed by a data controller concerning him or her, and to store those data for further personal use. The personal data can be stored on a personal device or private cloud without physically transmitting the data to another data controller.

Data portability complements the right of access. However, data portability offers an easier way for data subjects to manage and re-use personal data themselves.

It is important to note that the data should be received "in a structured, commonly used and machine-readable format".

Example 1

A data subject might be interested in retrieving his current playlist (or a history of listened tracks) from a music streaming service, to find out how many times he listened to specific tracks, or to check which music he wants to purchase or listen to on another platform. Similarly, he may also want to retrieve his contact list from his webmail application, for example, to build a wedding list, or get information about purchases using different loyalty cards, or to assess his or her carbon footprint.

2.2. A right to transmit personal data from one data controller to another data controller

Article 20(1) of the GDPR provides data subjects with the right to transmit personal data from one data controller to another data controller "without hindrance". Article 20(2) of the GDPR adds that personal data should be transmitted directly from one data controller to another upon the request of the data subject and where it is "technically feasible". Furthermore, Recital 68 encourages data controllers to develop interoperable[1] formats that enable data portability but without creating an obligation for controllers to adopt or implement processing systems which are technically compatible. However, the GDPR prohibits data controllers from establishing barriers to a data portability transmission.

The right to data portability is expected to provide opportunities for the sharing of personal data between data controllers in a safe and secure manner, under the data subject's orders.

2.3. When does data portability apply?

> **GDPR - Article 20(1)**
>
> The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, where:
>
> (a) the processing is based on consent pursuant to point (a) of Article 6(1) or point (a) of Article 9(2) or on a contract pursuant to point.

According to Article 20(1)(a) of the GDPR, in order for a request to fall under the scope of data portability, processing operations must be based:

- either on the data subject's consent (pursuant to Article 6(1)(a), or pursuant to Article 9(2)(a) when it comes to special categories of personal data); or
- on a contract to which the data subject is a party pursuant to Article 6(1)(b).

As an example, the titles of books purchased by an individual from an online bookstore, or the songs listened to via a music streaming service are examples of personal data that are generally within the scope of data portability, because they are processed on the basis of the performance of a contract to which the data subject is a party.

[1] Interoperable: computer systems or software able to exchange and make use of information.

The GDPR does not establish a general right to data portability for cases where the processing of personal data is not based on consent or contract.[2] For example, a financial institution will not be obliged to answer a data portability request concerning personal data processed as part of their legal obligation to prevent and detect money laundering and other financial crimes.

When it comes to employees' personal data, the right to data portability applies only if the processing is based on a contract to which the data subject is a party of. In many cases, it will not be considered that consent will have been freely given in this context, due to the imbalance of power between the employer and employee. Some HR data processing operations are instead based on the legal ground of legitimate interest, or are necessary for compliance with specific legal obligations in the field of employment. In practice, the right to data portability in an HR context will undoubtedly concern some processing operations (such as pay and compensation services, internal recruitment) but in many other situations a case by case approach will be needed to verify whether all conditions applying to the right to data portability are met.

Finally, the right to data portability only applies if the data processing is "carried out by automated means", and therefore does not cover most paper files.

3. INFORMING DATA SUBJECTS OF THEIR RIGHTS

In order to comply with the new right to data portability, data controllers must inform data subjects of the new right to data portability. Where the personal data is collected directly from the data subject, this must happen at the time where personal data are obtained.

Where the personal data has not been obtained from the data subject, Article 14(3) of the GDPR requires the information to be provided within a reasonable time not exceeding one month after obtaining the data, during first communication with the data subject, or when disclosure is made to third parties.

When providing the required information, the initial data controllers must ensure that they distinguish the right to data portability from other rights. Therefore, it is advised that data controllers clearly explain the difference between the types of data that a data subject can receive through the rights of subject access request and a data portability request.

