Concepts for data erasure and how to implement them

Erasure of personal data requires a well-planned approach. After all, the right data should be erased at the right time and in the right place.

A white paper by Stefan Hessel, LL.M. and Christina Kiefer, LL.M.

Status: 04/2023

Risks with no data protection-compliant erasure

The regular erasure of personal data is one of the basics of data protection compliance. Especially for companies with a large amount of data and an IT infrastructure that has grown over the years, data protection-compliant erasure is a considerable challenge. It is not sufficient to erase personal data at the request of the data subject. The General Data Protection Regulation (GDPR) requires storage limitation and thus regular erasure. Failure to erase personal data can result in severe fines or claims for damages. In addition, old data that are ripe for erasure jeopardise data quality and thus become an obstacle to the data-driven digitalisation of a company. The larger the data stock, the greater the risk that data protection breaches or IT security incidents will result in fines and/or claims for damages.

The data erasure concept

In order to properly comply with the obligations under the GDPR, companies are in need of an erasure concept. This follows from the fact that the GDPR establishes the principle of storage limitation and accountability. According to the GDPR, the controller may only store personal data in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data are processed. The accountability principle in Art. 5 (2) of the GDPR says that the controller must demonstrate compliance with the principles. It is recognised that this can be done by creating an erasure concept.[1] In cases where companies have not been able to present an erasure concept, the data protection supervisory authorities of various European countries have already imposed fines in the past.[2]

There are various models that can be used as a guide when developing a corresponding concept: for example, DIN 66398 "Guideline for the development of concept for data deletion with derivation of deletion periods for personal identifiable information", which still refers to the legal situation under the German Federal Data Protection Act (BDSG), but which has proven itself in practice and can be transferred to the current legal situation.[3] However, such schematic specifications can only be the starting point for the development of an erasure concept. The individuality of the company concerned must be taken into account.

[1] *Voigt*, in: Taeger/Gabel, DSGVO - BDSG - TTDSG, Art. 5 GDPR, para. 34.
[2] Instead of all: News report: Danish SA: fine proposed for Danske Bank, available at: https://edpb.europa.eu/news/national-news/2022/danish-sa-fine-proposed-danske-bank_de, last retrieved: 03/04/2023
[3] *Voigt*, in: Taeger/Gabel, DSGVO - BDSG - TTDSG, Art. 5 GDPR, para. 35.

The aim of an erasure concept is to ensure an orderly process flow through clear specifications and instructions so that no important aspects are overlooked at the time of erasure.[4] Another advantage is that a clear erasure concept relieves data protection officers in the company, as they no longer need to be consulted in standard cases.[5]

The erasure concept should not stand in isolation next to other processes. Ideally, it should be coordinated both with data erasure as a reaction to any erasure requests according to Art. 17 (1) of the GDPR and with an authorisation and role concept.[6]

What data need to be erased?

The first step in developing an erasure concept is to identify the personal data that are processed in the company. Different types of data can be differentiated based on the purpose of the data processing and allocated to specific data objects. An example of a data type would be accounting data, to which accounting records and invoices as well as payment transactions with banks are allocated as data objects.[7]

Time limits for erasure

Once the personal data have been identified, the time limits for erasure must be determined. If the principle of purpose limitation were applied strictly, personal data would have to be erased immediately at the moment the purpose ceases to exist. This would pose an insurmountable task for companies managing large data stocks. Recital 39 to the GDPR states that the controller should establish time limits for the erasure of personal data or periodic review. This means that a certain degree of schematisation in the form of periodic review may be sufficient. The time limits for erasure depend last but not least on the sensitivity of the data concerned. Ideally, the erasure concept should clearly indicate for each type of data when data of that type are to be erased, so that employees can comply with the erasure obligation without further queries.[8]

Retention obligations

The law does not only provide for erasure obligations, but also for retention obligations, which must be taken into account in an erasure concept in order not to violate other legal provisions by over-fulfilment of data protection requirements.

§ 257 of the German Commercial Code (HGB) is an important provision in commercial transactions. According thereto, every merchant is obliged to keep certain documents, which include commercial books, commercial letters or vouchers for bookings, for six or ten years, depending on the category. In addition, retention obligations arise from tax law. § 147 (1) no. 3 of the German Fiscal Code (Abgabenordnung, AO) stipulates, among other things, that also business letters must be kept in addition to commercial letters.

