15 February 2017

Comments by the Centre for Information Policy Leadership

on the Article 29 Data Protection Working Party's

"Guidelines on the right to data portability"

adopted on 13 December 2016

On 13 December 2016, the Article 29 Data Protection Working Party (WP29) adopted its "Guidelines on the right to data portability" (guidelines) and associated Frequently Asked Questions (FAQ). The WP invited public comments on these documents by 15 February 2017. The Centre for Information Policy Leadership (CIPL)[1] welcomes the opportunity to submit the brief comments below.

The right to data portability is laid down in Article 20 GDPR as a new right of individuals in Chapter III on the rights of the data subject. It seeks to give individuals greater empowerment over their personal data and to stimulate competition and innovation by making it easier to switch between different service providers.

Given that data portability is a new right in the area of data protection, without a significant track record of practical application and implementation by industry, CIPL welcomes that the WP29 has focused on this new right by developing practical guidance on how to implement it.

These CIPL comments must be seen in light of the double objective of the right to data portability, which has also been recognised by the WP29: providing individuals with an additional tool for control over their personal data and contributing to competition and innovation, which is beneficial to individuals, businesses and society at large. The right to data portability must be implemented in a way that effectively supports both objectives. More specifically:

- The data portability right should be applied in a way that effectively provides added value to individuals, in addition to the other rights in Chapter III of the GDPR and already existing under the Data Protection Directive. Data portability should not replace or recalibrate these other rights. It should also be considered that there are areas where the exercise of data portability does not create added value to individuals. For example, it is not obvious that data portability has added value in

[1] CIPL is a privacy and data protection think tank in the law firm of Hunton & Williams LLP and is supported by approximately 50 member companies that are leaders in key sectors of the global economy as well as by additional companies that are participating in issue-specific CIPL projects. CIPL's mission is to engage in thought leadership and develop best practices to ensure effective privacy protection in the modern information age. For more information, please see CIPL's website at http://www.informationpolicycentre.com/. Note that nothing in this submission should be construed as representing the views of any individual company supporting CIPL or participating in CIPL's projects or of the law firm Hunton & Williams.

respect of employees' data or personal data in the context of B2B activities.[2] Even in the consumer context, there are circumstances where porting data would not necessarily be in the interest of the individual because the receiving controller may not use the ported data for the same purpose or because an excessive amount of data would be overwhelming to the individual.

- An overbroad implementation of the data portability right may stifle competition and innovation and impose unnecessary burdens on organisations. It may require substantive and unrealistic efforts from controllers in order to have the technical systems in place facilitating the data portability right. In many instances, controllers will have to make a significant technical investment and create compatible IT infrastructures and API to make the right workable. Of course, this should not restrict the use of an effective data portability right, but it should not lead to disproportionate efforts, especially in areas where the right does not present added value to individuals. The costs of the implementation of Article 20 GDPR, a consequence of its technical complexity, should be balanced with its advantages.

- In addition, processors may be also significantly impacted by the data portability right, since they will have to implement the technical measures to enable data portability of the controllers' clients data in outsourced systems.

- Organisations need to have full legal certainty about the scope of application of the data portability right, as envisaged in the GDPR, in order to be able to make the appropriate changes and investments and not to be required to 'reinvent the wheel' later on.

Moreover, we do suggest a few clarifications of the guidelines as outlined below, particularly in relation to:

- The definition of the data that may be subject to a data portability request.
- The responsibilities of the sending and receiving parties.
- The status of shared and third-party data.
- The requirement and feasibility of technical formats.

CIPL's comments are organised under the headings used in the guidelines. We note that our comments are limited to the issues the WP29 included in the guidelines and not a comprehensive discussion of data portability. As a result, we may not cover every important issue raised by the new right and may seek to provide further input to the WP29 at a future time when and if useful and appropriate.

Particularly because data portability is uncharted territory in many ways, we recommend that the guidelines be treated as a 'living document' subject to amendment and clarification

[2] Interestingly, in French law (see LOI n° 2016-1321 du 7 octobre 2016 pour une République numérique), the right to data portability has been recently introduced in the Code de la Consommation (in Art 48, with a reference to the GDPR), as a right which only applies in the consumer area.

based on evolving future experiences. Equally, it may be prudent to focus on ensuring legal certainty for controllers and individuals and avoiding unnecessary costs and infrastructure and system changes.