It is also advised that data controllers always include information about the right to data portability before data subjects close any account they may have. This allows the data subjects to take their personal data, and to easily transmit the data to their own device or to another provider.

Finally, as leading practice for "receiving" data controllers, it is recommended that data subjects are provided with complete information about the nature of personal data which are

[2] See Recital 68 and Article 20(3) of the GDPR. Article 20(3) and Recital 68 provide that data portability does not apply when the data 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 data controller, or when a data controller is exercising its public duties or complying with a legal obligation.

relevant for the performance of their services. In addition to underpinning fair processing, this allows users to limit the risks for third parties, and also any other unnecessary duplication of personal data even where no other data subjects are involved.

4. DATA PORTABILITY VS. OTHER RIGHTS OF DATA SUBJECTS

When an individual exercises his or her right to data portability, he or she does so without prejudice to any other right (as is the case with any other rights in the GDPR).

A data subject can continue to use and benefit from the initial data controller's service even after a data portability operation. Data portability does not automatically trigger the erasure of the data from the systems of the initial data controller, and does not affect the original retention period which the data controller has in effect.

Equally, if the data subject wants to exercise his or her right to erasure ("right to be forgotten" under Article 17 of the GDPR), data portability cannot be used by a data controller as a way of delaying or refusing such erasure.

Should a data subject find that the personal data requested under the right to data portability does not fully address his or her request, any further request for personal data can be made under a right of access and this should be fully complied with, in accordance with Article 15 of the GDPR.

Where a specific European or local law in another field also provides for some form of portability of the data concerned, the conditions laid down in these specific laws must also be taken into account when satisfying a data portability request under the GDPR. First, if it is clear from the request made by the data subject that his or her intention is not to exercise rights under the GDPR, but rather, to exercise rights under sectorial legislation only, then the GDPR's data portability provisions will not apply to this request.[3]

If the request is aimed at portability under the GDPR, the existence of such specific legislation does not override the general application of the data portability principle to any data controller.

5. ASSESSING A DATA PORTABILITY REQUEST

[3] For example, if the data subject's request aims specifically at providing access to his banking account history to an account information service provider, for the purposes stated in the Payment Services Directive 2 (PSD2), such access should be granted according to the provisions of this directive.

5.1. What personal data must be included?

Pursuant to Article 20(1) of the GDPR, to be within the scope of the right to data portability, data must be:

- personal data concerning him or her; and
- which he or she has provided to a data controller.

Article 20(4) of the GDPR also states that compliance with data portability shall not adversely affect the rights and freedoms of others.

5.2. First condition: personal data concerning the data subject

Only personal data is in scope of a data portability request. Any data that does not concern the data subject, will not form part of the data portability scope. However, pseudonymous (i.e. key coded) data that can be clearly linked to a data subject (e.g. by him or her providing the respective identifier - see Article 11 (2) of the GDPR) is within the scope.

In many circumstances, data controllers will process information that contains the personal data of several data subjects. Where this is the case, data controllers should not take an overly restrictive interpretation of the sentence "personal data concerning the data subject". As an example, telephone or messaging may include (in the subscriber's account history) details of third parties involved in incoming and outgoing calls. Although records will therefore contain personal data concerning multiple people, subscribers should be able to have these records provided to them in response to data portability requests, because the records are (also) concerning the data subject. However, where such records are then transmitted to a new data controller, this new data controller should not process them for any other purpose which would adversely affect the rights and freedoms of the third parties (see below: third condition).

5.3. Second condition: data provided by the data subject

The second condition narrows the scope down to data "provided by" the data subject. There are many examples of personal data, which will be knowingly and actively "provided by" the data subject such as account data (e.g. mailing address, user name, age) submitted via online forms. Nevertheless, data "provided by" the data subject also result from the observation of his activity. As a consequence, "provided by" should also include the personal data that are observed from the activities of users such as raw data processed by a smart meter or other types of connected objects, activity logs, history of website usage or search activities.

