

Dear Members of the Article 29 Working Party

First of all, let us state our gratitude to the Art. 29 Data Protection Working Party for preparing and issuing the „Guidelines on the right to data portability“ (the “Guidelines”) which in many points provide for much needed clarification of issues concerning right to data portability, a new right of data subjects, provided for by the General Data Protection Regulation (the “GDPR”).

At the same time please consider and acknowledge our deep concern in regard to very broad concept of personal data, which should fall – according to the Guidelines – under the scope of the right to data portability. It is undisputed that right to data portability covers personal data provided to controller by data subject. At the same time it seems that term “provided” has been interpreted in Guidelines in a very broad way, without sufficient justifications to such interpretation to be found the GDPR.

As stated in art. 20 paragraph 1 of the GDPR : *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: [...].*

Across the GDPR text the need to respect and strengthen personal data subject’s intention, will, awareness and ability to make informed decisions is being emphasized and underlined. Thus the term “provided”, used in art. 20 paragraph 1 of the GDPR, should be understood and interpreted using the same set of standards as used to describe obligations of data controllers towards data subjects. Bearing this in mind, term “provided” in this context should be understood as an **intentional** action of data subject, and should mean that personal data provided to controller encompasses only such data which has been **intentionally** given by data subject to controller. This means, than personal data other than intentionally given to controller, especially data which is a by – product of the data subject activity while using a service provided by the controller, should not fall in any way in the scope of the right to data portability.

Unfortunately, we cannot agree with a broad interpretation of term “provided” presented in the Guidelines, resulting in broadening - way beyond the text art. 20 of the GDPR - the scope of data covered by the right to data portability. As stated in the Guidelines: *WP29 considers 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***. It means that the Guidelines proposes two categories of personal data covered by the right to data portability, namely: 1) data provided knowingly and actively by the data subject, and 2) personal data generated by his or her activity, hence the Guidelines create the second category of personal data which – unlike first category – are “provided” without data subject intention and awareness, which poses serious question: how data subject can “provide” his or hers data without his or hers intention and will. Such concept goes against the need to respect and strengthen data subject’s will, awareness and ability to make informed decisions, emphasized and underlined across the GDPR text. It is impossible to assume, on the grounds of the GDPR, that data subject, using for example social media service, is intentionally giving (i.e. providing) the controller (in this case service provider) data like time of connection, list of contacts, consumed content etc., which is merely a by-product of using such services.

It is symptomatic, that the Guidelines (page 8) uses quotation marks to describe provision of personal data in case of data which has not been given intentionally to controller (*Observed data are "provided" by the data subject by virtue of the use of the service or the device*), which shows that even authors of the Guidelines feel that such situations cannot be reasonably considered as providing personal data by the data subject to controller.

Concept presented in the Guidelines introduce ambiguity as to which personal data is covered by the right to data portability, and will cause in the future immense legal and practical problems, giving room to different interpretations and depriving data subjects and data controllers of highly needed legal certainty and ease while exercising the new right to data transfer. The Guidelines attempt – unfortunately unsuccessfully – to clarify the concept of unintentional “providing” of data, stating that *the terms “provided by” includes personal data that relate to the data subject activity or result from the observation of an individual’s behavior but not subsequent analysis of that behavior. By contrast, any personal data which have been generated by the data controller as part of the data processing, e.g. by a personalisation or recommendation process, by user categorisation or profiling are data which are derived or inferred from the personal data provided by the data subject, and are not covered by the right to data portability.* In case of most modern information society services and electronic communication services it will be very difficult, in some cases even impossible, to determine, which data *relate to the data subject activity or result from the observation of an individual’s behavior* and which data is a result of *subsequent analysis of that behavior*. By way of an example of future problems such interpretation may cause, let us draw your attention to art. 6 paragraph 2 letter (c) of the proposal for the Regulation concerning the respect for private life and personal data in electronic communications and repealing Directive 2002/58/EC (“Privacy and Electronic Communication Regulation”), which states that end-user’s electronic communication metadata may be processed by the provider of electronic communications services if end-user has given his or hers prior consent. According to the draft Regulation electronic communication metadata covers very broad set of data relating to end-user, concerning *inter alia*: data processed for the purposes of transmitting, distributing or exchanging content; data to trace and identify the source and destiny of the communication; data on the location of the device generated in the context of providing electronic communications services; date, time, duration and type of the communication. Taking under consideration the broad definition of personal data provided for in the GDPR, such electronic communication metadata could be considered personal data, processed on the grounds of consent. At the same time it would be very difficult to objectively distinguish electronic communication metadata which *relate to the data subject activity or result from the observation of an individual’s behavior* from electronic communication metadata which a result of *subsequent analysis of that behavior*. Furthermore, it would be very difficult to find legitimate interest of data subject to access, store and transfer such vast amounts of such detailed information about one’s usage of electronic communication services, not even mentioning the cost of implementing technical solutions allowing for portability of such data.

It is also necessary to emphasize, that such broad notion of personal data to be subject of right to data portability, presented in the Guidelines, pose serious risk to security of such data, when accessed, stored or transferred to data recipient. As presented in the Guidelines and in examples above, broad interpretation of term “provided” would mean, that data covered by right to portability could encompass also very detailed, very sensitive information about private life, financial situation, consumer preferences, race, political or sex orientation etc. While controller is obliged to protect

personal data, controller cannot guarantee the security of such data once data is transferred to data subject and stored by data subject. This may have adverse effect on data protection and privacy of data subjects, exposing sensitive personal data to risk of being accessed by unauthorized third party.

We would be delighted to answer any questions you may have so please do not hesitate to contact us: [REDACTED]

Sincerely yours

[REDACTED]
Chief Specialist in Legal Department
[REDACTED]

[REDACTED]
[REDACTED]
[REDACTED] Warszawa
Poland