McCann FitzGerald
Solicitors
Riverside One
Sir John Rogerson's Quay
Dublin 2
D02 X576

Tel: +353-1-829 0000
Fax: +353-1-829 0010
Email: inquiries@mccannfitzgerald.com
Dx 31 Dublin
www.mccannfitzgerald.com

McCann FitzGerald

OUR REF	YOUR REF	DATE
PAL\25194796.1		31 January 2017

JUST-ARTICLE29WP-SEC@ec.europa.eu
presidenceg29@cnil.fr

McCann FitzGerald Comments on Article 29 Working Party Guidelines on the right to data portability; on Data Protection Officers ("DPOs"); and for identifying a controller or processor's lead supervisory authority

By Email

Dear Sirs

McCann FitzGerald is one of Ireland's premier law firms representing both Irish and overseas clients. The firm is owned by the partners and comprises some 71 partners and 350 lawyers and professional staff. It is based in Dublin (our principal office), London, New York and Brussels. The firm is widely recognised as a leader in the field of data protection law.

McCann FitzGerald has prepared these comments in response to the three sets of guidelines published by the Article 29 Working Party (**"A29WP"**) on 13 December 2016 on the right to data portability; on Data Protection Officers; and for identifying a controller or processor's lead supervisory authority (together, the **"Guidelines"**).

1. **General**

1.1 As a preliminary observation, the intended legal effect of the Guidelines seems unclear. If it is envisaged that they will be adopted by the European Data Protection Board (**"EDPB"**) as guidelines, recommendations, or best practice for the purpose of Article 70 of the General Data Protection Regulation (**"GDPR"**), which we assume to be the case, then we suggest that this should be clarified. If this is not the intention, then in the interests of legal certainty it would be helpful if the A29WP could clarify that the guidelines set out the recommendations and views of the A29WP but may not necessarily reflect how the GDPR will be applied.

2. Guidelines on the right to data portability

2.1 The guidelines state that for the purpose of this right the concept of data "provided by" the data subject includes "observed data"[1]. This is a very broad construction of the express wording of GDPR. While the guidelines suggest that this is consistent with the policy of the data portability right, it is notable that this interpretation is not supported by any express wording either in Article 20 or in the Recitals of the GDPR. If the data portability right had been intended to apply to "observed data", this should have been made explicit. The Art29WP's view on this point is likely to lead to uncertainty, as it is questionable whether a court would uphold such a broad interpretation.

2.2 The guidance regarding Article 20(4) GDPR[2] does not provide enough clarity as to how the data portability right should be balanced against the "rights and freedoms of others." In particular, it is not clear whether potential prejudice to the intellectual property rights of the data controller in "observed" personal data, or the way in which "observed" personal data was generated, might entitle a data controller to refuse to comply with a data portability right request under Article 20(4). As a further comment, the guidelines do not currently offer any meaningful guidance on how the provisions of Article 20(4) and Recital 63 should be interpreted with regard to third party intellectual property rights and this section would benefit from further examples of when this might apply.

2.3 The sections of these guidelines[3] that deal with situations where the data subject's data is mixed with personal data relating to third parties take a surprising approach to third parties' personal data. They state that data controllers should not take an overly restrictive interpretation of the sentence "personal data concerning the data subject" and that third party personal data (e.g. relating to other parties to telephone calls or banking transactions, etc.) should be provided to the data subject. While the guidelines indicate that the data subject should only be entitled to use such third party data for its own personal or domestic use and that any new receiving data controller would not be entitled to use the data for its own new purposes, this is likely to be difficult to control and would increase the risk of such third party data being misused, particularly since the data will be in automated form. It also seems an excessively broad approach, given that, in the context of data subject access requests, third party personal data should not be released without the third party's consent. To address these risks the guidelines suggest that data controllers should implement tools which allow the data subject to select the required data and exclude (where relevant) any third party personal data. This seems a risky approach, as it allows the data subject to assume practical control over third party data even though the data controller may still be legally responsible for the data.