A distinction can be made between different categories of data, depending on their origin, to determine if they are covered by the right to data portability. The following categories can be qualified as "provided by the data subject":

- Data actively and knowingly provided by the data subject (for example, mailing address, user name, age, etc.)

- Observed data provided by the data subject by virtue of the use of the service or the device. They may, for example, include a person's search history, traffic data and location data. It may also include other raw data such as the heartbeat tracked by a wearable device.

In contrast, inferred data and derived data are created by the data controller on the basis of the data "provided by the data subject". For example, the outcome of an assessment regarding the health of a user or the profile created in the context of risk management and financial regulations (e.g. to assign a credit score or comply with anti-money laundering rules) cannot in themselves be considered as "provided by" the data subject. Even though such data may form part of a profile kept by a data controller and derives from the analysis of the personal data provided by the data subject, this type of data will typically not be considered as "provided by the data subject" and therefore will not be covered by the right to data portability.[4]

A data controller can exclude the inferred data and derived data, but should include all other personal data provided by the data subject.

5.4. Third condition: the right to data portability shall not adversely affect the rights and freedoms of others

With respect to personal data concerning other data subjects:

The third condition is intended to avoid the retrieval and transmission of data containing the personal data of other (non-consenting) data subjects to a new data controller. This condition applies specifically in cases where the personal data is likely to be processed in a way that would adversely affect the rights and freedoms of the other data subjects (Article 20(4) of the GDPR).

Such an adverse effect would occur, for instance, if the transmission of data from one data controller to another, would prevent third parties from exercising their rights as data subjects under the GDPR (such as the rights to information, access, etc.).

The data subject making the request for the transmission of his or her data to another data controller, either gives consent to the receiving data controller for processing or enters into a contract with that controller.

Where personal data of third parties are included in the data set, another legal basis for the processing must be identified. For example, a legitimate interest may be pursued by the data

[4] Nevertheless, the data subject can still use his or her "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" as well as information about "the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) of the GDPR 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", according to Article 15 of the GDPR (which refers to the right of access).

controller under Article 6(1)(f)[5] of the GDPR, in particular when the purpose of the data controller is to provide a service to the data subject that allows the latter to process personal data for a purely personal or household activity.

Example 1

A data subject's bank account will contain personal data relating to the transactions not just of the account holder but also those of other individuals (e.g. if the data subject has transferred money to another individual's account). Under this example, the rights and freedoms of these third party individuals are unlikely to be adversely affected by the transmission of the bank account information to the account holder once a portability request is made, provided that the data is used for the same purpose (i.e. a history of the data subject's bank account.)

Example 2

A webmail service may allow the creation of a directory of a data subject's contacts, friends, relatives, family and broader environment. Since these data relate to (and are created by) the identifiable individual that wishes to exercise his right to data portability, data controllers should transmit the entire directory of incoming and outgoing e-mails to that data subject.

The processing operations initiated by the data subject in the context of personal activity that concerns and potentially impacts third party individuals remain under his or her responsibility, to the extent that such processing is not, in any manner, decided by the data controller.

However, should the receiving data controller process the personal data for other purposes, the rights and freedoms of the third-party individuals will not be respected and this will likely result in a data protection breach.

With respect to data covered by intellectual property and trade secrets:

The rights and freedoms of others are mentioned in Article 20(4) of the GDPR. While not directly related to portability, according to Recital 63, this can be understood as "including trade secrets or intellectual property and, in particular, the copyright protecting the software. However, even though these rights should be considered before answering a data portability request, "the result of those considerations should not be a refusal to provide all information to the data subject".

Data controllers should not reject a data portability request on the basis of an infringement of another contractual right (for example, an outstanding debt, or a trade conflict with the data subject). A potential business risk cannot serve as a basis for a refusal to answer the portability request. Data controllers can transmit the personal data provided by data subjects in a form that does not release information covered by trade secrets or intellectual property rights.

