Opinion of Deutsche Telekom AG concerning the evaluation and review of the General Data Protection Regulation by the EU Commission pursuant to Article 97 GDPR

The General Data Protection Regulation has created a good basis for data processing in the non-public area in the European Union, based on a set of uniform rules.

Experience so far has shown, however, that the intended harmonization and the intended "level playing field" are at risk. This is why, based on the experiences of Deutsche Telekom Group, some amendments to the Regulation (I) and improvements in the consistent application of the existing rules (II) are required.

I) Need for regulatory action

1) Consistency mechanism is not used – no consistent application of the Regulation

Request: The consistency mechanism has to be obligatory in respect of any matter of general application or producing effects in more than one Member State. The urgency procedure referred to in Article 66 GDPR must be used more often.

Actual situation: Unclear legal definitions are interpreted differently by different supervisory authorities (e.g., data portability, scope of right of access, etc.). This is contrary to the harmonization objective of the General Data Protection Regulation. National data protection supervisory authorities sometimes issue instructions without making clear whether these are permanent or whether they should be handled in the consistency mechanism and then canceled.

Problem: The failure to take the consistency mechanism into consideration leads to legal uncertainty for both industry and citizens. Moreover, the different interpretation has a considerable financial impact because business models and processes cannot be implemented uniformly across Europe.

Solution: Article 64 (2) GDPR is worded as follows:

*"Any supervisory authority, the Chair of the Board or the Commission ~~may~~ request **within a reasonable period** that any matter of general application or producing effects in more than one Member State be examined by the Board with a view to obtaining an opinion, in particular where a competent supervisory authority does not comply with the obligations for mutual assistance in accordance with Article 61 or for joint operations in accordance with Article 62."*

In addition, the urgency procedure as laid down in Article 66 GDPR should be applied more often.

2) Company-specific divergent interpretation, depending on where the company is established – standardized enforcement

Request: The consistency mechanism must be obligatory for the evaluation of similar business models operated by different companies established in different Member States.

Actual situation: In terms of enforcing compliance with the GDPR, supervisory authorities are not strictly required to use the consistency mechanism laid down in Article 63 GDPR et seq., even if it is a matter of general application or producing effects in more than one Member State.

Problem: It is possible for national supervisory authorities to make decisions regarding the enforcement of compliance with the GDPR in the area of their competence, which differ from decisions made in other Member States on similar matters. This applies above all to different companies of the same sector in different Member States (e.g., internet service provider X is treated differently in country A from internet service provider Y in country B). This puts the harmonization objective of the General Data Protection Regulation at risk and results in considerable legal uncertainty for both industry and citizens. Different decisions may have a considerable impact on the cost-effectiveness of business models and could therefore also compromise the intended "level playing field."

Solution: Article 64 (2) GDPR is worded as follows:

*"Any supervisory authority, the Chair of the Board or the Commission ~~may~~ request **within a reasonable period** that any matter of general application or producing effects in more than one Member State be examined by the Board with a view to obtaining an opinion, in particular where a competent supervisory authority does not comply with the obligations for mutual assistance in accordance with Article 61 or for joint operations in accordance with Article 62."*

3) Scope of the right of access under Article 15 GDPR – handover of documents

Request: Clarification that Article 15 GDPR refers only to the information specified in Article 15 GDPR and that data subjects do not have the right to request copies of documents on which that information is based.

Actual situation: In some cases data subjects not only ask for information on and copies of their personal data, but also request copies of the original documents on which these data are based.

Problem: This raises the question of distinction between this right and other rights, such as per Article 20 GDPR and rights to request the handover of documents under public law, criminal law, civil law, and labor law in particular. Article 15 GDPR must not become an across-the-board right to information that replaces other rights. This would be a way of bypassing legal requirements and mechanisms for balancing different interests that have to be applied in other processes of information disclosure.