Finally, data portability is a subject where novel ideas should be discussed with all stakeholders, in order to turn the concepts included in the GDPR into effective and workable arrangements. Thus, CIPL proposes to facilitate a roundtable with key stakeholders, which could be instrumental in reaching the right outcomes. Possible subjects for discussion include: the selection of ported data by the individual, obligations on the receiving controller to assess the data received and what is needed for purposes of his own processing, and interoperability and technical formats (as start of a multi-stakeholder process, see 4 a, below).

Comments

1. What are the main elements of data portability?

    a. A right to receive personal data/A right to transmit personal data from one data controller to another data controller (p. 4)

The guidelines state that 'data portability is a right to receive personal data' and 'complements the right of access' (p. 4). The WP29 further notes that data portability offers an easy way for the data subject to manage his or her personal data. However, further clarification would be helpful in respect of the following:

- The relationship between data portability and other individuals' rights, in particular the right to access in Article 15 GDPR and the right to erasure ('right to be forgotten') in Article 17 GDPR. The guidelines should make it clear that the data portability right should neither replace nor recalibrate these other rights and that its implementation should focus on domains where it effectively has added value.

- High-level and non-prescriptive guidance concerning controllers' responsibility to inform individuals of the implications of exercising a data portability request in accordance with Article 14(2) GDPR ('information to the data subject'), leaving flexibility to organisations with respect to the specific information they provide. Where relevant, helpful and appropriate, information to data subjects may include more than a mere statement of the right, but may also include a short explanation of the scope, the purpose of the right, the type of data that can be ported, and the pros and cons of the exercise of the right.

- How the right to data portability may be modulated in practice, to give individuals an effective means to select what data should be transferred, also taking into account technical restrictions and costs. There is a direct relation to the right of access which requires the controller to distinguish categories of personal data. More specifically, such a selection should be done bearing in mind that the individuals may not be in a

position to evaluate what data are in the scope of the data portability right. In addition, one recognised option should be to rely on standard download functionalities in the controllers' systems that would create a CSV or similar file without any systematic ability to tailor the data set.

Recommendation: Clarify the following main elements of the right to data portability along the lines described above:

(1) the connection of the right to data portability with Article 14 of the GDPR ('information to the data subject');

(2) the connection between the right to data portability and the right to access as well as the right to erasure ('right to be forgotten');

(3) the application of the right to data portability, in a way that effectively allows the individual to select the data he or she wishes to port.

b. Data portability tools

The guidelines note that individuals should be offered the right to port personal data directly from one controller to another controller where technically feasible. For cloud services the feasible mechanism for fulfilling that right is driven by responsibilities of the 'sending' and 'receiving' controller and the need to support the variety of different services available to customers. In some instances, the mechanism that would likely be the best solution for portability would be that of the 'pull' model.

The 'pull' model has several attractive attributes. First, it provides the opportunities for individuals and the receiving service to agree on appropriate processing of the customer data before any data is transferred. Second, it does not require competing services to understand the internals of each other's systems. Finally, the receiving service has an incentive to create the tools needed to absorb the transferred data and gain a new customer.

Recommendation: Recognise the possibility of using the 'pull' model in appropriate circumstances for porting personal data directly from one data controller to another data controller.

c. Controllership (p. 5)

The exercise of the right to data portability involves three parties: the individual who requests data to be ported, the sending controller who has the obligation to select and send the data, and the receiving controller who should make it possible for the sending data controller to fulfil its obligation in an appropriate manner.

An effective and proportionate implementation of the data portability right requires these three parties to co-operate. We refer in this context to Recital 63 which states—in

connection to the right to access—the need for the individual to co-operate with the controller: 'Where the controller processes a large quantity of information concerning the data subject, the controller should be able to request that, before the information is delivered, the data subject specify the information or processing activities to which the request relates.'

The guidelines state that 'a receiving data controller is responsible for ensuring that portable data provided are relevant and not excessive with regard to the new data processing' (p. 6).