Equally, the right to data portability is not a right for an individual to misuse the information in a way that could be qualified as an unfair practice or that would constitute a violation of intellectual property rights.

[5] Article 6(1)(f) of the GDPR: "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."

6. RESPONDING TO A DATA PORTABILITY REQUEST

6.1. Identifying the data subject before answering a data portability request

GDPR - Article 12(6)

Without prejudice to Article 11, where the controller has reasonable doubts concerning the identity of the natural person making the request referred to in Articles 15 to 21, the controller may request the provision of additional information necessary to confirm the identity of the data subject.

Data controllers can request further information to verify the data subject's identity where they have reasonable doubts. In this regard, the GDPR does not prescribe a specific measure in which to authenticate a data subject (see Article 12(6) of the GDPR).

A data controller does not have to comply with a data portability request in cases where it can demonstrate that they are not able to identify the data subject (see Article 12(2) of the GDPR), except where the data subject, for the purpose of exercising his or her rights under those articles, provides additional information enabling his or her identification (see Article 11(2) of the GDPR). Where the latter is the case, a data controller cannot refuse to act on a data portability request.

It is important to note that there are often identification procedures already in place as data controllers regularly authenticate data subjects prior to entering into a contract or collecting his or her consent to the processing of their personal data.[6] These procedures can form part of the identification measures used to handle data portability requests. As a consequence, when an individual has registered their details with an organisation, the personal data used to register the individual concerned by the processing can also be used as evidence to identify them for portability purposes.[7] For example, where information and data collected online is linked to pseudonyms or unique identifiers (e.g. username and passwords), data controllers can implement appropriate procedures enabling an individual to make a data portability request and receive the data relating to him or her. In essence, this would prevent an initial data controller from having to request additional information regarding a data subject's identity which could lead to excessive demands and the collection of personal data which are not relevant or necessary.

[6] Examples of existing authentication procedures may include usernames and passwords which are frequently used to allow individuals to access their data in their email accounts, social networking accounts, and accounts used for various other services, some of which individuals chose to use without revealing their full name and identity.

[7] For example, when the data processing is linked to a user account, providing the relevant login and password might be sufficient to identify the data subject.

In any case, data controllers are required to implement an authentication procedure in order to ascertain the identity of the data subject requesting his or her personal data or more generally exercising the rights granted by the GDPR.

6.2. How must the initial data controller provide the portable data?

In this section, guidance is provided on how the initial data controller can transmit the information that is subject to a data portability request to the receiving data controller or individual.

What approach should the initial data controller implement?

GDPR – 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 data have been provided […].

The GDPR stipulates that data subjects have the right to transmit the data to another controller "without hindrance" from the controller to whom the data was originally provided (see Article 20(1) of the GDPR).

The Article 29 Working Party (the "WP29") characterises hindrance as any legal, technical or financial obstacles placed by the data controller in order to refrain or slow down access, transmission or re-use of the personal data. Examples of this could include requesting fees for delivering data, lack of interoperability or access to a data format or Application Programming Interfaces ("APIs")[8] or the provided format, excessive delay or complexity to retrieve the full dataset, deliberate complication of the dataset, or specific and undue or excessive sectorial standardisation or accreditation demands.[9]

Article 20(2) of the GDPR also places obligations on data controllers for transmitting the portable data directly to other data controllers "when technically feasible".

Recital 68 further clarifies the limits of what is technically feasible indicating that:

"it should not create an obligation for the controllers to adopt or maintain processing systems which are technically compatible".

[8] Application Programming Interface (API) means the interfaces of applications or web services made available by data controllers so that other systems or applications can link and work with their systems.

[9] Some legitimate obstacles might arise, as the ones, which are related to the rights and freedoms of others mentioned in Article 20(4) of the GDPR, or the ones that relate to the security of the controllers' own systems. It shall be the responsibility of the data controller to justify why such obstacles would be legitimate and why they do not constitute a hindrance in the meaning of Article 20(1) of the GDPR.

