

Information on the whistleblower protection law and the external reporting office at DAKOSY

1. Introduction

In 2020, the European Union introduced the so-called ‘EU Whistleblowing Directive’.

According to this, all companies and associations in the member states of the European Union that employ more than 50 employees (m/f/d) and/or generate more than EUR 10 million in annual sales are obliged, among other things, to set up an external reporting point which whistleblowers can contact confidentially if they wish to report violations of the law relating to the respective company.

These EU requirements are implemented in Germany through the German Whistleblower Protection Act (HinSchG), which came into force in 2023. The Whistleblower Protection Act expands the protection of whistleblowers.

In order to implement legal requirements and as part of compliance, a uniform, anonymous and sanction-free whistleblower system is necessary that ensures that company management is informed about the detection, prevention and defence of harmful and criminal actions that go against the financial interests and reputation of DAKOSY Datenkommunikationssystem AG (hereinafter ‘DAKOSY’).

Due to the further development of compliance at DAKOSY, as well as the requirements of the ‘EU Whistleblower Directive’ and the Whistleblower Protection Act, an external reporting office with an electronic whistleblower system has been introduced at DAKOSY.

2. Goals

The aim of this paper is to establish clear rules for the operation of the external reporting office and for dealing with incoming reports of criminal or administrative misconduct at DAKOSY and to give potential whistleblowers some security and knowledge about this topic at DAKOSY.

Clear regulations in this area are intended to help understand and adhere to the compliance standards that apply at DAKOSY. The commission or planning of criminal offenses should be

uncovered as quickly as possible in order to prevent damage to the company, the shareholders, stakeholders and the employees (m/f/d in general).

3. Rules

In general terms, DAKOSY expressly desires or expects to receive information about existing or suspected criminal or administrative misconduct in the company.

All persons who become aware of violations of the law and criminal or administrative misconduct in the company should report this to DAKOSY immediately.

This applies in particular if the whistleblower must expect that serious damage may arise for DAKOSY. Whistleblowers who report criminal or administrative misconduct are also requested to describe the matter as precisely as possible to the best of their knowledge so that DAKOSY may take appropriate countermeasures as quickly as possible.

DAKOSY assures all whistleblowers that all incoming reports made to the compliance officer, the trusted lawyer (ombudsman) or the external electronic reporting office of DAKOSY will be investigated within the scope of the legal possibilities or have them examined by a lawyer. The requirements of the EU General Data Protection Regulation (EU-GDPR) and the Federal Data Protection Act (BDSG) in their current version are adhered to and all constitutional principles, including the presumption of innocence, are upheld.

DAKOSY guarantees that whistleblowers will be treated with strict confidentiality and, in this context, ensures compliance with all legal requirements for the operation of the external reporting office. Corresponding contractual agreements with the operator of the external whistleblower system ensure compliance with the above assurances.

The Whistleblower Protection Act does not exempt any party from the obligation to report any crimes if one becomes aware of a planned serious crime within the meaning of Section 138 of the Criminal Code. For example, according to Section 138 (1) of the Criminal Code, anyone who becomes aware of a credible plan or execution of a so-called reportable offense such as counterfeiting of money or securities, murder, manslaughter, robbery, extortion, or a crime dangerous to the public at a time when the execution is taking place or the success can still be averted, must report such an offense to an authority or to the person threatened in a timely

manner: A report within the meaning of the Whistleblower Protection Act via the process described below, even using an external reporting office, is not sufficient.

4. Data protection

Legal basis

The legal basis for data processing on DAKOSY is article 6 para. 1 c) and f) GDPR in conjunction with the 'EU Whistleblower Directive / Whistleblower Protection Act (HinSchG) and Section 26 BDSG in conjunction with article 88 GDPR (GENERAL DATA PROTECTION REGULATION)

Data processing

When reporting violations of rules of conduct, personal data are processed. The data collection includes conduct violations as well as the corresponding facts that may have a personal connection to the reporting and/or accused person or to any witnesses. This allows personal data to be processed, such as the name, position in the company and circumstances of observation.

The data collected will only be processed for the intended purpose. The safeguarding of the legitimate interests of those affected must be guaranteed when processing personal data. Data processing is limited to sending the recorded report by email to the ombudsman. Further processing takes place as part of the ombudsman's legal activities.

Obligation to provide information

In cases where a specific person is accused, this person must be informed about the matter, in accordance with article 14 Para. 3 a) GDPR, no later than one month after the report is made.

Both the person concerned and the whistleblower have the right to access information in accordance with article 15 GDPR. This concerns the data stored about them.

The right to information does not exist (according to Section 29 Paragraph 1 Sentence 2 BDSG) if the information would reveal information that must be kept secret due to the overriding legitimate interests of a third party. This also applies in cases where the rights and freedoms of other persons are restricted for the purpose of preventing or detecting crimes or for the purpose of protecting the person concerned (article 23 paragraph 1 d) and i) GDPR).

In principle, sharing the accused person's personal data with third parties is not permitted. Exceptions are: Rights to inspect files in criminal proceedings or the prosecution of criminal offenses (article 6 Paragraph 1 f) GDPR in conjunction with Section 24 Paragraph 1 No. 1).

Correction and deletion

DAKOSY ensures that in accordance with article 5 Para. 1 d) GDPR personal data collected are factually correct and up to date.

In principle, data will be deleted within two months after the investigation has been completed if the information has not been confirmed. Storage beyond this is only permitted for the duration of the clarification of necessary further steps such as disciplinary proceedings or the initiation of criminal proceedings, usually up to two years.

Personal data associated with reports that are deemed unfounded will be deleted immediately.

5. Specific reporting channels

What specific reporting channels are there for a whistleblower if they learn of, observe or become aware of criminal or administrative misconduct at DAKOSY?

- 1) The Compliance Officer of DAKOSY AG is available for external whistleblowers at compliance@dakosy.de , Tel 040/37003-0, postal address: DAKOSY AG, Mattentwiete 2, 20457 Hamburg.
- 2) In addition, an external whistleblower point may be used. In this case, DAKOSY has commissioned a company that specialises in this matter, namely Hinweisgebersystem24 GmbH. At that company, DAKOSY's legal ombudsman, Mr Stephan Rheinwald, receives information about criminal or administrative misconduct at DAKOSY.
 - a) You can communicate with him by providing your own name and contact details. Questions from the external lawyer regarding the matter can be discussed immediately, which can sometimes prove to be very helpful in further clarifying the matter. If desired, the identity will not be transmitted to DAKOSY.
 - b) If you do not want to reveal your identity to the external lawyer at Hinweisgebersystem24 GmbH, you can also submit the tip anonymously using a web form (see below). Anonymous tips are also followed up on.

The link to the IT whistleblower system: <https://portal-hinweisgebersystem24.de/#/dakosy>.

DAKOSY's IT whistleblower system is a web-based system that is provided as an ASP solution (Application Service Providing) in DAKOSY's branding. No hardware or software installation is required to use the IT whistleblower system. The HGS24 whistleblower system is cloud based; All data and information are stored/processed exclusively in Germany in the high-security data centre for business customers, so that compliance with the best possible security standards is guaranteed. The IT whistleblower system is operated in compliance with the data protection regulations of the EU GDPR and the BDSG.

DAKOSY's trusted lawyer in matters of whistleblowing can be reached using the following contact details:

Compliance Officer Services Legal

Stephan Rheinwald, attorney

Telemannstraße 22, 53173 Bonn

s.rheinwald@cos-legal.eu

Tel.: 0228/ 35036291

Fax: 0228/ 35036292