First, we note that it is not clear that under the GDPR the 'receiving' data controller has a blanket obligation to receive or ingest any and all data that someone might send to it under the data portability right. It appears that the supposed or presumptive receiving controller should be able to make choices with respect to whether it will accept and ingest any such data. We therefore ask that the WP clarify this point.

Further, when a receiving controller does accept data, the above language in the guidelines implies an allocation of responsibility to the receiving controller that may create an unrealistic compliance burden for the receiving controller to ensure the data is relevant and not excessive. Since the receiving controller may receive an unspecified data set, resulting from the original request of the individual, it may be impractical or even disproportionate to require the receiving controller to assess all data. It may be also hard to explain to the individual why certain data should not be retained or processed further.

We recommend that the sentence 'a receiving data controller is responsible for ensuring that the ported data provided are relevant and not excessive with regard to the new data processing' (p. 6) is deleted. It is unrealistic and impractical for the receiving data controller to be able to comply with this requirement, especially immediately upon receiving the data.

Moreover, it is unrealistic for the receiving controller to provide to individuals a full notice about data use, including the purpose of processing for ported data, before the request for transmission. The receiving controller is not going to know about the data portability request until they receive the request to include ported data.

It may also not be desirable to provide too many details about the modalities of data portability right and how it may work in practice between three parties, as this is likely to develop over time based on experiences and practices. In our view, the guidelines should emphasise flexibility for the parties to implement solutions that will meet the requirements under Article 20 in a practical and feasible manner.

Recommendations: Clarify whether supposed or presumptive "receiving" controllers are automatically required under the GDPR to receive any and all ported data or whether they can chose not to accept ported data. Further, when ported data is received, retain flexibility around the requirements on receiving controllers associated with determining whether ported data is relevant and not excessive and ensure that no undue burden is

placed on the receiving controller with respect to that requirement. Delete the sentence 'a receiving data controller is responsible for ensuring that the ported data provided are relevant and not excessive with regard to the new data processing'.

2. When does data portability apply? (p. 6)

    a. Which processing operations are covered by the right to data portability? (p. 6).

The guidelines state that in 'order to fall under the scope of data portability' the processing must be based on either the data subject's consent or on a contract. Further, the WP clarifies that '[t]he 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.'

This interpretation is fully in accordance with Article 20 GDPR. CIPL recommends that the WP29 clarify that it is the sending controller's processing operations that must be based on consent or contract. While this may appear obvious, given the limitation of the data portability right to personal data provided by the individual to the controller, it would be helpful to explicitly state that.

Moreover, we take the view that by exercising the data portability right, the individual by definition gives consent to the new controller to process the ported data, or very often enters into a contract with them.

We also believe that the guidelines should make clear that in respect of the receiving controller there may be other grounds for processing other than consent and contract (for example, legitimate interest), and that therefore the legal grounds for the processing may differ based on the circumstances in each case.

Recommendation: Clarify that the processing operations of the sending controller must be based on consent or contract. Confirm that the individual exercising the right to data portability by definition gives consent to the new controller or likely enters into a contract with them.

    b. What personal data must be included (p. 7)

First condition: personal data concerning the data subject

According to Article 20(1), the data that is within the scope of the right to portability are personal data concerning the data subject which he or she has '*provided*' to a controller.

The guidelines clarify that '[o]nly personal data is in scope of a data portability request', including pseudonymous data and excluding anonymous data. They further state that pseudonymous data is within the scope when it can be clearly linked to the data subject.

However, Article 11(2) GDPR clearly states that there is no right to data portability for data that no longer identify a data subject, unless the data subject provides more information

that enables the data controller to identify him or her. This could cover pseudonymised data, although the controller has no autonomous obligation to acquire additional information for the identification of the data subject according to Article 11 (1) and Recital 57. For instance, in clinical trials, the sponsor can only access coded data and the only one who is entitled to re-identify the patient is the investigator/hospital that has previously codified the data and that must keep confidential the links that enable the re-identification. Under those circumstances, no data subject's right, including the right to data portability, can be exercised as between the data subject and the sponsor of the trials who is being asked to port the data.