In addition, there are retention rights that are not mandatory but protect recognised legal interests of the controller. According to Art. 17 (3) (e) of the GDPR, the obligation to erase data does not apply if they are used for the establishment, exercise or defence of legal claims. This is the case when disputes are pending or are

[4] *Wehrmann*, in: Koreng/Lachenmann, Formularhandbuch Datenschutzrecht, Löschkonzept, notes 1-8.
[5] Ibid, note 7.
[6] Ibid, note 1.
[7] *Conrad,* in: *Auers-Reinsdorff/Conrad,* Handbuch IT- und Datenschutzrecht, § 34 Recht des Datenschutzes, para. 623 f.
[8] *Voigt*, in: Taeger/Gabel, DSGVO - BDSG - TTDSG, Art. 5 GDPR, para. 36.

reasonably to be expected.[9] This however involves great uncertainties. In practice, it may often be difficult to determine according to objective criteria whether a dispute is reasonably to be expected. At the same time, in many cases, for example during the period in which customers can assert warranty claims, it is indispensable to continue to store certain data. In order to minimise data protection risks and, where possible, store necessary data that are in the interest of the company, a legal assessment of the data in question is required in each individual case.

Anonymisation instead of erasure?

When complying with time limits for erasure, the question inevitably arises as to what requirements the GDPR places on the process of erasure itself. Unlike with many other terms in the Regulation, the GDPR does not provide an explicit definition for this. Erasure of personal data means the rendering of that data unrecognisable.[10] Erasure must make it impossible to take cognisance of the personal information contained in the data with a reasonable effort.[11] This means, for example, that merely pressing the delete key does not constitute sufficient erasure in the sense of data protection law.

The question is whether there are possibilities for companies to comply with their erasure obligations while continuing to benefit economically from the data. The GDPR only applies to personal data. Therefore, it is conceivable to fulfil the obligation by removing the personal reference of the data, i.e. by anonymisation. This may be of interest to a company in order to retain statistical or other information that may be useful for big data or artificial intelligence (AI) applications even after the personal reference has been removed. As far as can be seen by now, the question of whether the erasure obligation can also be duly fulfilled by anonymising data has not yet been decided by case law. However, there are good reasons for considering anonymisation as sufficient - a view that also seems to be shared by the German Federal Data Protection Commissioner.[12]

However, it should be noted that the relevant data must actually be processed in such a way that no further reference to the person concerned can be established. It is therefore necessary to carefully check whether there are other data in the company which, when viewed together, still allow the person to be identified. However, whether this also applies to the fulfilment of the obligation to erase data at the request of the data subject pursuant to Art. 17 of the GDPR is, however, controversial.[13] Companies should monitor developments on this issue in order to actually exploit any possibilities to still benefit from the use of data in anonymised form.

What to expect in the case of breaches?

Numerous fine notices issued by European data protection supervisory authorities in recent years illustrate how real the danger of negative consequences is in the case of

[9] *Meents/Hinzpeter*, in: Taeger/Gabel, DSGVO - BDSG - TTDSG, Art. 17 GDPR, para. 133.
[10] *Arning/Rothkegel*, in: Taeger/Gabel, DS-GVO - BDSG - TTDSG, Art. 4 GDPR, para. 98.
[11] Ibid.
[12] Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, Positionspapier zur Anonymisierung unter der DSGVO unter besonderer Berücksichtigung der TK-Branche, p. 8 f., available at: https://www.bfdi.bund.de/SharedDocs/Downloads/DE/Konsultationsverfahren/1_Anonymisierung/Positionspapier-Anonymisierung , last retrieved: 03/04/2023.
[13] *Roßnagel*, ZD 2021, 188, 192.

missing or inadequate data erasure concepts. The *Commission Nationale de l'Informatique et des Libertés (CNIL),* for example, found numerous breaches of the GDPR at the French state-owned company *RATP* and imposed a fine of 400,000 euros, last but not least because of the processing of data beyond the period required for the specific purpose.[14]

Considerable consequences are also looming in Germany. A case is currently pending before the Berlin Higher Regional Court (Kammergericht) concerning a fine of 14.5 million euros imposed on the real estate group *Deutsche Wohnen* by the Berlin data protection supervisory authority in September 2019. The group is accused of having stored data of former tenants that were no longer required in an archive system from which they could no longer be erased. Although the outcome of the case is still unclear, it illustrates that a lack of erasure concepts can lead to considerable financial consequences.[15] Companies should eliminate such risks where possible.

