23.

LIFE IS FOR SHARING.

Statement on the Guidelines on the right to data portability of the Article 29 Data Protection Working Party

In order to clarify the interpretation of the new right to data portability, the Article 29 Data Protection Working Party (WP29) has published an opinion on the respective provision laid down in Article 20 of the GDPR. The draft opinion contains highly problematic statements, due to the fact that the WP 29 tries to significantly extent the scope and aim of the given regulation. This contradicts the extensive process and the political discussions around the creation of the GDPR, while also creating new levels of legal uncertainty for companies and data subjects alike.

In detail:

1) The GDPR purposefully has narrowed down the personal data affected by the right to data portability to data „provided by" the data subject. This wording was chosen deliberately over "processed" personal data. The EU legislators have chosen this angle to avoid conflicts regarding the different rights of data controllers, data subjects an third parties while also creating an easy to execute right for the data subject. Any further interpretation contradicts this limitation. The WP 29 has neither the right nor mandate to arbitrarily broaden the scope of the GDPR.

2) The broadening of the scope to data ""provided" by the data subject by virtue of the use of the service or the device" would lead to insolvable problems for the data controller. From a technical point of view, most service providers do not have a separate data base containing only the raw data that can easily be separated from the algorithms to create profiles for customer analytics. Transferring this data to another service provider would in almost all cases give detailed background information about the technical setup of the original controller and the used algorithms. Therefore the very base of the controllers business would be revealed, essentially always tackling intellectual properties and trade secrets. Therefore, most data controllers can only provide data that is not affected by these concerns, linking back to the original language of Article 20 of the GDPR (data provided by the data subject, not data by virtue of usage).

3) The burden on the new data controller to analyze the data provided by the data subject in terms of whether it contains information that goes beyond the consent or contractual obligations is overly cumbersome and creates legal uncertainties. If the data is not covered by the consent given by the data subject or contractual obligations, the controller has no right to process such data. Since processing starts with the saving of data, the inspection of the data by the controller would already be illegal. Especially with regard to telecommunications data such as traffic and location data where a processing based on legitimate interests is not allowed. In addition, the

described practice to hand over full sets of data to further investigate whether all the data points are actually needed is very alarming from a data privacy perspective.

4) Especially for electronic communication data with legal deletion obligations, the right to data portability creates a myriad of legal uncertainties. In case of traffic and location data, it is totally unclear what the implications for the data subject and the new data controller are, given the obligation to delete respective data according to the ePrivacy directive. In addition, the porting of traffic data always tackles the right of third parties. This would be a clear violation of section 4 of Article 20.

5) The WP 29 has the right to encourage the development of common standards and interoperable systems creating easy ways to enforce the right to data portability. However, it must be made clear that this cannot mean an establishment of open API layers until the GDPR will enter into force. Technical standards are surely challenging to achieve and their development will take time and effort from many parties involved, including supervisory authorities and public entities.

In conclusion:

Any interpretation of Article 20 should stick closely to its wording, in order to not contradict the intention of the European legislator:

"data provided to a controller":

- → means only the data which the data subject controls and accesses on its own (e.g. photos, emails) during the performance of the contract.
- → does not mean usage data and necessary data for the conclusion of the contract.

the controller is not obliged to provide any data, which has been generated automatically by the service while the data subject is using the service (e.g. logfiles, traffic or location data).