Solution: insert the following sentence after the sixth sentence in recital 63: *"That right does not include the handover of copies of original documents."*

4) Scope of the right to data portability, Article 20

Request: Clarification that the right to data portability does not include data generated automatically by the service when it is used by the data subject (e.g., log data, traffic or location data).

Actual situation: Article 20 GDPR gives the data subject 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.

Problem: In guidelines issued by supervisory authorities the term "provided" is very broadly interpreted. According to such guidelines, the term also includes data generated when a service is performed in an IT system or, for instance, in the network technology of a telecommunications network. Although these data are required in order to operate a telecommunications network, they are not actually provided by the data subject. While it would take the service provider a considerable amount of time and effort to hand over such data to the data subject, they would be of no benefit to the latter if, for instance, he or she wanted to change providers. Moreover, this broad interpretation loses sight of the fact that the legislator has deliberately decided to use the term "provided" by the data subject. In the legislative process, the legislator expressly decided not to extend the right of data portability to all processed personal data, regardless of whether they were provided by the data subject or not. The starting point was to enable the data transfer of the "history" from one social network to another.

Solution: Insert the following sentence after the first sentence in recital 68: *"Data that are created automatically when a service is used and that are by-products of using that service (e.g., log files, traffic or location data) are not considered data provided by the data subject."*

5) Notification of a personal data breaches

Request: Limitation of notifiable personal data breaches by introducing clear materiality thresholds.

Actual situation: As a result of the changed legal definition of a data privacy incident, increasing sensitivity among employees in the companies, and the new framework for sanctions available under the GDPR, the number of reported data breaches has increased. The notification obligation is only not applicable in cases where the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons.

Problem: The application of the undefined legal term "risk" results in considerable legal uncertainty. To avoid mistakes that may incur penalties, all incidents are reported if in doubt, regardless of the risk potentially associated with a personal data breach. This sharp increase in data breaches, which may potentially be notifiable, constitutes an excessive burden on companies and authorities without improving data protection.

Solution: Insert the following sentence after the second sentence in recital 85: *"Where the personal data breach concerns special types of personal data, personal data that are subject to professional secrecy, personal data related to criminal or administrative offences or to suspected criminal or administrative offences, personal data related to bank and credit card accounts or authentication data such as passwords or similar codes which are not publicly accessible, then it should be assumed that a risk to the rights and freedoms of natural persons is likely to exist."*

6) Media disruption in data privacy information

Request: Clarification that a media disruption in data privacy information is permissible under certain circumstances

Actual situation: Pursuant to Article 13 GDPR, data privacy information must be provided to the data subject at the time when personal data are obtained. The information specified in Article 13 GDPR is very comprehensive.

Problem: Where data is collected, e.g., when entering into a contract over the phone, the data privacy information would have to be read out or a recorded message played at that very moment. Since Article 12 (1) GDPR requires that this information is provided in an easily accessible form, it is not clear whether what is known as a media disruption, i.e., for instance, a reference to privacy notices available online, is acceptable.

Solution: Insert the following sentence after the first sentence in recital 58: *"It should suffice for such information to be, if not directly accessible, at least retrievable without effort."*

7) Record of categories of processing activities pursuant to Article 30 (2) GDPR

Request: Where the same category of processing activities is performed on behalf of a large number of controllers (≥ 1,000) it will suffice, in order to complete the record referred to in Article 30 (2) GDPR, to submit upon request by the supervisory authority the full list of names and contact details of the controllers within a reasonable period.

Actual situation: The processor must maintain a record of the categories of processing activities including the names and contact details of each controller on behalf of which the processor is carrying out the processing activities.

Problem: In the case of mass market products (e.g., cloud solution for business customers), a separate entry must be made in the record for each customer although the category of processing is always the same. In addition, the record must be continually updated due to changes in the customer base. The result may be several thousand entries for one and the same category of processing activities. This is not only prone to error, it is also a case of duplicate record keeping, with the same data being kept in customer data systems.

