THE RECORD OF PROCESSING ACTIVITES –

WHAT IS A PROCEDURE AND HOW MANY PROCEDURES MUST BE DOCUMENTED?

Information on data protection I March 2024

Introduction

Under the General Data Protection Regulation (GDPR), companies are subject to the so-called accountability obligation pursuant to Article 5 (2) GDPR. This means that they must provide positive proof that they comply with data protection regulations. This requires comprehensive documentation of the issues relevant to data protection law. This documentation also includes the creation of a record of processing activities. According to Article 30 (1) (1) GDPR, every controller and, where applicable, their representative is obliged to keep a record of all processing activities for which they are responsible. All data processing operations in which personal data is processed must be listed in the record, insofar as this falls within the responsibility of the controller. The record has the task of summarizing and documenting the essential information on the individual processes. At the same time, the documentation also serves the purpose of self-monitoring. The mandatory information that the record must contain is then derived from Article 30 (1) (2) GDPR. This includes the name and contact details of the controller and its data protection officer, the purposes of the processing, a description of the data subject and the personal data processed as part of the process, the recipients to whom the data is disclosed, the transfer of data to third parties and the duration of storage. The record must be maintained on an ongoing basis so that it always reflects the current status of data processing in the company.

According to the concept of the GDPR, the creation and maintenance of the record is the responsibility of the data controller, i.e. the company. However, the data protection officer provides support and advice in the creation and maintenance of the register, particularly in the context of risk assessments and legal evaluation. The record must be made available to the supervisory authorities upon request. The processes must be documented in such a way that the supervisory authority can gain an initial impression of whether the controller is complying with its data protection obligations by requesting the list of processing activities or individual process descriptions. With the help of the record of processing activities, the company can simultaneously prove that the required examination of the data protection requirements for each data processing operation has taken place.

What is a procedure within the meaning of the record of processing activities?

Although the term “processing activity” is used several times in the GDPR, it is not defined. Linguistically, the term could initially be understood as a subset of the term processing defined in Article 4 No. 2 GDPR, which could, however, result in several processing activities having to be documented for each processing. Yet such a detailed break-down quickly leads to uncertainty, would therefore not comply with the transparency requirement and would counteract the approach of reducing bureaucracy set out in recital 89. The term processing activity is therefore to be equated with the term processing, so that every process in the company in which personal data is processed must in principle be documented as a separate procedure.

Regarding the question as to the extent to which different data processing procedures can be summarized within a procedure description, the objectives of Article 30 GDPR and the transparency requirement must again be taken into account. On this basis, closely related matters and series of processes that are linked by a common purpose or concern the processing of very similar data can be bundled and documented together. For example, it is not necessary to create a separate procedure for the creation of each individual Word document; instead, thematic groups can be formed and described. When combining different processes, a limit should be set at the point where the clear structure of the individual process is obscured. If, on the other hand, a process that is uniform in principle consists of several discrete sub-processes, it may be appropriate to split up the documentation and record the individual subprocesses separately. If, for example, newly introduced software has different functionalities or applications that are used to process different data and pursue different purposes, a corresponding approach should generally be appropriate for reasons of transparency. In addition, it may be useful to create a general, overarching procedure for the software, in which general topics such as registration processes, authorization structures and the involvement of service providers are addressed and reference is made to the individual functionalities and the associated individual procedures with further descriptions.

In order to implement the objective of reducing bureaucracy as defined in recital 89, mechanisms should be created that make it possible to deal primarily with those data processing operations that are likely to pose a high risk to the rights and freedoms of data subjects. It can be deduced from this that within the record of processing activities, the focus should be placed in particular on those processes that involve a corresponding risk. In practice, this means

that particularly high-risk and complex processes should be analyzed and described in greater detail. Nevertheless, the documentation of procedures that result in fewer risks for the data subjects cannot be neglected. When documenting, it is generally important to ensure that the respective procedure is described in such a way that even people who are not familiar with the specific workflows and data processing procedures can understand the description and, accordingly, the procedure.

The primary aim of the documentation is to present the respective process transparently. The amount and degree of detail accorded to the individual descriptions then depend primarily on the categories of data processed as well as the type, complexity and risk of the respective processing procedures.

How many procedures must be documented?

How many procedures a company needs to document depends primarily on its area of activity. The more customer and employee data a company processes within various processes, the more procedures need to be created. Apart from these activity-related procedures, there are also topics that must usually be documented by every company. These include processes from accounting or human resources as well as data processing in the context of standard applications such as word processing programs, calendars, telephone and e-mail applications. When identifying the procedures to be documented, those responsible can use the general structures in the company as a guide. In this respect, a breakdown according to the various departments of the company is often useful. A large number of procedures will need to be recorded, especially in those departments that are particularly intensively involved in the processing of personal data.

What are the consequences of failing to keep a proper list of procedures?

If there is no proper record of processing activities in the company, this may result in a fine. It is particularly relevant if the supervisory authority becomes aware, as a result of a complaint from a data subject, of a specific area of activity of the company or a specific subject area, such as cooperation with service providers in the course of the company's online offerings or the transfer of data to third countries, and subsequently requests the associated process descriptions. If the controller then fails to comply with its obligation to keep the record, a fine of up to 10 million euros or up to 2% of the company's total annual global turnover may be imposed for breach of Article 30 GDPR in accordance with Article 83 (4) (a) GDPR.

Conclusion

Within the record of processing activities, companies must document all processes in which they process personal data. On the one hand, the creation of the record serves to fulfill the accountability obligation anchored in Article 5 (2) GDPR. On the other hand, by examining the individual processes and their documentation, optimization potential in the company can be determined, further audit requirements can be formulated, and aspects relevant to data protection law identified in the context of projects can be structured for subsequent implementation. The exact structure of the individual procedures must be determined with particular regard to the principle of transparency. How many procedures a company has to create in total depends primarily on the company's area of activity. When creating the record of processing activities, particular attention must be paid to processing-intensive areas and processes within the company.

Christina Prowald

Contact:

BRANDI Rechtsanwälte
Partnerschaft mbB
Adenauerplatz 1
33602 Bielefeld

Christina Prowald
Research Associate

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