13.

ČESKÁ BANKOVNÍ ASOCIACE
CZECH BANKING ASSOCIATION

Comments of the Czech Banking Association on the WP 29 Guidelines on data portability

General observation:

We welcome and appreciate the effort of the WP 29 to further explain and interpret the selected provisions of the General Data Protection Regulation (GDPR). On the top of that, we consider it as a necessary precondition for removing the high level of legal uncertainty generated by the GDPR and a precondition for any GDPR implementing projects of the personal data controllers.

However, in our view, the interpretation provided by the Working Party 29 (WP 29) and contained in the WP 29 draft opinion on the data portability is on a wrong track. Openly said, it contradicts Article 20 of the GDPR which establishes rules for the data portability. We regard the use of such greatly extensive interpretation by the WP 29 as a dangerous circumventing of the elementary principles of the European law as well as of the legislative process, a denial of the principles of legitimate expectations and – from the perspective of legal certainty – as a very negative signal for the efforts on the implementation of the GDPR requirements. Should the meaning of the individual provisions of the GDPR continue to be altered in this manner it would be practically impossible to rely on another legal opinion than on the opinion of WP 29 or on the decision of the ECJ. In the end, both make it unfeasible to implement the requirements of the GDPR on time.

Moreover, the new interpretation of WP29 substantially changes the impacts of the provision in question and paradoxically significantly increases the legal uncertainty. In practice, it would be very difficult to decide, which personal data processed by the data controller are data generated by the activity of the data subject (observed data). The WP 29 interpretation would extremely increase the complexity of the solution enabling the data portability the way WP 29 imagines, it would multiply the costs for the development of the solution without creating a corresponding and adequate added value for the customer and there is no assurance that all this would be functional. It would also lead to completely new risks for the data subjects in terms of security. Moreover, the principle of rendering services free of charge means a totally disproportionate interference into the fundamental principles of the freedom of enterprise.

Another important aspect is, that the WP 29 wide concept of the data portability contradicts the rules for switching a payment service provider stipulated in Chapter III of the EU Directive 2014/92/EC on the comparability of fees related to payment accounts, payment account switching and access to payment accounts with basic features and with the provisions of the PSD 2 - EU Directive 2015/2366/EC on payment services in the internal market introducing the new service – account information service. Those provisions on switching and on account information service fully satisfy the need to enable and easy the customer mobility within the sector and introduce relevant safeguards.

Personal data provided by the data subject

We have fundamental objections to the interpretation of the term "personal data provided by the data subject" to which the right to data portability relates. WP 29, without sufficient reasoning and rather arbitrarily, states that the term must be interpreted broadly (page 8).

Although the linguistic meaning of the term "personal data provided by the data subject" is rather unambiguous WP 29 includes not only data which have been provided by the data subject to the data controller in it but also "data generated by the activity of the data subject" while this broadened term is further widened in the interpretation provided by WP 29 to include also data which are generated by the activities of the controller i.e. data which have been generated as a result of a service rendered by the controller. A typical example of broadening the term "personal data provided by the data subject" is the opinion of WP 29 that the right to portability relates to data from the history of a bank account. Data relating to account history are basically data of payment transactions. However, personal data of payees (recipients of the payments), let alone personal data of payers who send financial funds to a bank account, cannot be regarded as personal data relating to the data subject under any circumstances (such data are not provided to a controller by the data subject - account owner - at all). Although the regulation speaks in Article 20(1) explicitly about the "personal data concerning the data subject" WP 29 in its interpretation rather arbitrarily widens this term to include the personal data of third persons (personal data of beneficiaries or payers). Also information on effecting a payment transaction provided to the controller by the data subject cannot be regarded as personal data concerning the data subject as such information is a result of the activity of the controller (i.e. result of a service rendered).

