21.

AMERICAN
CHAMBER of COMMERCE
IRELAND

American Chamber of Commerce Ireland

Comments pertaining to Article 29 Working Party Guidelines on GDPR implementation

European Commission

15 February 2017

The Right to Data Portability

The American Chamber of Commerce Ireland welcomes the guidelines set out by the Article 29 Working Party (WP29) on the right to data portability. The implementation of data portability will be beneficial to consumers and contribute to the development of the Digital Single Market.

The right to data portability should help to:

- Enable the free flow of data across the EU.
- Lower costs for consumers when switching services.
- Enhance competition in the market.

Given that companies have already recognised the market value of providing data subjects with the ability to download their data in a machine-readable format, WP29 guidance should strive to draw on existing best practices. Competition fostered through data portability should be supported by allowing companies the flexibility to develop their own standards to enable portability. One-size-fits all standards will impact competition by favoring the better-resourced companies able to design technically complex tools.

The intent of the provision is essentially that the data subject should have control of "their" data and the right to move it between service providers. WP29 guidelines and supporting uses cases make it clear that data portability is a consumer-oriented right: "This right, which applies subject to certain conditions, supports user choice, user control and consumer empowerment." Therefore, the foremost consideration should always be whether the data subject (consumer) has a legitimate interest to transmit the data to another controller. Data portability rights should only apply where such an interest exists.

Scope

- The American Chamber of Commerce Ireland welcomes WP29's clear distinction between the right to portability and the right of access (and other data subject rights) under the GDPR. However, guidance should more explicitly state that the right to data portability is narrower than the right to access, and data subjects may not need or want to port all data available to them.
- The Chamber welcomes WP29's recognition that the right to data portability is limited. This is reiterated by the following references:
    - The right to portability "does not include data that are exclusively generated by the data controller such as a user profile created by analysis of the raw smart metering data collected."
    - "Inferred data and derived data are created by the data controller" and do not fall within the scope of the right (e.g. algorithmic results).
- However, WP29 has adopted a very broad interpretation of data that a data subject has "provided":
    - Guidance suggests that "the right to data portability covers data provided knowingly and actively by the data subject as well as the personal data generated by his or her activity."
    - WP29 states that controllers must "include the personal data that are generated by and collected from the activities of users in response to a data portability request," for example, search history and location data.

- This scope is too broad for the following reasons:
    - Observed data is proprietary, just as inferred and derived data is, and should therefore be out of scope:
        - WP29 recognises that inferred data and derived data are not in scope for portability. The reason is to protect the IP rights of data controllers.
        - WP29 acknowledges that inferred data and derived data are created or enriched by the data controller on the basis of the data initially "provided by the data subject." WP29 further acknowledges that "provided by" includes personal data that relate to the data subject activity or result from the observation of an individual's behaviour, but not subsequent analysis of that behaviour.
        - This distinction does not appear to be practical:
            - The very questions or data fields asked by the data controller may be where the data controller applies innovation and trade secrets, particularly when these questions/data fields are responded to by a large number of data subjects.
            - Moreover, where the data is not actively provided by a data subject, but rather collected from the data subject's use of a service, this data is usually processed and analysed immediately and then stored in a way that provides value to the data subject and the data controller alike. This value is created by the data controller's analysis and processing of the data, similar to inferred data. Therefore, "observed data"— data collected from devices and the use of services should be considered out of scope, for the same reasons that inferred and derived data are.
        - WP29 describes search history and location data as examples of observed data. These are key examples of how value is created by subsequent analysis of "raw" user data. For example, a data controller may create a map to help users visualise their observed location data or may create a dashboard to help users navigate and sort through their search history on the site. The effort undertaken by the data controller to organise and derive meaning out of this data means this data is enriched and therefore proprietary to the data controller. As such, it should be out of scope of the right to data portability.
- WP29 suggests scope goes beyond what the text of the GDPR states:
    - Art 20 GDPR expressly limits the right to data portability to data which the data subject has "provided." This does not encompass "observed" data, which the controller has collected by implementing technical means, and where the data subject has taken no action.
    - Recital 63 confirms this view; it expressly states that the right to data access includes personal data which have been "collected". No such clarification is made for Art 20. Therefore, portability should be read as excluding data that is passively "collected" from users.