In addition, late erasure after a request pursuant to Art. 17 of the GDPR or unlawful processing of personal data after the purpose of the processing has ceased to exist may result in claims for damages by the data subject under Art. 82 of the GDPR. Our analysis of the current case law on Art. 82 of the GDPR shows that damages are awarded to data subjects in particular in labour courts.[16] The amount of damages awarded by the courts is usually in the four-digit range.[17] In order to minimise such risks, data protection-compliant erasure should be part of every company's data protection compliance.

Steps for data protection-compliant erasure

The erasure of personal data in a company in compliance with data protection regulations requires careful analysis and planning. The core of data erasure is the erasure concept, which, as a manual of data erasure in the company, provides all important points for the erasure of personal data as a guideline. Legal requirements for erasure, the identification of relevant retention rights and retention obligations, requirements for data protection-compliant erasure as well as the processes for erasure including a role and authorisation concept for erasure decisions are mapped out here. An erasure concept typically includes structured and unstructured data as well as analogue data and data carriers. A central component in the creation of the erasure concept are the parameters for determining the respective time limits for erasure. Aspects such as the sensitivity of the data concerned and the above-mentioned retention obligations must be taken into account. In some cases, as shown by a decision of the Dresden Higher Regional Court (OLG),[18] courts require that not the entire document or file

[14] News report: French data protection authority imposes fine in the amount of EUR 400,000, available at: https://www.reuschlaw.de/en/news/french-data-protection-authority-imposes-fine-in-the-amount-of-eur-400000/, last retrieved: 03/04/2023.

[15] News report: Datenschutzbußgeldverfahren gegen die „Deutsche Wohnen" vor dem EuGH, available at: https://www.behoerden-spiegel.de/2023/01/20/datenschutzbussgeldverfahren-gegen-die-deutsche-wohnen-vor-dem-eugh/, last retrieved: 03/04/2023.

[16] reuschlaw Report: Risk of damage compensation claims due to data protection violations, available at: https://www.reuschlaw.de/en/news/reuschlaw-report-risk-of-damage-compensation-claims-due-to-data-protection-violations/, last retrieved: 03/04/2023.

[17] Ibid.

[18] OLG Dresden, judgment of 14/12/2021, case no. 4 U 1278/21, para. 13, available at: https://rewis.io/s/u/ZusS/, last accessed: 03/04/2023.

be taken as a basis for the assessment, but rather the specific datum in question.

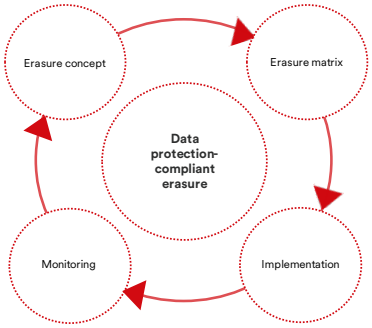

Figure 1: Data protection-compliant erasure
© reuschlaw, 2023

The erasure concept is concretised with the help of an erasure matrix, which can be created in different granularities. In this matrix, data types are assigned to erasure classes and provided with the respective retention periods and time limits for erasure as well as the relevant starting times.

Comprehensive support

We offer you comprehensive and exhaustive data protection advice on the development and implementation of erasure concepts. In this context, we will gladly support you in particular with the following measures:

- Development of an erasure concept that includes all relevant time limits for erasure, retention rights and obligations as well as the definition of roles and responsibilities and appropriate erasure procedures;
- Concretisation of the concept in an erasure matrix;
- Inclusion of the dependencies of the entire IT infrastructure (including data and dataflow mappings);
- Internationalisation of your erasure concept.

Next step: Get in touch

We would be pleased to support you in the development and implementation of your data protection-compliant erasure concept. We will gladly explain to you the details of our approach in a personal meeting.
Contact us now without obligation!

T + 49 681 / 859 160 0

E info@reuschlaw.de