CIPL notes that the GDPR does not specifically exclude the application of the data portability right to personal data created exclusively in the context of the employee/employer relationship (human resources data). However, application in this specific area would be complex, in view of the labour protections already in place under national law and the many additional considerations that would arise in terms of the appropriateness of porting human resources data from one employer to another, whereas the added value for the individual is not clear. We suggest that the WP29 clarify that the data portability right does not extend to the employment context.

Recommendation: Clarify that under certain circumstances the right to data portability cannot be exercised in relation to pseudonymised data. Clarify that the data portability right does not extend to the employment context as we do not believe that this was the original legislative intent, or that the right may be limited in that context to a narrow subset of data which is processed as necessary for the performance of an employment contract.

Second condition: data provided by the data subject (p. 8)

The WP29 states that 'provided by' the data subject not only includes data that the data subject has knowingly provided, such as account data, but also 'personal data that are generated by and collected from the activities of users.' The WP29 divides provided data into two categories: (i) 'data actively and knowingly provided by the data subject'; and (ii) '[o]bserved data … "provided" by the data subject by virtue of the use of the service and device.' (p. 8).

CIPL appreciates this specification and explicit exclusion of 'derived' and 'inferred' data from the scope of the data portability right. Our understanding is that observed data includes 'raw', primary data (such as tracked health information, geolocation, traffic data and search data), while 'derived' or 'inferred' data refers to the analysis of such data, secondary data which is excluded from the data portability right. We agree that data portability cannot be applied to secondary personal data—'derived' or 'inferred'—as that goes beyond the text of Article 20 GDPR and may also hinder protection of other rights, such as trade secrets or intellectual property, or other commercial interests, such as a competitive advantage. By way of an example, often data that is collected from the data subject's use of a service, is

processed and analysed immediately. The guidelines should make clear that this creates secondary data, similar to inferred data, that should be excluded from the data portability right. We would welcome more examples of the distinction between observed and derived/inferred data to ensure that our interpretation is correct.

In this context, we would like to draw attention to the difference in the wording between Articles 20 and 13 of the GDPR. The former refers to data provided to the controller and the latter refers to data collected from the data subject.

We thus suggest that under Article 20, there must be a voluntary, affirmative element of 'providing' data to the controller, as opposed to collecting data from an individual who may be passive. The requirement that data be 'provided' as opposed to 'collected' raises the question of whether 'observed' data qualifies as 'provided' data, given that the individuals may not have had an active role in the process. Rather, it appears that 'observed' data might be classified as 'collected' data that is different from and goes beyond the scope of 'provided' data covered by Article 20.

Including all observed data within the definition of 'provided' data under Article 20 does not seem to be justified under a plain reading of the text of the GDPR. On the contrary, including all 'observed' data within the scope of the data portability right would extend its scope arbitrarily and without any additional criteria or factors to take into account. We take the view that the scope of data portability right should not be extended. This would be counterproductive and would only lead to disproportionate efforts and unnecessary costs and burdens, especially in cases where there isn't an obvious added value to individuals.

Examples of observed data that could be included within the scope of 'provided' are data relating to a wearable tracking device where such data is processed by a data controller, where the individuals willingly and knowingly provide tracking data and sensed data because it is part of the desired service to the individual and conveys a desired benefit to the individual. However, other observed data should not considered 'provided' under Article 20. This includes 'network traffic data,' as we believe such data falls under the category of technical analysis as it is data generated by systems and not provided by the individual in return for a specific benefit or as part of the service he or she intended to receive.

Recommendation: Clarify the scope of covered data to affirmatively 'provided' data and exclude observed data, unless this data is inextricably linked to the provided data and its provision presents added value to the data subject. The guidelines should provide further examples of the various situations, including examples of the distinction between observed and derived/inferred data.

Third condition: the right to data portability shall not adversely affect the rights and freedoms of others (p. 9)

c. With respect to personal data concerning other data subjects (p. 9)

This section is somewhat contradictory and it places unreasonable burdens on controllers.

