BRANDI
RECHTSANWÄLTE

DATA PROTECTION IN THE IMPLEMENTATION OF THE WHISTLEBLOWER PROTECTION ACT

Information on data protection I July 2023

Introduction

The Whistleblower Protection Act (Hinweisgeberschutzgesetz, HinSchG) came into force on July 2, 2023. The HinSchG regulates the protection of persons who have obtained information about certain violations in connection with or in advance of their professional activities and who report or disclose such information to the reporting bodies provided for under the Act (whistleblowers), as well as the protection of persons who are the subject of a report or disclosure or are otherwise affected by it.

The law requires employers of a certain size or with a certain activity to set up internal reporting offices through which employees can report violations of the law. The implementation of these requirements, in particular the processing of whistleblower reports, involves the processing of personal data, whereby the requirements of data protection law, in particular the requirements of the General Data Protection Regulation (GDPR) and the Federal Data Protection Act (BDSG), must be complied with.

Data processing activities in the implementation of the HinSchG

In the course of processing reports of violations, the internal reporting office will, for example, confirm receipt of the whistleblower's report, check whether the reported violation is covered by the HinSchG, maintain contact with the whistleblower, check the validity of the report received, request further information from the whistleblower if necessary, and take appropriate follow-up action. In particular, the data submitted in a report is processed. This includes, for example, information about the accused person and his or her behavior as well as - if the report is not anonymous - the name of the whistleblower and, if applicable, his or her contact data, his or her position in the company and the circumstances of the observation of the misconduct.

Legal bases

In principle, the HinSchG provides for an obligation to introduce reporting offices as a rule for employers with at least 50 employees. If an employer is required by the HinSchG to set up a reporting office and to process and document the reports it receives, the legal basis for the associated processing of personal data is the corresponding legal obligation pursuant to Article 6 (1) (1) (c) GDPR. Since the data processing serves the legitimate interests of the employer in the detection and correction of violations of the law and grievances, the health of employees and the prevention of criminal acts, Article 6 (1) (1) (f) GDPR can also be used as the legal basis for the data processing.

If there is no legal obligation for an employer to establish and operate a procedure for the internal reporting of violations due to its size and the nature of its activities, it has the option of voluntarily establishing an internal reporting office. The legal basis for data processing in this respect is the aforementioned legitimate interest pursuant to Article 6 (1) (1) (f) GDPR.

Section 10 HinSchG provides for a special regulation and allows the reporting offices to process personal data insofar as this is necessary for the fulfillment of their tasks specified in the HinSchG. In deviation from Article 9 (1) GDPR, the processing of special categories of personal data by a reporting office is also permitted if this is necessary for the fulfillment of its tasks.

In principle, whistleblowers can decide for themselves whether they wish to submit a report to the reporting office and which data they provide. The legal basis for processing the whistleblower's data is therefore the whistleblower's consent pursuant to Article 6 (1) (1) (a) GDPR. If the processing of employees' personal data serves the purpose of investigating criminal offenses and there are documented indications that give rise to the suspicion that the data subject has committed a criminal offense in the employment relationship, the processing is necessary to uncover the offense and the legitimate interest of the employee in the exclusion of the processing does not prevail, Section 26 (1) (2) BDSG shall also be the legal basis for the data processing.

Data privacy statement for whistleblowers

Pursuant to Article 13 GDPR, whistleblowers must be informed about the extent to which their personal data is processed in connection with the use of the hotline. It is therefore necessary to prepare a data privacy statement that is made available to the whistleblowers. In particular, the data protection statement must provide information about the extent to which and the purposes for which personal data is processed, to whom the data is disclosed and how long the data is stored.

The specific design of the data privacy statement depends, among other things, on the design of the reporting office. Depending on whether reports are submitted verbally, in text form or in person, digitally or analogously, i.e., for example, via an e-mail address, a platform on the Internet or intranet, a hotline, an answering machine, in a personal meeting or in a video conference, the data protection information must be adapted to the corresponding circumstances.

