On 16 December 2016, the Article 29 Working Party (the **WP29**) published guidelines and FAQs on key implementation issues arising under the EU General Data Protection Regulation (the **GDPR**). The WP29 is an independent advisory body composed of representatives from data protection authorities of the Member States, the European Data Protection Supervisor and a representative of the European Commission. As part of its advisory role, the WP29 will provide guidance on the implementation of the GDPR.

The guidance issued concerns three important topics under the GDPR: (i) the right to data portability; (ii) data protection officers (**DPOs**); and (iii) the determination and role of the Lead Supervisory Authority. The WP29 published guidance and FAQs on each of these topics. The documents provide useful guidance for companies helping them to bring their processing activities into line with the GDPR by the time it applies: *i.e.*, on 25 May 2018.

In this note, we will discuss the guidance on the new right to data portability.

### 1. PURPOSE OF THE DATA PORTABILITY RIGHT

The right to data portability is one of the main and controversial new rights granted by the GDPR to data subjects. The right is intended to give individuals more control over their personal data. Importantly, the right will also have implications for competition and innovation. The WP29 explains that the purpose of the right to data portability is consumer empowerment. At the same time, the WP29 notes the right should foster opportunities for innovation and the sharing of personal data amongst controllers.

Article 20 of the GDPR, defines the right of data portability as follows:

> “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 WP29 opinion provides guidance on the implementation and interpretation of this new right to data portability. It helpfully clarifies the conditions under which the right applies. It furthermore provides concrete examples and criteria to illustrate the circumstances where the right will arise.
2. WHAT CAN DATA SUBJECTS REQUEST?

The WP29 distinguishes two elements of the right to data portability: (i) a right for data subjects to receive personal data processed by a data controller and to store it for their own personal use on a device; and (ii) a right to transmit personal data from one controller to another without hindrance. The WP29 cites the second element as fundamental to consumer empowerment and encouraging innovation in data portable technologies. Controllers must implement tools to ensure compliance as to both elements of the data portability right. The WP29 encourages controllers to not only offer direct download opportunities to the data subjects, but also to allow data subjects to directly transmit data to another data controller through an application programming interface (API).

3. OBLIGATIONS FOR DATA CONTROLLERS AND HOW TO PREPARE

If data are transferred from one service provider to be used for another service, the WP29 illustrates that both the transferring and the receiving service providers should ensure compliance with the GDPR. For instance, the transferring service provider will have to assess whether it can keep a copy of the data after the transfer. On the other hand, the recipient should determine whether the data provided are relevant and not excessive, with regard to that new data processing. The WP29 also outlines that the receiving organisation may become a new data controller. It consequently must clearly and directly state the purpose of the new processing before any request for transmission of the portable data is made.

The guidance also clarifies the conditions under which the right to data portability applies:

- **Consent or performance of a contract**: the right to data portability is only applicable if the legal basis of the data processing is the data subject’s consent or the necessity to perform a contract. As a consequence, the data portability right does not apply to data that have been processed with another legal basis, such as processing that is required by law, or for the legitimate interest of the controller;

- **Provided by the data subject**: the data portability right is limited to personal data provided by the data subject: The WP29 adopts a broad interpretation of ‘provided by the data subject’, suggesting that the right not only covers data actively and knowingly provided by the data subject (for example, by completing an online form), but also data provided by the data subject by virtue of the use of the controller’s services or devices (such as search history, traffic data, or location data). In contrast, the WP29 excludes from the right to data portability ‘inferred data’ and ‘derived data’ created by the data
controller on the basis of the data provided by the data subject, such as a credit score or analysis of the user’s health; and

- **Rights and freedoms of others**: the right to data portability cannot adversely affect the rights and freedoms of others. Controllers must assess whether the data includes information about third parties, and whether the transfer of this information could affect the third parties’ rights and freedoms. Controllers may need to exclude other data subjects’ data or implement consent mechanisms for other data subjects involved. The guidance indicates such issues are unlikely to arise with the transfer of bank account history, which will include data on other persons, provided that the transferred information is used for the same purpose (i.e., bank account history). If the information is to be used for a different purpose, such as a contact directory or for marketing purposes, the third party’s rights and freedoms are likely to be affected.

Finally, the guidelines clarify a number of obligations for data controllers to take into account when providing the right to data portability:

- Data controllers must inform the data subjects regarding the availability of the right to portability. Controllers should also include information about the right to data portability before any account closure;
- Data controllers must adopt procedures to identify data subjects wishing to exercise their data portability right;
- The procedures adopted by the data controller must ensure that the right is complied with “without undue delay” and in any case within one month of receipt of the request (this term may be extended to three months for complex cases);
- Data controllers are encouraged to ensure the interoperability of the data format provided in the exercise of a data portability request, and to include as much metadata as possible; and
- The data controller is responsible for taking all security measures necessary 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). Because of the risk that data subjects might request their data but then fail to keep it secure, controllers responding to portability requests should as best practice, recommend appropriate format(s) and encryption measures to help the data subject maintain security.

The WP29 guidelines on the right to data portability can be found [here](#). The FAQs can be found [here](#).