3 Erasure of Personal Data

3.1 The right to be forgotten

If pseudonyms are generated and assigned to a unique personal identifier (mapping) and this assignment of a PSN-Value relationship is deleted (virtual anonymisation), no more conclusions about the identity of a person can be made within the TTP.

Does this procedure correctly implement the right to be forgotten?

The term "right to be forgotten" is often used without taking into account the differences to the general right to erasure. While the right to erasure is intended to ensure that data is not unlawfully processed by a particular data controller, the right to be forgotten addresses the special constellation of published data that can easily be found on the Internet via search engines worldwide. In its landmark ruling of 13 May 2014 (Google Spain), the European Court of Justice (ECJ) established the right to be forgotten as the right of a data subject to demand the deletion of personal search results (de-listing) from the operator of a search engine under certain conditions on the basis of Art. 7 and 8 Charter of Fundamental Rights of the European Union and from Art. 12 and 14 of the Data Protection Directive.[9] Under the GDPR the 'right to be forgotten'

9 EuGH Urt. v. 13.5.2014 – C-131/12, BeckRS 2014, 80862; ECLI:EU:C:2014:317.

as an aspect of the right to erasure is laid down in Article 17 GDPR which is overwritten with "Right to erasure ('right to be forgotten')".

In a first step Article 17 para. 1 GDPR lists groups of cases in which personal data of the data subject must be erased. As a second step Art. 17 para. 2 GDPR provides: Where the controller **has made the personal data public** and is obliged (pursuant to Art. 17 para. 1 GDPR) to erase the personal data, the controller, taking account of available technology and the cost of implementation, shall take **reasonable steps**, including technical measures, **to inform controllers** which are processing the personal data that the data subject has requested the erasure by such controllers of any **links to, or copy or replication of, those personal data**. Finally, Article 17 para. 3 GDPR contains exceptions to the obligations set out in paragraphs 1 and 2.

One can say that there is no comprehensive right to be forgotten in the GDPR. There is only a deletion duty according to Article 17 para. 1 GDPR and an information duty towards third parties who process this published data according to Article 17 para. 2 GDPR. The latter is specifically tailored to the online environment (see recital 66). Article 17 para. 2 GDPR precedes the more general regulation of the Article 19 GDPR according to which a general "Notification obligation regarding rectification or erasure of personal data or restriction of processing" exists. Art. 19 GDPR states:

> *"The controller shall communicate any rectification or erasure of personal data or restriction of processing carried out in accordance with Article 16, Article 17 (1) and Article 18 to each recipient to whom the personal data have been disclosed, unless this proves impossible or involves disproportionate effort. The controller shall inform the data subject about those recipients if the data subject requests it."*

Considering the above-mentioned remarks, it becomes clear that the question does not concern a case of the "right to be forgotten" in the sense of the obligation to inform, but rather directly concerns the erasure claim according to Article 17 para. 1 GDPR. Under normal circumstances, a TTP will not publish any personal data and, most importantly, will not publish it on the Internet.

The question of the correct implementation of erasure of data and whether the virtual-anonymisation described above can suffice is answered in Part II.6.

3.2 Erasure of Personal Data in backups

> *Data are regularly part of incremental or complete backups or dumps, which are written on tape as a series that partly rotates with a long cycle (years). Backups are generally encrypted. In the case of withdrawals or deletion requests, how do we deal with the fact that it is almost impossible to clean all series and databases in backups? Please develop and suggest a data protection compliant procedure model for this.*

The obligation to erase personal data derives from Article 5 para. 1 lit. a), b), e) GDPR and Art. 17 GDPR. If one of the grounds set out in Article 17 para. 1) GDPR applies, the personal data of the data subject has to be erased by the controller. As a rule data copies that are created during data backup must be taken into account during erasure. If the data is erased in the active system operation, it must also be erased promptly in the backup and in other backup media, regardless of how many backups are available.

However, according to Article 17 para. 3 GDPR the right of erasure of personal data shall not apply to the extent that processing is necessary for

- exercising the right of freedom of expression and information,
- compliance with a legal obligation which requires processing,
- reasons of public interest in the area of public health,
- archiving purposes in the public interest, scientific or historical research purposes or statistical purposes and
- the establishment, exercise or defence of legal claims.

None of these exceptions apply in the case that is to analyse here and the right of erasure is granted **unconditionally**. Despite that, Article 23 GDPR allows the Member States to enact further restrictions to the right to erasure, which the German legislator made use of in **Section 35 BDSG**. According to this, the data subject shall not have the right to erasure, if in the case of **non-automated data processing** erasure would be impossible or would involve a **disproportionate** effort due to the specific mode of storage **and if the data subject's interest in erasure can be regarded as minimal**. In this case, the controller only has to make sure that the requirements of Article 18 GDPR (restriction of processing) are met. As described in the question, it can very well be argued, that Section 35 BDSG is applicable. Though we have to point out that this Section has been discussed controversially and the National Data Protection Board (Datenschutzkonferenz—DSK) has expressed doubts about the conformity with European law.

We therefore suggest to implement procedures to make sure that the right to erasure can be guaranteed in the future: IT-systems processing personal data should be designed in such a way that individual data sets can be identified and deleted in all redundancies. Since the purpose of a security backup can only be fulfilled if deletions in the active system are not immediately effective in the backup system, a deletion concept should specify the intervals at which deletions also affect backups. In the event of data recovery, data may be restored to systems where it was previously erased. In this case, the data must be erased again immediately. It must also be ensured that the backup copies are only used for system recovery purposes. A concept on erasure should specify the intervals at which deletions are transferred to backups. The concept on erasure should become part of the general data protection concept and include the essential considerations for justifying the design of the erasure process. The person concerned must be informed about the fixed erasure periods according to the obligations under Articles 13, 14 GDPR.