Solution: Insert the following sentence after the second sentence in recital 82: *"If categories of processing activities apply to more than 1,000 controllers, it is sufficient that the processor provides the details regarding the controllers upon request by the competent supervisory authority within a reasonable period."*

8) Commissioned data processing, deletion or return of data, Article 28 (3) (g)

Request: Due consideration must be given in a contract on commissioned processing of data to the question of technical feasibility with regard to the controller's choice as to whether the processor is to delete or return all the personal data to the controller after the end of the provision of his processing services.

Actual situation: A contract governing the processing of data by a processor must stipulate, among other things, that the processor, at the choice of the controller, deletes or returns all the personal data to the controller after the end of the provision of services relating to processing, and deletes existing copies.

Problem: Due to the technical implementation of the processing services it is, in certain cases, not possible to offer the choice of either deleting or returning the data. However, pursuant to Article 28 (3) (g) GDPR this choice must be stipulated in the contract on commissioned data processing.

Solution: Article 28 (3) (g) GDPR is worded as follows: *"at the choice of the controller, deletes or returns all the personal data to the controller* ***taking account of the type of data processing and the technical feasibility,*** *after the end of the provision of services relating to processing, and deletes existing copies unless Union or Member State law requires storage of the personal data."*

II) Consistent/adequate interpretation and application

1) Abuse of the right of access under Article 15 GDPR

Request: The abusive incentive to exercise rights of access is prohibited.

Actual situation: There has been a sharp rise in the exercise of the right of access laid down in Article 15 GDPR. Requests to Deutsche Telekom have doubled since May 25 and more than tripled during the introduction period.

Problem: A significant portion of the information requests is made by professional providers who motivate data subjects to exercise their right to information. It is often in their commercial self-interest in relation to the controller that these providers are trying to instigate as many information requests as possible.

Solution: Statement issued by the European Data Protection Board that the incentive to exercise the right to information given by providers acting in their commercial self-interest is an infringement of the principle of data avoidance and/or data minimization and must be prohibited.

2) Developed procedures called into question – anonymization

Request: The established practice of anonymization of personal data for the purpose of their further processing, which was previously permitted by law, continues to be possible.

Actual situation: The anonymization of personal data for the purpose of further processing these anonymized data has so far been established practice and agreed with the data protection authorities. Business models based on this are commercially successful.

Problem: The anonymization of personal data for the purpose of further processing these anonymized data is called into question as a result of the GDPR's purportedly new definition of the term 'processing.' However, this definition is no different to the definition provided in Directive 95/46 EC.

Solution: The definition of processing provided in Article 4 (2) GDPR is the same as the definition of processing given in Article 2 (b) of Directive 95/46 EC. The European Data Protection Board should make clear that an anonymization which was permitted under Directive 95/46 EC continues to be permissible under the GDPR. Procedures established and used until now should be reviewed with care and good judgment, and this evaluation should take into account in particular the continuation of regulations from Directive 95/46 EC under the GDPR.

3) Clarification of the scope of legal grounds for processing

Request: Clarify the scope and relationship between the 3 legal grounds for processing such as **performance of a contract**, processing necessary for the purposes of the **legitimate interests** pursued by the controller and **consent**.

Actual situation: Currently processing of personal data in comparable scenarios is conducted on different legal grounds depending on the legal interpretation of the respective controller. Guidance of the Data Protection Authorities is missing.

Problem: Processing of personal data in comparable scenarios on different legal grounds hampers harmonization under the GDPR and produces legal uncertainty for controllers. Controllers have to take into account very different requirements depending on the respective legal ground for processing. It is unclear where the purpose of processing covered by performance of a contract ends and the necessity for consent or legitimate interests begins.

Solution: Statement issued by the European Data Protection Board giving guidance for controllers on the scope of legal grounds for processing provided for in the GDPR, especially regarding **performance of a contract**, processing necessary for the purposes of the **legitimate interests** pursued by the controller and **consent**.