DataGuard

PRIVACY CHEAT SHEET

# WHISTLE-BLOWING

## What to do from a privacy perspective if a report pops up?

DataGuard | Privacy Cheat Sheet

# Whistleblowing

What to do from a privacy perspective if a report pops up?


## Information to Whistleblowers (Art. 13 GDPR)

- at the time when personal data are obtained
- for tool-based whistleblowing systems, privacy notices on the landing page
- also as link in confirmation of receipt to whistleblower

## Information to accused / involved person(s) (Art. 14 DSGVO)

- only possible if identifiable & reachable
- in general, ***no later than 1 month*** after receipt of the relevant information or ***at the time of the first communication*** with the accused / involved person
- Deferral possible

## Possible Legal Bases for Processing

- HinSchG applicable: Art. 6(1)(1)(c) GDPR + Sec. 10 HinSchG
- HinSchG not applicable: Art. 6(1)(1)(f) GDPR
- for criminal offenses in the employment relationship: Sec. 26(1)(2) BDSG
- Transfer of data to third parties (including other Group companies) only permissible if necessary (e.g. local investigation of the facts in another country, law enforcement agency)

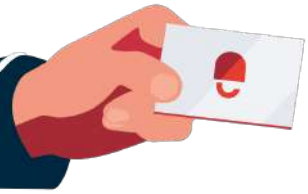
## Deferred information accused / involved person(s) (Art. 14(5)(b) GDPR, Secs 29(1)(1), 33(1)(2)(a) BDSG)

- as long as (one reason sufficient):
  a. risk that the ***facts cannot (or can no longer) be clarified***,
  b. assertion, exercise or defense of ***civil claims would be impaired***,
  c. preparation of criminal charges or ***criminal prosecution*** would be ***considerably impeded***
- ***Best Practice:*** Information at the time of initiating labor law action or filing criminal charges (whichever is earlier)
- ***Balancing of interests always necessary*** on a case by case basis
- Identity of whistleblower not to be disclosed as a matter of principle
- ***Documentation*** of reasons for information delay and balancing of interests in case file

## Retention / Deletion Periods (Sec. 11(1), (5) HinSchG)

- Documentation to be deleted ***no later than two years*** after completion of the procedure
- Documentation must be kept in a ***permanently retrievable manner*** until it is deleted
- ***Best Practice:*** Restricted access to the case file & logging of accesses incl. access policy

The Data Protection Officer should always be consulted in the event of any ambiguities regarding privacy or inquiries from data subjects in connection with incoming reports.



**DataGuard** is a Compliance software company focused on Data Privacy and Information Security. As a European leader in the Compliance SaaS category, we enable over thousands of SMB and Corporate customers to automate and operationalize Privacy, InfoSec, and Compliance ("PIC") with ease. Our end-to-end SaaS solution drastically reduces the time and money companies spend to comply with privacy legislation such as GDPR, manage consents and preferences, and obtain infosec certifications such as ISO 27001. This enables our customers to focus on their core business, create value through trust and compliance, whilst mitigating risks and preventing breaches. We have offices globally in Munich, Berlin, London, and Vienna.

**Let's talk about your challenges and define first steps on your compliance journey:**

**Contact us**

## You might also like:

→ **Webinar: Whistleblowing 101**

→ **A report pops up - now what? 12 steps to successful case management**