Additionally, initial data controllers are expected to transmit personal data in an interoperable format, although this does not place an obligation on receiving data controllers to support these formats. Direct transmission from one data controller to another could therefore occur when communication between two systems is possible, in a secured way,[10] and when the receiving system is technically in a position to receive the incoming data. If technical impediments prohibit direct transmission, the initial data controller should explain those impediments to the data subjects, as failure to communicate this could be similar in its effect to refusing to take action regarding a data subject's request (see Article 12(4) of the GDPR).

The WP29 recommend that data controllers explore and assess two different and complimentary paths for making portable data available to the data subjects or to other data controllers:

1. A direct transmission of the overall dataset of portable data (or several extracts of parts of the global dataset).

2. An automated tool that allows extraction of relevant data.

The second way may be preferred in cases of complex and large data sets as this allows for:

- the extraction of any part of the data-set that is relevant for the data subject in the context of his or her request;

- the use of data synchronisation mechanisms (e.g. in the context of a regular communication between data controllers); and

- it helps minimise privacy risks on the part of the initial controller and may help compliance for the receiving controller.

These methods could be implemented through various means such as secured messaging, SFTP server, a secured WebAPI or WebPortal.

Additionally, data subjects should be enabled to make use of personal data stores, personal information management systems or other kinds of trusted third parties to hold and store personal data, and grant permission to data controllers to access and process this data as required.

What is the expected data format?

The GDPR does not specify in what format personal data should be provided. However, the GDPR places requirements on data controllers to provide it in a format which supports re-use. Article 20(1) of the GDPR explicitly states that personal data should be provided in a "structured", "commonly used" and "machine-readable format". Recital 68 further clarifies that this format should be interoperable, a term defined[11] in the EU as:

"the ability of disparate and diverse organisations to interact towards mutually beneficial and agreed common goals, involving the sharing of information and knowledge between the

[10] Through an authenticated communication with the necessary level of data encryption.

[11] Article 2 of Decision No 922/2009/EC of the European Parliament and of the Council of 16 September 2009 on interoperability solutions for European public administrations (ISA) OJ L 260, 03.10.2009, p. 20.

organisations, through the business processes they support, by means of the exchange of data between their respective ICT systems."

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 initial data controller. In that way, "structured, commonly used and machine readable" are specifications for the means, whereas interoperability is the desired outcome.

Recital 21 of Directive 2013/37/EU[12,13] defines "machine readable" as:

"a file format structured so that software applications can easily identify, recognize and extract specific data, including individual statements of fact, and their internal structure. Data encoded in files that are structured in a machine-readable format are machine-readable data. Machine-readable formats can be open or proprietary; they can be formal standards or not. Documents encoded in a file format that limits automatic processing, because the data cannot, or cannot easily, be extracted from them, should not be considered to be in a machine-readable format. Member States should where appropriate encourage the use of open, machine-readable formats."

The WP29 recognises that the most appropriate format will differ across sectors and adequate formats may already exist, and should always be chosen to achieve the purpose of being interpretable and affording the data subject with a large degree of data portability. As such, formats that are subject to costly licensing constraints would not be considered an adequate approach.

Recital 68 clarifies that:

"The data subject's right to transmit or receive personal data concerning him or her should not create an obligation for the controllers to adopt or maintain processing systems which are technically compatible."

Thus, portability aims to produce interoperable systems, not compatible systems.[14]

The WP29 state that personal data are expected to be provided in formats that have a high level of abstraction from any internal or proprietary format. As such, data portability implies an additional layer of data processing by controllers, this allows for data to be extracted from the platform and for data outside the scope of portability (such as inferred data or data related to the security of systems) to be filtered out. Therefore, data controllers are encouraged to identify beforehand which formats are within the scope of portability in their own systems.

