DataGuard

PRIVACY CHEAT SHEET

WHISTLE-BLOWING

Was ist aus Datenschutzsicht bei eingehenden Hinweisen zu beachten?

DataGuard | Privacy Cheat Sheet

Whistleblowing

Was ist aus Datenschutzsicht bei eingehenden Hinweisen zu beachten?

Information des Hinweisgebers (Art. 13 DSGVO)

- muss ***zum Zeitpunk der Erhebung*** erfolgen
- bei tool-gestützten Hinweisgebersystemen Datenschutzhinweise auf der Landingpage
- daneben auch als Link in Eingangsbestätigung an Hinweisgeber

Information Beschuldigte/Beteiligte (Art. 14 DSGVO)

- nur möglich, wenn identifizierbar & erreichbar
- grds. ***spätestens 1 Monat*** nach Eingang des entsprechenden Hinweises bzw. ***zum Zeitpunkt der ersten Kommunikation*** mit Beschuldigten/ Beteiligten
- Verzögerung ggf. möglich

mögliche Rechtsgrundlagen der Verarbeitung

- HinSchG anwendbar: Art. 6 Abs. 1 S. 1 lit. c DSGVO iVm § 10 HinSchG
- HinSchG nicht anwendbar: Art. 6 Abs. 1 S. 1 lit. f DSGVO
- bei Straftaten im Beschäftigungsverhältnis: § 26 Abs. 1 S. 2 BDSG
- Übermittlung der Daten an Dritte (auch andere Konzerngesellschaften) nur bei Erforderlichkeit (z.B. lokale Sachverhaltsaufklärung in einem anderen Land, Strafverfolgungsbehörde) zulässig

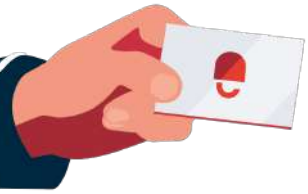
Verzögerung Information Beschuldigter/Beteiligter (Art. 14 Abs. 5 lit. b DSGVO, § 29 Abs. 1 S. 1 BDSG)

- solange (ein Grund ausreichend):
  a. Gefahr besteht, dass durch Information ***Sachverhalt nicht (mehr) aufgeklärt*** werden kann,
  b. Geltendmachung, Ausübung oder Verteidigung ***zivilrechtl. Ansprüche beeinträchtigt*** würde,
  c. Vorbereitung von Strafanzeigen bzw. ***Strafverfolgung erheblich erschwert*** würden
- ***Best Practice:*** Information zum Zeitpunkt der Einleitung arbeitsrechtlicher Schritte bzw. Stellen einer Strafanzeige (je nachdem, was früher erfolgt)
- ***Interessenabwägung*** im Einzelfall ***immer erforderlich***
- Identität des Hinweisgebers grds. nicht preiszugeben
- ***Dokumentation*** der Gründe für Informations-verzögerung und Interessenabwägung in Fallakte

Aufbewahrungsfristen/Löschpflichten (§ 11 Abs. 1, 5 HinSchG)

- Dokumentation ***spätestens zwei Jahre*** nach Abschluss des Verfahrens zu löschen
- bis zur Löschung ist Dokumentation in ***dauerhaft abrufbarer Weise*** vorzuhalten
- ***Best Practice:*** Sperren der Fallakte (eingeschränkter Zugriff) & Logging der Zugriffe

Bei Unklarheiten in puncto Datenschutz oder Betroffenenanfragen im Zusammenhang eingehender Hinweise sollte stets der Datenschutzbeauftragte konsultiert werden.



DataGuard ist ein Compliance-Software-Unternehmen mit Fokus auf Datenschutz und Informationssicherheit. Als einer der europäischen Marktführer im Bereich Compliance-SaaS ermöglicht DataGuard Tausenden KMU und Großunternehmen die unkomplizierte Operationalisierung von Datenschutz (Privacy), Informationssicherheit und Compliance (kurz: „PIC"). Mit seiner Komplettlösung reduziert DataGuard für Unternehmen Zeit und Kosten bei der Einhaltung von Datenschutzgesetzen wie der DSGVO, der Einholung und Verwaltung von Einwilligungen und Präferenzen oder beim Erhalten von Zertifizierungen wie der ISO 27001. So können sich Kunden auf ihr Kerngeschäft konzentrieren, Mehrwert durch Vertrauen und Compliance schaffen und gleichzeitig Risiken minimieren. DataGuard hat Standorte in München, Berlin, London und Wien.

Jetzt Termin vereinbaren, um über Ihre Herausforderungen zu sprechen und erste Schritte zu definieren:

Erstgespräch buchen

Weiterführende Ressourcen:

→ **On-Demand Webinar: Updates zur EU-Whistleblower-Richtlinie**

→ **Ein Hinweis erfolgt - und nun? In 12 Schritten zum erfolgreichen Case Management**

→ **EU-Whistleblowing-Richtlinie: Zentrale Herausforderungen & Einsichten eines Experten**

dataguard.de kontakt@dataguard.de +49 89 452 459-900

DataGuard