First, the discussion on pages 9 and 10 contradicts the discussion on pages 7 and 8, particularly the statement that where the data to be ported 'contains the personal data of several data subjects' the 'data controller must not take an overly restrictive interpretation of the sentence "personal data concerning the data subject." '

This issue of the rights of other data subjects arises in cases where there is one account holder and/or multiple account users underneath that account, such as in banking, telecommunications, cable and Internet services, etc. Should an individual account holder be able to request and download other people's data (such as family members' data)? This may raise issues with respect to these other people's data protection rights. Organisations lack clarity on how to respond to cases in which the data of different individuals is co-mingled and the WP29 guidelines are silent on this point. In many cases, there may be a legitimate reason to port such data, but the criteria need to be further specified.

Second, where the individual decides to port data to a receiving controller that includes the data of other individuals, the guidelines place a considerable burden on the receiving controller, including determining a legal ground for processing of such data belonging to other individuals. Such third-party data is incidental to the main data and the third party should not be the focus of the receiving controller. If the individual chooses to port all their data, including family members' data, that should be allowed, especially where the legitimacy of the request is obvious from the circumstances.

Indeed, the current wording in the guidelines (pp. 7-8 and 9-10) may place a disproportionate burden on the sending controller, who may not be in a position to port personal data of other individuals, and on both the sending and receiving controllers, who cannot easily determine the risk associated with portability of data that belongs to others.

Recommendation: Provide further guidance on the data controllers' obligation to comply with a data portability request involving shared and third-party data, including the legal basis for processing the data of third parties by the sending and the receiving controllers.

d. With respect to data covered by intellectual property and trade secrets (p. 10)

The guidelines cite Article 20(4) and Recital 68 of the GDPR, which provide that the exercise of the right to data portability should not adversely affect the rights and freedoms of others, including rights of controllers. These rights and freedoms of others also include 'trade secrets or intellectual property and in particular copyright protecting the software' mentioned in Recital 63 (p. 10).

We acknowledge that these rights will be taken into consideration and would recommend a stronger acknowledgment from WP29 of the right of the controller to protect its intellectual property, as this is addressed only briefly in the guidance. We would also welcome clarification as to how a balance is achieved. The guidelines consider that 'the result of these considerations should not be a refusal to provide all information to the data subject' and that '[a] potential business risk cannot, however, in and of itself serve as the basis for a refusal to answer the portability request' (p. 10).

We agree that one should avoid that controllers invoke by default intellectual property rights or trade secrets in order to circumvent the exercise of an individual's right to data portability. However, the data provided in data fields, for example, may aggregate to a specific analysis and competitive advantage that a business has carefully constructed; thus parting with the data could be seen as giving an unfair advantage to a competing business. With data driving new products, services and economic growth, the guidelines should confirm that the interests and rights of controllers are taken into account when dealing with a request to data portability. Indeed, the implementation of the data portability right should take place in a balanced manner, doing full justice to these other competing rights and interests.

We recommend that the guidelines include more flexibility in recognising the competing rights and interests, with further examples of situations in which intellectual property rights or legally protected trade secrets might be invoked to justify restrictions to the data portability right under Articles 20 (4) and 23(1). This is a complex area, where various interests must be balanced and which may merit further guidance at a later stage, as the experiences and best practices start to emerge.

Recommendation: <u>Clarify the weighing of the right to data portability and intellectual property rights/trade secrets, and include room for flexible interpretation where the balancing of different interests can be adapted based on emerging best practices</u>.

3. <u>How do the general rules governing the exercise of data subject rights apply to data portability? (p. 10)</u>

    a. The general rules governing the exercise of data subject rights

In general, we emphasise that while Article 20 introduces a new right, this right must be exercised in compliance with the conditions set out in Articles 11 (processing which does not require identification), 12 (transparent information, communication and modalities for the exercise of the rights of the data subject) and 13 (information to be provided where personal data are collected from the data subject) of the GDPR, and thus cannot burden the data controller in a disproportionate manner.