Where there are no common formats in use for a given industry or given context, the WP29 suggest that initial data controllers should provide personal data using regularly used open formats (e.g. XML, JSON, CSV…) along with useful metadata at the best possible level of granularity, while maintaining a high level of abstraction. As such, suitable metadata should

[12] Amending Directive 2003/98/EC on the re-use of public sector information.

[13] The EU glossary (http://eur-lex.europa.eu/eli-register/glossary.html) provides further clarification on expectations related to the concepts used in this guideline, such as machine-readable, interoperability, open format, standard, metadata.

[14] 35 ISO/IEC 2382-01 defines interoperability as follows: "The capability to communicate, execute programs, or transfer data among various functional units in a manner that requires the user to have little or no knowledge of the unique characteristics of those units."

be used in order to accurately describe the meaning of exchanged information. This metadata should be enough to make the function and re-use of the data possible but without revealing trade secrets. For example, providing an individual with PDF versions of an email inbox would not be sufficiently structured or descriptive to allow the data to be easily re-used. Instead, the e-mail data should be provided in a format which preserves all the metadata, to allow the effective re-use of the data.

Therefore, when selecting a data format, initial data controllers should consider how different formats would impact or hinder the individual's right to re-use the data. In cases where a data controller is able to provide choices to the data subject regarding the preferred format of the personal data, a clear explanation of the impact of the choice should be provided. However, data controllers must take into account that there is no legitimate ground for processing additional metadata for the sole purpose that they might be needed or wanted to answer a data portability request.

The WP29 strongly encourages cooperation between industry stakeholders and trade associations to work together on a common set of interoperable standards and formats to deliver the requirements of the right to data portability. This challenge has also been addressed by the European Interoperability Framework (EIF) which has created an agreed approach to interoperability for organizations that wish to jointly deliver public services. Within its scope of applicability, the framework specifies a set of common elements such as vocabulary, concepts, principles, policies, guidelines, recommendations, standards, specifications and practices.[15]

6.3. What is the time limit imposed to answer a portability request?

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

Article 12(3) of the GDPR requires that initial data controllers provide "information on action taken" to the data subject "without undue delay" and in any event "within one month of receipt of the request". This period can be extended to a maximum of three months for complex cases, provided that the data subject is informed about the reasons for the delay within one month of the original request. Data controllers operating information society

[15] The new European Interoperability Framework (EIF) is part of the Communication (COM(2017)134) from the European Commission adopted on 23 March 2017. The framework gives specific guidance on how to set up interoperable digital public services. Source: https://ec.europa.eu/isa2/eif_en.

services are likely to be better equipped to be able to comply with requests within a very short time period.

However, the WP29 note that extensions should be avoided where possible. For example, if transmission of data via the internet is problematic due to its size, then the initial data controller may consider alternative means such as streaming or saving on to physical media (DVD, CD, etc.) or transmitting directly to the receiving data controller (as per Article 20(2) of the GDPR where technically feasible), in order to comply with the request without delay. It is good practice to define the timeframe in which a data portability request can typically be answered and communicate this to data subjects.

6.4. In which cases can a data portability request be rejected or a fee charged?

Charging a fee for a data portability request:

> **GDPR - Article 12(5)**
>
> Information provided under Articles 13 and 14 and any communication and any actions taken under Articles 15 to 22 and 34 shall be provided free of charge. Where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character, the controller may either:
>
> (a) charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested; or
>
> (b) refuse to act on the request.
>
> The controller shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request.

Article 12 of the GDPR prohibits the initial data controller from charging a fee for the provision of the personal data, unless the data controller can demonstrate that the requests are manifestly unfounded or excessive, "in particular because of their repetitive character". For information society services that specialise in automated processing of personal data, implementing automated systems such as APIs can facilitate the exchanges with the data subject, hence lessen the potential burden resulting from repetitive requests. Therefore, there should be very few cases where the data controller would be able to justify a refusal to deliver the requested information, even regarding multiple data portability requests.

