In connection with the EU General Data Protection Regulation (GDPR), many companies are wondering how to implement a “data deletion policy”. This article describes the essential steps that companies need to undertake when preparing a GDPR-compliant data deletion policy and the associated documentation.

GDPR: Legal Background

Companies must implement the GDPR by 25 May 2018. The steps required for this include the definition of policies on how personal data should be stored and, above all, deleted. The legal requirements which stipulate when a data controller must delete personal data are described, for example, in Art. 17 and 25 of the GDPR. In principle, personal data should be kept only for as long as absolutely necessary (the so-called “storage limitation principle”, cf. reason 39 of the GDPR). An obligation to delete personal data may also arise if a data
subject requests the deletion of its data as per the “right to be forgotten” (Art. 17 GDPR), if they revoke a previously given consent, or if they object to the further processing of the person’s data.

The concept of a “right to be forgotten” is not an entirely new legal notion, and is, in fact, older than the so-called “Google judgement” from the Court of Justice of the European Union (CJEU, decision as of 13 May 2014, case no. C-131/12), which spread the public knowledge of this right . The obligation to delete personal data at the request of the relevant data subject had already been stipulated in the EU Data Protection Directive of 1995 and accordingly in its implementation into national laws, such as Sec. 35 of the German Federal Data Protection Act (Bundesdatenschutzgesetz, BDSG). However, even after so many years, there are still some companies which have not yet fully implemented the processes to comply with the obligations stipulated in the EU Data Protection Directive or the applicable national law. This may be due to the fact that, in practice, the selective deletion of a particular data subject’s personal data often presents companies with considerable technical, organisational and sometimes legal challenges.

A common practical problem is to know where the company may have stored the data to be deleted, which systems exchange data with each other and how as well as who has received the data and who, if necessary, needs to be informed about the deletion request. What may still seem feasible in a company with a monolithic-centralized IT infrastructure, however is quite difficult for small companies, especially if a variety of data processing systems has to be managed. Adding to this, the introduction of modern technologies such as cloud computing, virtualization at all levels and outsourcing of entire business processes does not really help in that respect.

From a legal perspective, the desire of a data subject that their data is deleted must be weighed against the company’s general legal document retention obligations, which in Germany are stipulated primarily in the commercial code (Handelsgesetzbuch, HGB) and the German Fiscal Code (Abgabenordnung, AO). These document retention obligations apply to many, but not all, business documents. In addition, the authenticity and integrity of the documents to be retained plays a major role. The company must ensure that the retained documents are not changed later. Therefore, if data has to be deleted, a distinction must be made between data that cannot be removed without violating the authenticity and integrity of the document to be retained, and those (parts of) documents that can, or which are not subject to retention. The strategy pursued by many up to now of complying with the legal retention obligations – some of which have a rather wide scope – by storing simply all documents and data which may, even remotely, be subject to document retention obligations, for the longest stipulated term, is therefore no longer compatible with the DSGVO.

German DIN standard as a solution?

The German industry’s strong commitment to standardization is proverbial, and it also has tangible financial advantages. It is therefore surprising that it took until the end of 2017 before the German Institute for Standardization (DIN) released its DIN standard 66398 on the development of a data deletion policy. The full
text of any DIN standard can only be obtained for a fee, but preliminary versions are available free of charge and can easily be found on the internet. The website http://din-66398.de also provides a wide range of additional information (German).

The final text of the DIN standard as well as the preliminary version are quite long, and they do not provide specific deletion rules and deletion periods for individual companies. Obviously, there can be no universal solution: as described below, deletion periods depend not only on the legal and regulatory requirements to which a company is subject, but also to a large extent on the business needs of a company:

The general provisions of the laws on data protection, commercial law and tax law apply to every company: HGB, AO, GDPR;

Banks and other “obliged entities” as per the relevant anti-money-laundering act (in Germany: Geldwäschegesetz, GwG – German) must retain the relevant documents, e.g. copies of identity cards made as part of the customer due diligence process;

Companies that are subject to the German Securities Trading Act (Wertpapierhandelsgesetz, WpHG – German) must record and store telephone calls with their customers (Sec. 83 para. 3 WpHG);

Companies that are subsidiaries of US companies, or have subsidiaries in the US, must be able to block documents and thus protect them from deletion and modification, if, for example, they are subject to litigation hold as part of a so-called “pre-trial discovery” (see below);

Companies whose customers include public clients may be required to produce documents, in particular tender documents, for a price review procedure (German regulation on auditing prices, Preisprüfungsverordnung VO PR 30/ 53 – German).

However, the DIN standard or the preliminary version provide valuable information on how a data deletion concept can be implemented in practice, in such a way that other legal provisions are observed in addition to the DSGVO.

**In a nutshell: how to define a data deletion policy**

The implementation projects for the GDPR now require that companies must find a workable compromise between the obligations described above and the rights of the data subject that their data be deleted. Contrary to the situation in the past, infringements of the GDPR are now subject to severe penalties. While it is quite unlikely that a small company will receive a fine in the millions as has been repeatedly conjured up, in the event of an infringement, it will in future play a role when assessing the amount of the penalty whether the violation is merely a single, individual incident or if it indicates a wider systematic problem (c.f. Art. 83 para. 2 lit. a GDPR).