In practical implementation, a platform on the Internet or intranet can be linked to a data privacy statement, for example. If an e-mail address or hotline is set up, the data privacy information can be made available to employees together with the general information about the reporting office. If a mailbox is set up, the data privacy information can be posted next to the mailbox. In any case, it is important that data subjects are able to inform themselves about the data processing before they decide to submit a report to the reporting office.

Further information requirements

A report usually contains information about the accused person and his or her misconduct, which the whistleblower has provided in his or her report. In these cases, where personal data has not been collected from the data subject, Article 14 GDPR applies with regard to the information requirements. Not only the whistleblower, but also the reported party must therefore be informed about the processing of his or her personal data. In addition to information about the type of data, the purpose of the data processing and the data recipients, the obligation to provide information pursuant to Article 14 GDPR also includes, in particular, information about the source of the personal data.

However, information of the data subject may be excluded due to legal requirements. This is the case in particular pursuant to Article 14 (5) (b) GDPR if and insofar as the realization of the objectives of the data processing would be seriously impaired by the information. In this respect, it is conceivable that the direct information of the accused would prevent the investigation of criminal acts.

Data protection-compliant design of the reporting office

The principles of data processing should be observed in the design of the notification center. Pursuant to Article 5 (1) (c) GDPR, the principle of data minimization applies, according to which personal data must be adequate and relevant to the purpose and limited to what is necessary for the purposes of the processing. When submitting notifications, therefore, only the absolutely necessary data should be requested. In principle, the whistleblower should be able to decide for himself/herself what information he/she wishes to include in his/her report. According to the HinSchG, there is no obligation to enable anonymous reports; however, if anonymous reports are received, the employer is obliged to process them as well. As a rule, therefore, the provision of a name should not be one of the mandatory details to be included in a report.

Technology design and data protection-friendly default settings should also ensure that only personal data whose processing is necessary for the specific processing purpose is processed and that the data is not made accessible to unauthorized persons (Article 25 GDPR). The reporting points must be designed in such a way that only the persons responsible for receiving and processing the reports and the persons supporting them in the performance of these tasks have access to the incoming reports. Suitable technical and organizational measures must be taken for this purpose in accordance with Article 32 GDPR. Appropriate measures also include training for hotline officers and confidentiality obligations for these persons.

Data transfer

When implementing technical and organizational measures, responsible bodies must observe the confidentiality requirement pursuant to Section 8 HinSchG. According to this, reporting offices must always maintain the confidentiality of whistleblowers as well as the persons who are the subject of a report and other persons named in the report. The identity of these persons may only become known to the persons responsible for receiving reports or for taking follow-up measures, as well as to the persons assisting them in fulfilling these tasks.

Exceptions to the confidentiality requirement are provided for in Section 9 HinSchG. According to this, information about the identity of a whistleblower in criminal proceedings may be disclosed to the competent authority at the request of the prosecuting authorities or on the basis of a court decision. The disclosure of information about the identity of the whistleblower is also permitted if the disclosure is necessary for follow-up measures and the whistleblower has previously consented to the disclosure. Information about the identity of persons who are the subject of a report or are named in a report may be disclosed, among other things, if consent has been given in this regard, if this is necessary for taking follow-up measures or in criminal proceedings at the request of the prosecuting authority. Disclosure by internal reporting offices is also permitted if this is necessary in the context of internal investigations at the respective employer or in the respective organizational unit.

Data processing

Pursuant to Section 14 (1) HinSchG, a third party can also be commissioned with the tasks of an internal reporting office. For example, if a company commissions a technical service provider to provide the infrastructure for a reporting office, the service provider will process the company's personal data on its behalf, insofar as it would have access to this data itself. In this respect, there is usually data processing between the company and the technical service provider. In this case, an agreement on data processing must be concluded to safeguard data processing on behalf of the company. If, on the other hand, the operation of the reporting office is the overall responsibility of a service provider, the exact arrangement is decisive for classification as possible data processing. Professional secrecy holders such as lawyers, for example, are privileged in this respect because they are already subject to special secrecy by law and therefore no data processing is required.