The overall cost of the processes created to answer data portability requests should not be taken into account to determine the excessiveness of a request. In fact, Article 12 of the GDPR focuses on the requests made by one data subject and not on the total number of requests received by a data controller. As a result, the overall system implementation costs should neither be charged to the data subjects, nor be used to justify a refusal to answer portability requests.

Rejecting a data portability request:

GDPR - Article 12(4)

If the controller does not take action on the request of the data subject, the controller shall inform the data subject without delay and at the latest within one month of receipt of the request of the reasons for not taking action and on the possibility of lodging a complaint with a supervisory authority and seeking a judicial remedy.

It is important to note that the initial data controller cannot remain silent when it is asked to answer a portability request. The above requirement states that data controllers who refuse a data portability request must do this within one month of receiving the request and must inform the data subject of "the reasons for not taking action and on the possibility of lodging a complaint with a supervisory authority and seeking judicial remedy".

6.5. How to deal with a large or complex personal data collection?

The GDPR does not explain how to address the challenge of responding to a request that involves a large data collection, a complex data structure or other technical issues that could create difficulties for data controllers or data subjects.

Nevertheless, it is crucial that the individual is in a position to understand the definition, schema and structure of the personal data that could be provided by the data controller. Therefore, the WP29 recommend that initial data controllers, in the first instance, provide data in a summarised form using dashboards allowing data subjects to transfer a subset of the personal data rather than the entirety. Further, the initial data controller should provide an overview in a concise, transparent and easily accessible form, using plain language, as required by Article 12(1) of the GDPR, and in such a way that data subjects always have clear information of what data to download or transmit to another data controller in relation to a given purpose.

As referenced in the foregoing, a practical way by which an initial data controller can answer requests for data portability may be by offering an appropriately secured and documented API. This may enable individuals to make requests of the initial data controller for their personal data via their own or third party software or grant permission for others to so do on their behalf (including another data controller) as specified in Article 20(2) of the GDPR. By granting access to data via an externally accessible API, it may also be possible to offer a more sophisticated access system that enables individuals to make subsequent requests for data, either as a full download or as a delta function containing only changes since the last download, without these additional requests being onerous on the initial data controller.

6.6. How can portable data be secured?

GDPR - Article 5(1)(f)

Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

The GDPR requires data controllers to have appropriate organisational and technical security measures in place to protect personal data from being accidentally or deliberately compromised.

Data portability raises some security issues that need to be considered:

<u>How can initial data controllers ensure that personal data is securely delivered to the right individual?</u>

As the aim of data portability involves the transfer of personal data out of a data controller's information system, the transmission may become a possible source of risk (in particular of data breaches during the transmission).

The initial data controller is responsible for taking all the security measures needed to ensure that:

- personal data is securely transmitted (by the use of end-to-end or data encryption) to the right destination (by the use of strong authentication measures);
- the personal data remaining in their systems continues to be protected; and
- there are transparent procedures in place for dealing with possible data breaches.

Therefore, initial data controllers should generally assess the specific risks linked with data portability and take appropriate mitigation measures. Examples of such measures could include:

- using additional authentication information, such as a shared secret, or another factor of authentication, such as a onetime password;
- suspending or freezing the transmission if there is suspicion that the account has been compromised; and/or
- authentication by mandate such as token-based authentications where there is direct transmission from controller to controller.

It is important to note that such security measures must not be obstructive in nature and must not prevent users from exercising their rights, e.g. by imposing additional costs.

How can users be assisted to secure the storage of their personal data in their own systems?

As data portability allows data subjects to retrieve their personal data from an online service, there is always the risk that users may store this in less secured systems than the one provided by the service.

The WP29 note that the data subject requesting the data is responsible for identifying the right measures in order to secure personal data in their own system. However, data controllers should make data subjects aware of this responsibility so that they may take steps to protect the information he or she has received. To assist the data subject achieve this goal, data controllers may recommend appropriate format(s), encryption tools and other security measures.