Companies intending to implement a data deletion policy should carry out the following steps:
1. Identify and localize all personal data held by the company

For each department of the company, it should be identified and recorded what personal data is processed there. Which data is stored on which systems? Is there a central system for master data?

As part of this assessment, the following should be recorded:

- the data categories, i.e. the type of data;
- whether the data contains special categories of personal data;
- the duration for which this data is directly required for a business transaction; in the case of mass business, e.g. the processing of payment transactions, an average retention period could be determined;
- whether there is a legal obligation to retain the data in question; for this purpose, the legal provisions that apply to the data must be determined. The retention periods stipulated in Sec. 257 HGB and Sec. 147 AO apply to most documents, and amount to between 5 and 10 years;
- how long the retention obligation applies, i.e. when the respective retention period begins and when it ends;
- on which system or data carrier this data is stored;
- which data flows to other systems and/or is received from other systems, i.e. it should be determined for which systems the system under consideration is the data source, and which systems are the data source for the system under consideration (e.g. a central master data base).

Such an inventory includes all applications with which personal data is processed in the company. Regardless of the industry, most companies have a lot of such applications: databases (including any self-written Notes or MS Access databases!), customer relationship management software, software for archiving documents and information, software for data analysis including big data, as well as the usual e-mail and office applications. Additionally, most companies have special program packages for the personnel department, payroll accounting (outsourced, if applicable), applicant management, etc.

At least this inventory must be carried out anyway if the company identifies and documents the individual processing activities in order to subsequently include them in its records of processing activities (Art. 30 GDPR).

2. Classify data into categories

The data types collected should be assigned to different data categories, each with data that has the same retention period. A distinction should be made between special personal data as further restrictions may apply.

Separate categories should be created for data that is processed on behalf of the company by a data processor, or that the company processes itself on behalf of a third party data controller. Remember, group companies can also be the company’s data processors or data controllers!
3. Define data deletion rules per category

The GDPR stipulates that personal data may only be stored for as long as absolutely necessary (Art. 25 para. 2 GDPR in conjunction with reason 39). Therefore, a data deletion rule should be determined for each category of data, based on the collection date, the expected (average) processing time and the start of the respective retention period. It makes sense to keep the number of deletion rules as low as possible.

It should be noted, however, that even if data is no longer required, for example to perform a contract, it may be subject to data retention requirements due to statutory retention obligations. This would then constitute a legally determined change of purpose.

4. Archiving

Once the processing of data for a particular business transaction is complete, it is then usually archived before the data is finally deleted. As a general rule, companies usually archive data in a system that complies with the legal regulations on the storage of accounting data, including specifications such as the German “principles for the orderly management and storage of books, records and documents in electronic form and for data access” (Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff (GoBD) – German). The justification for such storage under data protection law is usually based on the interest of the responsible party i.e. the company, to comply with its legal obligations, but it can also be justified with a different legitimate interest (e.g. retention because of an ongoing legal dispute). In this case, the above-mentioned change of purpose also occurs.

How long data is archived must be determined in accordance with the legal provisions for document retention or the duration of the legitimate interest; the latter usually only justifies shorter storage periods.

5. Special cases

If a data subject makes use of their “right to be forgotten” (Art. 17 GDPR), or if it turns out that a particular data record has been collected illegally or if a supervisory authority requires a company to delete this data (Art. 58 para. 2 lit. g GDPR), the company may have to delete a data record outside the deletion rules defined for this purpose.

A company may also be obliged to block all deletions and changes to a particular set of data. In US procedural law there is the so-called “pre-trial discovery”, which requires that certain documents and data must be handed over to the opposing party. If such documents or data to be released are nevertheless deleted, e.g. because the data deletion rules for that set of data have not been suspended, this alone can lead to the case being lost.

Companies that are subject to the jurisdiction of the US courts are therefore affected, e.g. if they are the subsidiary of a US company or they themselves have a subsidiary in the USA.

Ideally, companies should prepare their own descriptions of their processing activities and specify therein how a
deletion process works in a particular case, so that they can prove to the data subject, a US court or a supervisory authority that the data has been deleted or, in the case of pre-trial discovery, blocked and protected against changes. This includes defining the procedure and specifying any manual interventions (for example, data selection, principle of dual control, documentation/log).

6. Actual deletion

Once the retention period for a group of (archived) data records has expired, they must be deleted. For this, secure deletion procedures should be established which, if necessary after manual confirmation, carry out the deletion and automatically log the deletion process (deletion log). If errors occur, for example, if a data record cannot be found or is locked, the deletion procedure should generate a message. The deletion log should be checked by an appropriately instructed employee.

In doing so, the company should also consider which paths the data takes within the company. If there are several copies of the data, e.g. master data in different systems, this must be taken into account as well as any data exchange between different systems, one of which is the decisive one. A central database for master data can therefore simplify a lot.