Moreover, the exercise of the right to data portability may be subject to the restrictions laid down in Article 23 (restrictions). We would ask the WP29 to issue further guidance regarding situations where a data portability request may be refused on the basis of such a

restriction. It would be helpful if examples are provided that give an insight into the instances where data cannot be ported on public policy grounds, such as for example the prevention against fraud or against attacks on the security and integrity of systems (under Article 23(d)), or member state economic interest (Article 23(e)). Those public policy grounds may override the individual's right to data portability.

Recommendation: Specify in the guidelines how the general rules governing the exercise of data subject rights should be applied, including the restrictions under Article 23.

b. How can the data controller identify the data subject before answering his request? (p. 11)

The guidelines state that '[t]here are no prescriptive requirements to be found in the GDPR on how to authenticate the data subject' (p. 11). Instead, the guidelines require controllers to implement an authentication procedure to "strongly ascertain the identity of the data subject", which may include asking for additional information for verification purposes in accordance with Article 12(6) of the GDPR. However, we note that there is no obligation for the controller to do so.

CIPL fully supports the requirement for authentication of the individual making a data portability request. The guidelines should further stress the need for security in making sure that the individuals' identity can be ascertained, especially when requesting for data to be transferred directly to another controller.

CIPL recognises that a data portability request should be met in a timely manner, but not at the expense of security. There is a danger that this right may be misused by bad actors to gain unauthorised access to valuable personal data. Data portability raises concerns regarding temporary unauthorised access to user accounts and data that may enable the download and copying of data. In our opinion, individuals should be able to control their data by disabling data portability features until further enabled and also features that delay authentication. We recommend that, in a dialogue with stakeholders, solutions are found allowing individuals to suspend or freeze the portability mechanisms with respect to their accounts if there is suspicion that the account has been compromised, and a delay feature to enable robust verification of identity of the individual making the data portability request.

Recommendation: Stress further the importance of data security in the context of the data portability right. Provide further guidance on implementation, taking into account the need for security to be balanced with the need for a speedy response.

c. What is the time limit imposed to answer a portability request? (p. 12)

The guidelines elaborate on the requirement in Article 12(3) GDPR that the controller should provide information on action taken on a data portability request, and must deal with the request within a month, or three months in complex cases (p. 12).

We note, however, that one month and even three months may not be enough in cases where a data portability request requires transfer of large sets of data into new technical formats in order to be compatible with the recipient controller's systems. We would ask the WP29 to recognise that there may be circumstances where a controller reasonably extends the three-month period and to specify these circumstances.

Recommendation: Recognise that there may be circumstances where a controller reasonably extends the three-month period and specify these circumstances.

d. In which cases can a data portability request be rejected or a fee charged? (p. 12)

CIPL supports the requirement that, generally, a request for data portability must be executed free of cost to the recipient in accordance with Article 12(5) of the GDPR. However, we emphasise that Article 12(5) further states that in cases of excessive or unfounded requests, the controller may charge a fee or deny the request. We ask that the WP29 clarify what kind of requests might impose a considerable burden to a controller and set general criteria for identifying excessive requests that require rejection or the charging of a fee. Examples of situations where a fee, or even a rejection of the portability request, would be reasonable include repeated or vexatious requests that require the transfer of large sets of personal data into a new technical format without presenting any added value to the individuals.

Recommendation: Further clarification that the exercise of the right to data portability at no cost must not be unreasonable.

4. How must the portable data be provided?

a. What is the expected data format? (p. 13)

CIPL welcomes that the WP29 explains the term 'interoperable' in Recital 68 of the GDPR by referring to a definition under EU law that defines it 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 organisations, through the business processes they support, by means of the exchange of data between their respective ICT systems.' We also welcome the clarification that interoperability is not the same as compatibility, but would welcome a clear statement that there is no obligation on the controller to provide data in a specific or common format (in accordance with Recital 68[3]).

Due to significant technical implication of the new data portability right, it is understandable that organisations have serious concerns over their ability to a) deliver this right in practice, b) technically enable download and porting of data, c) ensure that data portability is carried

[3] '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.' (Recital 68 GDPR).

out in common and expected format and in a way that is interoperable with the recipient and d) make the necessary system and process changes to enable the right to be fully effective from May 2018.