- WP29 suggests that "Data controllers should provide as many metadata with the data as possible at the best possible level of granularity":
    - This suggestion similarly goes beyond the text of the GDPR.
    - The metadata which businesses create often enables features that create value for its users. Therefore, WP29 guidance obliges businesses to transfer data that should be considered proprietary, similar to inferred and derived data.
- Businesses should have the freedom to offer people choice: The right to portability is designed to enable people to switch services with greater ease. However, not all information provided to one service is relevant to another. WP29 should therefore clarify that:
    - Controllers may choose to offer people technical means of selecting which information they want to transfer to another controller, rather than offering an all or nothing solution.
    - Receiving businesses may decide not to process all data they receive via a transfer from another controller, for example if the data set contains information that does not serve the purpose of enabling the consumer to switch services.
- The right to data portability is limited to data that is collected and processed on the legal basis of consent. If WP29 insists on crafting a broad scope of data included in the right – i.e. including all "observed" data — data controllers will be incentivised to rely on alternative legal bases to process data.

Security

- WP29 guidance suggests that "data controllers operating information society services are technically able to comply with requests within a very short time-period. To meet users' expectations, it is a good practice to define the timeframe in which a data portability request can typically be answered and communicate this to data subjects."
    - The American Chamber of Commerce Ireland recommends that WP29 guidance should take security considerations into account, as opposed to calling for speedy processing of portability requests.
    - Data portability features pose significant security concerns, because temporary unauthorised access to an account can be leveraged to permanently copy all information from the account.
    - Businesses need the ability to offer protections, such as controls that data subjects can use to disable data portability features, and the ability to delay fulfilling portability requests to authenticate the data subject invoking the right. Businesses should retain flexibility to determine the circumstances in which they need to authenticate users, based generally on a reasonableness standard.
- WP29 should acknowledge that strict security measures are necessary and not "obstructive in nature." Such security measures could include:

- The ability to disable portability mechanisms if there are reasons to believe an account might be compromised.

- Delayed provision of data upon a portability request to verify the identity of the data subject making the request.

Responsibilities of the receiving controller & third party data considerations

- WP29 guidance suggests that "all data controllers (both the 'sending' and the 'receiving' parties) should implement tools to enable data subjects to select the relevant data and exclude (where relevant) other data subjects' data. Additionally, they should implement consent mechanisms for other data subjects involved, to ease data transmission for those cases where such parties are willing to consent, e.g. because they as well want to move their data to some other data controller. Such a situation might arise with social networks."

    - The American Chamber of Commerce Ireland is of the opinion that these obligations go beyond Article 20. This article does not opine on the methods by which data controllers must provide or receive data, but instead leaves it to data controllers to determine the means that are most suitable for their specific services.

    - These practices should be market-driven; businesses should be free to build such mechanisms if such mechanisms would benefit their users/customers, and use it as a competitive advantage.

    - Many businesses already provide tools to select and exclude their data, or other subjects' data, from being ported to other services.

    - In addition, it's important to note that the guidance unfairly calls out social networks. Companies across many industries hold data that can be related to multiple data subjects simultaneously, and thus would be in a similar position to social networks in determining appropriate protections for third data subjects' rights.

- The guidance advises controllers to provide records in response to data portability requests even if they contain third-party data. WP29 requires the receiving party to identify an additional "ground for lawfulness of processing" of such third party data, e.g. legitimate interest, in particular where the household exception applies. Guidance should ensure that the receiving controller is not burdened with this requirement in cases where it was not required of the original controller.

- WP29 states that it is the receiving controller's responsibility to ensure that received information which is not relevant with regard to the purpose of the new processing, is not kept and processed.

    - WP29 should clarify that the deletion should be in line with the storage limitation principle in Article 5(1)(e), rather than "as soon as possible".