We should not forget to mention in this connection Directive PSD 2 which introduces a new service of providing information about the account based on which the payment service provider administering a payment account shall provide account information to a provider of account information services. The provider of account information services shall be a regulated subject which will have to obtain a license from the relevant regulator and shall have to observe the strict rules of secure communication with the payment service provider administering the account. The extensive interpretation of WP 29 basically liquidates the legal regulation of account information services because in accordance with the interpretation of WP 29 the payment service provider administering the account would have to transmit all information about the payment account to any controller irrespective of whether the controller in question shall be subject to any regulatory or prudential supervision. The interpretation given by WP 29 thus not only undermines the institute of banking secrecy but also fundamentally reduces data security and data protection in the area of payment services. The risks for the data subjects connected with this interpretation are obvious.

In accordance with the interpretation of WP 29 the right to data portability thus relates not only to the personal data of the data subject requesting the transfer of personal data but broadens this right also to the personal data of third data subjects. It thus fundamentally jeopardizes and

interferes with the rights of third data subjects and the result of the interpretation given by WP 29 would be an uncontrolled flow of personal data of third subjects among various controllers.

The broadened interpretation of WP 29 jeopardizes and interferes with such rights of third persons as trade secret or intellectual property right. In its interpretation WP 29 puts the right of the data subject to data portability in a position of a right which stands above the other rights of third persons and takes precedence over them. We therefore regard as unacceptable that the right to data portability should relate not only to the personal data of a data subject which he or she solely provided to the controller but also to personal data of third data subjects and even to such data which have not been provided to the controller by any data subject requesting data transfer (for instance the data of payers in the case of bank accounts) and also that the right to portability should relate also to data which are the result of the activity of the controller, or a result of service rendered by a controller (for instance information about a payment transaction which has been effected) + portability only within the controller rendering the same services and carrying out business based on the same license/ authorisation (bank / to a bank, telephone operator – to a telephone operator, Facebook to Twitter, etc., or the controller should be given a possibility to judge whether the transfer corresponds to the purpose in question.

We are of the opinion that it is not possible to interpret provisions of a legal norm in an extensive manner which not only departs from the authentic text of the legal norm, which is clearly in contradiction to the purpose of other legal rules (PSD 2), which would thus lead to a conflicting interpretation of the law, but which moreover interferes with the rights and legally protected interests of third persons and jeopardizes in its consequences also the interests of the data subjects whose alleged benefit this interpretation should serve.

The format of data transfer

We think that WP 29 again goes beyond the framework of GDPR in terms of the format of data transfer that it is requesting. In our view Article 20 cannot be interpreted in a way that the data subject could select one of the formats of data transfer. On the contrary, the requirement of the GDPR will be met where the data controller has at its disposal a transfer format which would comply with the basic requirements stipulated in Article 20, paragraph 1. It is in contradiction with the GDPR that the controller should be required to create API or special download mechanisms enabling selection of a format in which the data would be transferred.

Opinion provided by WP 29 on the lead supervisory authority

What impact does this opinion have on large financial groups which have their parent company outside the territory of the Czech Republic (CR)? These businesses in the territory of the CR (although owned by parent companies outside the CR) have independent legal personality and the Board of the business in question is responsible for the decision-making. Does it mean that the regulator in the country of the parent company may supervise the subsidiary entity in another EU State? If the answer is "yes" than in which cases?

Provisions of Article 55 GDPR are ambiguous also from the perspective of cross-border provision of services operating on the basis of a principle of a single licence. Does this automatically imply that the Office for Personal Data Protection is a lead supervisory authority where a bank with its Seat in the CR provides its services in another Member State through a branch and for these purposes processes personal data of persons from a Member State other than the CR?

Where a bank provides services in another Member State without opening a branch based on a principle of a free movement of services we expect that it is necessary to carry out a test of the "significant impact" on data subjects. A large quantity of data is processed as part of the provision of banking services (account transaction data, data related to credit rating and credibility in the case of a credit). Does this mean that the "significant impact" exists here? How should one take account of the fact where most personal data are processed for more purposes and where one of them is complying with a legal obligation? Will the scope of activity then be split for concrete purposes between the Czech supervisory authority and the supervisory authority of another Member State?