CIPL agrees with the objective that data portability should simplify the management of personal data by individuals. But how can we ensure that individuals are capable of managing their data in a practical manner if the ported data is selected from within a large data set? The individual may not wish to port all of his or her data, and may also wish that the sending controller retains a copy of the data.

The following are some specific challenges raised by the controllers:

- It is not clear from the guidelines what requirements for compatible formats (other than structured, commonly used and machine-readable) will be imposed on the controller to ensure interoperability with a receiving party. We would like the guidelines to clarify that although an Application Programming Interface (API)[4] could be a possibility, it is not a requirement. A simple word processing document or a spreadsheet would also meet the standard of Article 20, and we recommend a few more examples to that effect.

- There are technical challenges in relation to the individual's ability to select data, and we would welcome further guidance on standards for the implementation of this tool.

- The reference in the guidance to the definition of "machine-readable" formats in Recital 21 of the Directive 2013/37/EU is helpful, but not sufficiently specific. For instance, could it include open-source formats, ISO or other formats? These questions should be further explored in a multi-stakeholder process, as described below.

- The distinction between 'interoperable' and 'compatible' is not in all circumstances sufficiently clear. It may not be the format itself, but the technical implementation that will present a costly challenge for the controllers. It may not be realistic that data can be pulled together, especially where this may have to be done manually, within three months.

- It is not clear if unstructured data must be transferred into a machine-readable format for the purpose of complying with a data portability request, and if photos and images, such as passport pages (for verification purposes), are considered to be in machine-readable formats. The same issue arises regarding data held in enterprise legacy systems, or systems that were not originally designed with data portability in mind.

[4] As defined on p. 5 of the guidelines.

CIPL takes the view that the guidelines should be more explicit in recognising these challenges and should allow some flexibility to controllers in this respect, taking into account the time it takes to implement complex technological changes.

In these contexts, CIPL particularly welcomes the WP29's encouragement of '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.' We, therefore, propose that CIPL facilitate a roundtable or multi-stakeholder process on these issues.

Recommendation: Further clarification of the requirement of compatible formats. Support a roundtable or multi-stakeholder process facilitated by CIPL to discuss common sets of interoperable standards and formats to deliver data portability and to determine what obligations the data controller will have to transpose data held in legacy systems to fit the new technical format and what the threshold for 'common' will be.

b. How can portable data be secured? (p. 15)

According to the guidelines, 'the data controller should guarantee the "appropriate security of personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures" ' (Article 5(1)(f) GDPR) (p. 15).

Security is paramount for data protection and CIPL appreciates the WP29's recognition of the importance of adequate systems to ensure that data is not transmitted to an unauthorised party. Further, we note that the WP29 identifies particularly two areas that may be problematic in this regard: (a) 'how to ensure that personal data are securely delivered to the right person?' and (b) 'how to help users in securing the storage of their personal data in their own systems?'

We agree that these are areas of particular importance and therefore recommend further guidance as to the obligations of the sending controllers to ensure that the data is ported to the intended receiving controller or the individual. The guidelines consider that 'the data controller is responsible for taking all the security measures needed to ensure that personal data is securely transmitted (e.g. by use of encryption) to the right destination (e.g. by use of additional authentication information.' However, the guidelines do not consider the additional burden on the controller to develop and use such encryption. It does not consider either the acceptable standard of encryption to meet the legal obligation of security.

We have further concerns about allocating responsibilities to the sending controller in the instances where the individual asks for his or her data to be ported to another, but unverifiable, controller (based on the designation by the individual). The sending controller should not be required to refuse a data portability request based on the perceived inadequacy of the security systems of the receiving party.

Recommendation: Further clarify the obligations of the sending controller with respect to ensuring that the data is ported to a system that is secure.

Conclusion

Thank you for the opportunity to provide further comments on key implementation questions in relation to the data portability right. To the extent the WP29 decides to accommodate all or some of our suggestions, we would assume you would also update the associated Frequently Asked Questions. We look forward to providing further input on the data portability guidelines in the future as new issues arise, particularly in light of any practical experiences in applying the GDPR. In the meantime, please do not hesitate to contact us for further information or clarification at bbellamy@hunton.com; mheyder@hunton.com; and hhijmans@hunton.com.