Documentation and storage time

The persons who are responsible for receiving reports in a reporting office are obliged to document incoming reports in accordance with Section 11 HinSchG. The documentation must be permanently retrievable and must comply with the confidentiality requirement.

With regard to the type of documentation, Section 11 HinSchG contains various requirements. According to this, for example, in the case of telephone reports or reports by means of another type of voice transmission, a permanently retrievable audio recording of the conversation or its complete and accurate transcription may only be made with the consent of the whistleblower. The legal basis for data processing is then Article 6 (1) (1) (a) GDPR. In the absence of such consent, the report shall be documented by a summary of its contents to be prepared by the person responsible for handling the report. If the report is made in the context of a personal meeting, a complete and accurate record of the meeting may be made and kept with the consent of the whistleblower. The legal basis in this respect is also the consent of the whistleblower pursuant to Article 6 (1) (1) (a) GDPR.

The documentation must be deleted three years after completion of the procedure in accordance with Section 11 (5) HinSchG. However, the documentation may be kept longer in order to fulfill the requirements of the HinSchG or other legal provisions, as long as this is necessary and proportionate.

In order to comply with the requirements of the HinSchG regarding the documentation of reports, it is therefore necessary to define and implement deletion periods.

Documentation in the directory of processing activities

According to the GDPR, data controllers are subject to an accountability obligation (Article 5 (2) GDPR). They must therefore be able to prove compliance with the data protection requirements. This proof is provided, among other things, by the directory of processing activities pursuant to Article 30 GDPR, which must be kept by every controller and which contains a description of all data processing processes at a controller.

The processing activities to be documented also include the data processing associated with the processing of notifications under the HinSchG. The process via the internal notification office must therefore be included in the list of processing activities.

Data protection impact assessment

If a form of data processing, in particular when using new technologies, is likely to result in a high risk to the rights and freedoms of natural persons by virtue of the nature, scope, context and purposes of the processing, a controller shall carry out a prior assessment of the impact of the envisaged processing operations on the protection of personal data pursuant to Article 35 (1) GDPR.

Due to the potentially sensitive content of breach notifications, which may have criminal relevance and may result in severe consequences for the data subjects, the associated data processing will regularly involve a high risk to the rights and freedoms of natural persons. For the establishment of the hotline, it is therefore usually necessary to conduct a data protection impact assessment.

Conclusion

When implementing the HinSchG, employers must comply with the requirements of data protection law. This means that there is a need for action not only with regard to the establishment of reporting offices and the processing of incoming reports, but also with regard to various aspects of data protection law. In particular, data protection notices for whistleblowers must be created, information obligations towards accused persons must be fulfilled, the reporting office must be designed in a data protection-compliant manner and documented in the directory of processing activities, deletion periods must be observed, and a data protection impact assessment must be carried out. If an external service provider is used, an agreement on contract processing must also be concluded. In case of doubt, the data protection officer should assist with this.

The data protection requirements also apply accordingly to reports of violations that are not related to the HinSchG. If an employer is not required to set up a reporting office in accordance with the HinSchG and has not done so voluntarily, but employees nevertheless report violations of the law to the employer, then the employer must treat these reports in particular as confidential, process the personal data only with an appropriate legal basis and only for as long as necessary, and inform the affected persons about the processing of their personal data.

Johanna Schmale

Contact:

BRANDI Rechtsanwälte
Partnerschaft mbB
Adenauerplatz 1
33602 Bielefeld

Johanna Schmale
Research Associate

T +49 521 96535 - 883
F +49 521 96535 - 113
M johanna.schmale@brandi.net