7. CONTROLLERSHIP OF PERSONAL DATA

Initial data controllers, answering data portability requests, under the conditions set in Article 20 of the GDPR, are not responsible for the processing handled by the data subject or by the data controller receiving the personal data.

The initial data controller will act on behalf of the data subject, including when the personal data is being transmitted to another data controller under a data portability request. In this respect, the initial data controller is not responsible for the receiving data controller's compliance with data protection law.

At the same time, the initial data controller should set safeguards to ensure they genuinely act on the data subject's behalf. For example, they can establish procedures to ensure that the type of personal data transmitted are indeed those that the data subject wants to transmit. This could be done by obtaining confirmation from the data subject either before the transmission of personal data or when the original consent for processing is given by the data subject.

Initial data controllers answering a data portability request have no specific obligation to check and verify the quality of the data before transmitting it. As to be expected, these data should already be accurate, and up to date, according to the principles stated in Article 5(1) of the GDPR.

It is important to note that data portability does not impose an obligation on the data controller to retain personal data for longer than is necessary or beyond any specified retention period, simply to serve any potential future data portability request.

Where the personal data requested are processed by a data processor, the contract concluded in accordance with Article 28 of the GDPR must include the obligation to assist "the controller by appropriate technical and organisational measures, (…) to respond to requests for exercising the data subject's rights".

Under these circumstances, the data controller should implement specific procedures with its data processors to answer data portability requests. In case of a joint controllership, a contract should be established with clearly defined responsibilities between each data controller regarding the processing of data portability requests.

A receiving data controller is responsible for ensuring that the portable data provided is relevant and not excessive. If part of the data transmitted is not relevant with regard to the purpose of the new processing, it should not be kept and processed by the receiving data controller. For example, in the case of a data portability request made to a webmail service, where the request is used by the data subject to obtain emails and send them to a secured archive platform, the new data controller does not need to process the contact details of the data subject's correspondents. If this information is not relevant with regard to the purpose of the new processing, it should not be kept and processed. In any case, receiving data controllers are not obliged to accept and process personal data transmitted following a data portability request.

Similarly, where a data subject requests the transmission of details of his or her bank transactions to a service that assists in managing his or her budget, the receiving data controller does not need to accept all the data, or to retain all the details of the transactions once the information has been used for the purposes of the new service. In other words, the data accepted and retained should only be that which is necessary and relevant to the service being provided by the receiving data controller.

A receiving data controller, for the purposes of the newly received personal data, becomes a new data controller and must respect and comply with the principles stated in Article 5 of the GDPR, such as lawfulness, fairness and transparency, purpose limitation, data minimization, accuracy, integrity and confidentiality, storage limitation and accountability. The receiving data controller must also clearly and directly state the purpose of the new processing before any request for transmission of the portable data, in accordance with the transparency requirements set out in Article 14 of the GDPR.

Data controllers holding personal data should be prepared to facilitate their data subject's right to data portability.

IMPORTANT NOTE

This document is purely for guidance and aims to supplement the 29WP's Guidelines on the right to data portability.[16] The document does not constitute legal advice or legal analysis. All organisations that process data need to be aware that the GDPR will apply directly to them. The responsibility to become familiar with the GDPR and comply with its provisions from 25th May 2018 onwards therefore lies with the organisation.

Where necessary, the Data Protection Commissioner will review this Guidance Note in accordance with any updates or other developments. In the event of any conflict or inconsistencies between this Guidance Note and the GDPR, the GDPR will take precedence.

[16] Article 29 Working Party, 'Guidelines on the right to data portability' (5 April 2017).

CONTACT US

Gibraltar Regulatory Authority
2nd floor, Eurotowers 4, 1 Europort Road, Gibraltar

☎ (+350) 20074636
✉ privacy@gra.gi
🌐 www.gra.gi