Any physical data should be appropriately destroyed, e.g. by using a shredder. Hard disks and other types of memory in computers, printers or fax/multifunction devices are hereby often overlooked.

If the hardware is still to be used, or, as is often the case today, the destruction of the data carrier is practically impossible because the data carrier does not belong to the company, a technically secure method of deletion should be used. Note that the regular “delete” function of most operating systems and databases is generally not sufficient to meet the requirements of the GDPR. Even the frequently recommended overwriting method is not feasible in all cases, for example, if the data is stored on a shared system or on a database that contains additional data records that still need to be retained. The encryption of a group of data records with a common deletion date can be a solution as well as the proper anonymization of the data records.

For data stored in cloud applications, the company usually has to trust that the provider, as its data processor, will carry out the deletion. Another option is to use, from the beginning, a Cloud Access Security Broker or a Cloud Data Protection Gateway, where from the outset only encrypted data ends up in the cloud and where it is sufficient to delete the key to permanently render such data irretrievable in unencrypted form. Depending on the technical solution chosen, selective deletions or deletions of different data categories are also possible.

The deletion logs should be kept for a certain period of time because deletions may have to be proven in some cases. These could include, for example, data subjects or supervisory authorities requesting proof of the deletion of the relevant data.
7. Testing, testing, testing

Similar to software development projects, a comprehensive test should be carried out before the data deletion procedures are put into operation.

If at all possible, companies should test whether the deletion is carried out correctly and on time, and that the relevant logs are generated. This is especially true if there are dependencies between different systems. It is important to note that a file that is required for the production operation process and of which there is no backup copy cannot be restored if it is deleted in accordance with data protection regulations, even if such deletion was due to a malfunction or an error of the user triggering the deletion.

The effects of the deletion on any interconnected systems should also be observed. What happens, for example, if a master data record is deleted from the master data database? How fast does it synchronize with the connected systems? Are there any malfunctions?

8. Special case: data processing

If the company is itself a processor of another data controller, that data controller is required to specify the data deletion policies and will usually also request data deletion logs. Therefore, the implementation of the specifications should be documented, i.e. both the actual data deletion procedure and the execution of the data deletion. The former could be included in the documentation of the measures for the security of personal data (Art. 32 GDPR), the latter are the data deletion logs. Data deletion logs could, for example, be transmitted automatically to the data controller. For this, it must be strictly controlled that the data deletion protocols only reflect the deletion of the relevant data controller’s data!

If the company itself is the data controller, it should give the data processor instructions for the deletion of data in accordance with the steps described above, or check their procedures. In addition, the relevant data deletion logs should be requested from the data processor. This also includes checking how long it will take the data processor to implement a data deletion instruction, so that the data controller can set a reasonable deadline for subsequent instructions to the data processor, or for responding to requests for information from a supervisory authority or a data subject.

If any personal data has been disclosed to a third party, such as due to a change of purpose (Art. 6 para. 4 GDPR), the company may have to notify the recipient of the data of the correction and deletion (Art. 19 GDPR). Therefore, the company should regularly check whether all such transfers of data are documented and whether the corresponding communication channels are functioning properly. This requires that it is documented which third party received which data, when and why.

In the course of the GDPR implementation project, the company’s data processing agreements have probably
already been reviewed and, if necessary, updated. It should have been examined whether they contain provisions on the deletion of data (cf. Art. 28 para. 1 lit. f GDPR) which are in conformity with the company’s data deletion concept. Experience shows that even seemingly GDPR-compliant data processing agreements often contain incomplete rules on the deletion of data or are phrased too much in favour of the data processor (“simply delete everything”). Where necessary, such contracts must be amended.

9. The data deletion policy

The data collection procedures, categories of data, decisions and rules described above, in particular the policies governing the deletion of data, should be documented and compiled together et voilà, this provides companies with a data deletion policy. This can be referred to, for example, in the company’s description of the processing activities (Art. 30 GDPR).

Conclusion

Even if it may seem that when it comes to the deletion of data, the GDPR only burdens companies with unnecessary bureaucracy: it is not sufficient to only consider the data deletion policy from the perspective of the GDPR. Companies have long been obliged, by completely different rules, to have and maintain selective, time-controlled procedures for the storage and retention of data. Ultimately, this belongs to the general management and control of the company and of the risks it is exposed to. The GDPR, and before it, the BDSG, only prevent that the strategy which has been pursued by many enterprises so far to simply store everything indefinitely on mass storage devices which are cheap to obtain these days- can be maintained.

Therefore, the implementation of a GDPR-compliant data deletion policy is closely linked to the implementation of a document retention concept required by commercial law, fiscal law and other legal retention obligations which also require a precise knowledge of the data flows in the company and potentially an analysis of the data. It should also be noted that an objection against the receipt of advertisements via email (see Sec. 7 para. 3 of the German Act Against Unfair Competition - Gesetz gegen den unlauteren Wettbewerb, UWG) can only be implemented by deleting certain data. Therefore, if by implementing the GDPR you discover that there is a need for improvement in your company, you can cover several additional requirements at the same time. A well thought through, consistently implemented data deletion policy therefore makes a significant contribution to your company’s compliance policy.