3. Guidelines on Data Protection Officers ("DPOs")

3.1 The intended legal effect of the following statement is unclear:

---

[1] Section headed "Second condition: data provided by the data subject," pp. 8-9 of the Guidelines on the right to data portability

[2] Pp. 9-10 of the Guidelines on the right to data portability, particularly the section headed "With respect to data covered by intellectual property and trade secrets" on p.10

[3] Pp. 7-9 of the Guidelines on the right to data portability

> *"When an organisation designates a DPO on a voluntary basis, the same requirements under Articles 37 to 39 will apply to his or her designation, position and tasks as if the designation had been mandatory."*[4]

This statement seems misleading, as Articles 37 and 39 can have legally binding implications only for entities within the scope of Article 37. Entities that are outside its scope could be encouraged by the A29WP to comply with their provisions as a matter of best practice, but it is unclear how it is envisaged that Articles 37 and 39 could apply to them.

3.2 The intended legal effect of the last paragraph on page 5 is also unclear. The A29WP does not have the power to make "Data Protection Officer" or "DPO" a legally protected term. It is not clear what, if any, legal consequences are intended to arise if an organisation uses this term for a person who is not a "Data Protection Officer" for the purpose of the GDPR.

3.3 The guidelines regarding "large scale" processing in section 2.1.3[5] includes some very broad examples, such as processing of personal data by "an insurance company" or "a bank." The intended legal effect of this needs to be clarified, since it seems to suggest that all insurance companies and banks who process personal data relating to customers will be required to have a DPO, regardless of their scale or range of activities. Although some insurance companies might be obliged to have a DPO on the basis that they process health data (a special category of data) in relation to personal injuries claims, this might not be the case in respect of all insurance companies. For example, an insurance company specialising in property or non-medical professional negligence insurance would not necessarily meet the criteria in Article 37(1). With regard to banks, in particular, while some may process personal data on a large scale, we struggle to see why all banks should be automatically regarded as meeting the other requirements under Article 37(1)(b) (regular and systematic monitoring of data subjects on a large scale) or Article 37(1)(c) (processing on a large scale of special categories of data or personal data relating to criminal convictions or offences). While some of their activities may involve the types of processing referred to in Articles 37(1)(b) and (c) (e.g. anti-money laundering checks, health data provided in the context of mortgage forbearance proceedings, etc.) this may not always be the case and may not be done on a large scale or as part of a bank's core activities.

3.4 In Section 3.4,[6] one of the examples given of ways in which a DPO can be directly or indirectly penalised is the prevention of career advancement due to reasons related to his/her DPO activities. This appears to conflict with Section 3.5,[7] which seems to suggest that DPOs must be excluded from certain positions of senior management in an organisation (on the basis that such positions could result in the DPO being involved in determining the purposes and means of processing of personal data). This apparent conflict should be clarified.

4. Guidelines on identifying a controller or processor's lead supervisory authority

4.1 Under the heading "Substantially affects," the guidelines state: "Processing with little or no effect on individuals does not fall within the second part of the definition of 'cross-border

[4] P. 5 of the Guidelines on Data Protection Officers
[5] P.7 of the Guidelines on Data Protection Officers
[6] P.15 of the Guidelines on Data Protection Officers
[7] P.15-16 of the Guidelines on Data Protection Officers

processing.'"[8] This could be interpreted as implying that any processing that has anything more than "little or no" effect on individuals will come within the meaning of processing that "substantially affects" individuals within the meaning of the second part of the definition of "cross-border processing." This is potentially misleading as it gives the impression that processing that has anything more than a negligible effect on individuals in more than one Member State will be considered to be cross-border processing.

Yours faithfully

McCann FitzGerald

[8] P.3 of the Guidelines for identifying a controller or processor's lead supervisory authority