    - Data controllers should have the flexibility to offer data subjects the ability to manually exclude the data of third party data subjects and subsequently verify this action has been

taken. The data controller should then be able to rely on the data subject's verification that third parties' data has been excluded.

- WP29 states that the "new" data controller must clearly and directly state the purpose of the new processing before any request for transmission of the portable data.

    - It should be clarified that this obligation does not extend beyond the transparency requirements that already bind the new Controller under Arts 13 and 14.

- WP29's guidance suggests that a "receiving 'new' data controller (to whom the data can be transmitted at the request of the user) may not use the transmitted third party data for his own purposes e.g. to propose marketing products and services to those other data subjects. Otherwise, such processing is likely to be unlawful and unfair, especially if the third parties concerned are not informed and cannot exercise their rights as data subjects." It is unclear when this scenario would arise, given that Art 14 requires the new controller to notify third party data subjects within a reasonable period where the data has not been obtained from them. Moreover, it should be clear that the personal/household exemption (Art 2(2)(c)) should apply in these circumstances, meaning data subjects should be permitted to port the data of third party data subjects – and authorise the receiving data controller to use this data — if they would normally be able to do so with the original data controller under the personal/household exemption.

Format

- WP29 strongly encourages interoperability:

    - Per Recital 68, it should be acknowledged that the right to portability does not create an obligation for the controllers to adopt or maintain processing systems that are technically compatible with those of third parties.

    - Guidance should clarify that development of an API is a possibility, but not a requirement to honor the right to portability.

    - Guidance should clarify that formats such as common word processing and spreadsheet standards, can be compliant means of providing portability.

Identifying a Controller or Processor's Lead Supervisory Authority

Borderline cases

The American Chamber of Commerce Ireland acknowledges that WP29 has endeavoured to provide structure to the determination of an entity's main establishment.

However, the guidance appears to have exceeded the scope of the GDPR by asserting that "[c]onclusions cannot be based solely on statements by the organisation under review" and "[th]e burden of proof ultimately falls on controllers and processors." The text of the GDPR does not assign burden of proof to controllers/processors. The GDPR indicates that there should be an objective assessment of the facts pertaining to a controller/processor's main establishment, and therefore the controller/processor's

assertion of main establishment should carry a rebuttable presumption. Supervisory authorities may rebut this presumption upon an objective examination of the relevant facts, including requesting additional, relevant information from the controller/processor.

Supervisory authority concerned

The American Chamber of Commerce Ireland welcomes WP29's encouragement of cooperation among lead and supervisory authorities, in particular the goal of reaching mutually acceptable decisions with respect to substantive conclusions. Indeed, this is explicitly provided for in Article 60. However, the GDPR only provides for limited cooperation with respect to lead and supervisory authorities reaching mutually acceptable decisions on procedural matters. This cooperation is scoped to circumstances "where the lead supervisory authority and the supervisory authorities concerned agree to dismiss or reject parts of a complaint and to act on other parts of that complaint" (Article 60(9)). It does not, as WP29 suggests, include decisions about issuing a warning or a press statement. The guidance should make clear that, when in case of doubt, the lead supervisory authority's decision should prevail where it involves making procedural decisions to dismiss or reject part of a complaint.

Data Protection Officers ('DPOs')

Section 2.4 of the Guidelines, on Expertise and Skills of the DPO, states that in case of a service contract with an external DPO, each member of the team the external DPO assigns needs to be considered. Furthermore, "... individual skills and strengths can be combined so that several individuals, working in a team, may more efficiently serve their clients. For the sake of legal clarity and good organisation it is recommended to have a clear allocation of tasks within the DPO team ...").

This same approach should also apply for internal DPO functions, for example in the case of a complex international organisation where one individual couldn't meet all the skill requirements or the scope required by the role (including e.g. language skills).

General Comment

The American Chamber of Commerce Ireland strongly encourages WP29 to consult regularly and work closely with stakeholders, including industry when formulating guidance and rules on GDPR implementation. This should be a formalised process for an adequate period of time to allow for all stakeholders to engage their experts and provide expertise. A detailed consultation timeline would be helpful and welcome.