BRANDI
RECHTSANWÄLTE

DATA ERASURE – ONLINE AND OFFLINE

Information on data protection I April 2024

Introduction

In connection with the storage or other retention of data and its erasure, it is often said that erased data is the most secure data. This statement refers in particular to the principle of storage limitation pursuant to Article 5 (1) (e) GDPR, one of the key principles of data protection law. Accordingly, personal data may only be stored or otherwise retained for as long as necessary for the purposes pursued. As soon as the data is no longer required, it must be erased in accordance with Article 17 (1) GDPR. The erasure requirements are intended, among other things, to prevent personal data from falling into the hands of unauthorized third parties or being misused in any other way.

There is often a conflict between the obligation to erase or destruct data and the company's interest in continuing to store it. Various questions arise in this context: How long may personal data be stored? What is meant by the terms „erasure" and „destruction"? What needs to be considered when erasing data from online systems? And what applies with regard to the destruction of data carriers and paper documents?

How long may personal data be stored?

It follows from the principles of data processing and the recitals of the GDPR that personal data may only be stored for as long as it is needed. Personal data that is no longer necessary for the purposes for which it was collected or otherwise processed must be erased immediately. This is expressly stated in Article 17 (1) (a) GDPR. In addition, Article 17 GDPR contains further reasons why the company responsible is obliged to erase data. The basic obligation to erasure does not apply if the data is subject to a retention obligation or if one of the other exceptions listed in Article 17 (3) GDPR is fulfilled. The German legislator has standardized further exceptions in Section 35 BDSG, whereby the admissibility of further exceptions outside the GDPR is controversial (Nolte/Werkmeister in Go-la/Heckmann, § 35 Rn. 3). According to this, the obligation to erase in accordance with Article 17 GDPR does not apply if, in the case of non-automated data processing, erasure is not possible or only possible with disproportionate effort due to the special type of storage and the interest of the data subject in erasure is considered to be low. In this case, the restriction of processing pursuant to Article 18 GDPR takes the place of erasure. According to this, the data must be „blocked" and - apart from storage - may only be processed with the consent of the data subject or for the exercise, assertion or defense of legal claims or for reasons of important public interest.

It should be noted that the erasure obligation applies not only to data stored online, but also to data stored offline. In the latter case, the information must be made unrecognizable or destructed in accordance with data protection regulations when the storage period is reached.

What is meant by the terms „erasure" and „destruction"?

The GDPR does not describe in detail what is meant by the term „erasure". From the fact that Article 4 No. 2 GDPR differentiates between the erasure and destruction of data, it can be concluded that erasure does not necessarily have to be accompanied by the destruction of the data. Rather, the term encompasses every type of obliteration; it therefore covers all constellations from the anonymization of data to the overwriting or blackening of data to its physical destruction. Destruction is therefore only one possible form of erasure.

In principle, the data must no longer be perceptible after erasure and must no longer be available to the controller for further use. This also means that, in principle, data can only be regarded as erased or destructed once it has been ensured that no data backups or other copies of the data records exist in the controller's area of responsibility. In contrast, purely organizational measures that are merely intended to prevent the information from being perceived (e.g. appropriate labeling) are not sufficient.

What needs to be considered when erasing data from online systems?

If there is a reason for erasure, the data concerned must be removed from the online systems immediately, unless they are subject to a retention obligation. In this respect, the controller is obliged to regularly check whether there is a reason for erasure with regard to the data in its area of responsibility.

If data remains stored exclusively for the fulfillment of retention obligations, it is advisable to separate it from the data that is still actively used. In this way, it is easy to check which data records need to be erased after the retention period has expired. To make erasure easier to implement, an electronic archiving system should ideally have the option of systematically erasing certain data records from the archives. If one of the exceptions under Section 35 BDSG is fulfilled, the data may also be blocked in the systems instead of erased, provided this is technically feasible.

The obligation to erase data does not only apply to live systems and archives, but also includes data backups and backup systems. In this respect, there are usually no major problems if the backups are overwritten at regular, relatively short intervals anyway and old data is erased in this way. If, in contrast, data remains stored for a longer period of time with a staged backup concept, this serves the purpose of data security; the procedure can be based on Article 32 GDPR as technical and organizational measures and does not conflict with the erasure obligation pursuant to Article 17 GDPR (Korte, ZD-Aktuell 2020, 07001). In this case, it is only necessary to ensure that the backup data is really only used for backup purposes and that this data is at least blocked.

What applies with regard to the destruction of data carriers and paper documents?

Since the destruction of data carriers and printouts containing personal data such as names and addresses of individuals is considered to be the processing of personal data pursuant to Article 4 No. 2 GDPR, a level of protection appropriate to the risk must be ensured when disposing of such data in accordance with Article 32 (1) GDPR. The specific measures to be taken depend on the sensitivity of the data concerned. In this respect, it should be noted that comprehensive separate disposal of all paper waste and data carriers is not mandatory, as protected destruction is not required in every case in which a paper or data carrier contains personal data. Instead, a decision must be made on a case-by-case basis.

In general, a separate disposal must be carried out in particular if data processing by the company has taken place or data of third parties are disclosed. The following non-exhaustive examples serve to illustrate and substantiate this general requirement. If the papers or data carriers contain customer data that has been collected, processed or stored by the company, destruction is regularly indicated. The same applies if the documents or data carriers contain employee data to be protected. However, if only contact data of the company or business contact data of individual employees are affected, separate disposal is not required. This also applies if the company has been provided with contact details of other persons, e.g. in the form of sender information on unsolicited advertising letters. In the case of internal e-mails, it is important to differentiate which information is included and the context is also crucial. A message such as „I'll be late." or „The meeting has to be postponed." does not require separate disposal. However, if data such as the meeting with a named external person or customer data is disclosed in the e-mail, it must be destructed. The same applies in the case of information requiring confidentiality, such as a non-public meeting or contact with other companies that should not be made public.

In order to ensure that in all cases where data protection-compliant disposal is required it takes place, it is possible to generally opt for protected destruction. One reason for this may be that individual employees should not be expected to carry out the assessment in individual cases. Another is that a case-by-case decision means increased effort and a higher susceptibility to errors. If the disposal of paper waste is to be differentiated according to data protection requirements, it is advisable to provide employees with standards that enable them to make their own assessment in order to minimize the risk of disposal in breach of data protection regulations.

Conclusion

If the purposes for which the data was collected or otherwise processed no longer apply, or if one of the other reasons set out in Article 17 GDPR applies, the controller is obliged to erase the data unless it is subject to a further retention obligation or an exception applies. The controller must regularly check on its own initiative whether there is an obligation to erase. The concept of erasure includes not only the physical destruction of data, but also its anonymization, overwriting or blackening. It must be ensured that the information is no longer perceptible after erasure and that no copies of the data records exist. To ensure compliance with the requirements and simplify the processes, it is advisable to define the applicable erasure periods and document the intended processes for implementing the erasure within an erasure concept.

Christina Prowald

Contact:

BRANDI Rechtsanwälte
Partnerschaft mbB
Adenauerplatz 1
33602 Bielefeld

Christina Prowald
Wissenschaftliche Mitarbeiterin

T +49 521 96535 - 980
F +49 521 96535 - 113
M christina.prowald@brandi.net