GDD-Praxishilfe HinSchG

Leitfaden zur DS-GVO-konformen Nutzung interner Meldestellen

INHALT

Vorwort

Das Hinweisgeberschutzgesetz (HinSchG) ist am 2. Juli 2023 in Kraft getreten und verpflichtet spätestens ab dem 17. Dezember 2023. Bis zu dieser Frist sind die Bestimmungen des Gesetzes umzusetzen. Das HinSchG verfolgt den Zweck, Personen zu schützen, die Missstände, Rechtsverstöße oder Gefahren für die Allgemeinheit, an die im HinSchG dafür vorgesehenen Stellen melden (sog. hinweisgebende Personen oder Whistleblower), vor Repressalien wie Kündigung oder anderen beruflichen Benachteiligungen. Das Gesetz richtet sich an Unternehmen sowie sonstige öffentliche Stellen. Bei der Errichtung sicherer Kanäle zur Meldung von Missständen unterscheidet das HinSchG zwischen externen Meldestellen, die von staatlicher Seite eingerichtet werden (§§ 19 ff. HinSchG) und internen Meldestellen beim Beschäftigungsgeber selbst (§§ 12 ff. HinSchG). Die Verpflichtung zur Einrichtung einer internen Meldestelle besteht für öffentliche und private Beschäftigungsgeber mit in der Regel mindestens 50 Beschäftigten (§ 12 Abs. 2 und 3 HinSchG). Die Einrichtung der internen Meldestelle nach dem HinSchG kann auch durch die Beauftragung Dritter, also externer Personen (sog. externalisierte interne Meldestelle) erfolgen (vgl. § 14 Abs. 1 S. 1 HinSchG). Die externe Meldestelle ist beim Bundesamt für Justiz eingerichtet (§ 19 Abs. 1 HinSchG). Das HinSchG sieht ein gleichberechtigtes Nebeneinander von internen und externen Meldestellen vor.[1] Hinweisgebende Personen haben die freie Wahl, ob sie Missstände zuerst an eine interne Meldestelle des Unternehmens oder der Behörde oder direkt an eine externe, staatlich eingerichtete Meldestelle melden möchten.

1 Thüsing/Lüneborg, § 7 Rn. 1.

I. Wer ist vom HinSchG betroffen?

Das HinSchG trat am 2. Juli 2023 in Kraft und sah für kleinere Unternehmen eine verspätet eintretende Frist zur Umsetzung der Voraussetzungen bis zum 17. Dezember 2023 vor. Seitdem sind die Regelungen des HinSchG für folgende Beschäftigungsgeber relevant:

>> **Unternehmen**: Ab 50 Beschäftigten sind Unternehmen verpflichtet, interne Meldestellen einzurichten.

>> **Öffentliche Stellen**: Alle öffentlichen Verwaltungen, Behörden, Gemeinden und juristische Personen des öffentlichen Rechts (z.B. Körperschaften, Anstalten oder Stiftungen) müssen Meldestellen unabhängig der Mitarbeiteranzahl einrichten.

>> **Externe Meldestellen**: Staatliche Stellen wie das Bundesamt für Justiz sind für die Einrichtung und den Betrieb externer Meldestellen verantwortlich.

II. Welche personenbezogenen Daten werden im Rahmen des HinSchG verarbeitet?

Im Rahmen des HinSchG werden zwangsläufig verschiedene personenbezogene Daten verarbeitet. So enthalten Meldungen – sofern die Meldungen nicht anonym abgegeben wurden – Angaben zum Hinweisgeber (Name, Kontaktdaten und arbeitsplatzbezogene Informationen wie z.B. die Stellung im Unternehmen oder der Behörde). Zudem können Daten etwaiger beschuldigter Personen erfasst werden, wie deren Name und Informationen über den gemeldeten Verstoß. Auch Dritte, die im Zusammenhang mit der Meldung genannt werden, wie Zeugen oder andere Beteiligte, können datenschutzrechtlich betroffene Personen i.S.d. Datenschutzrechts sein.

An eine Meldung an die interne Meldestelle schließen im weiteren Verlauf der Aufklärung der gemeldeten Rechtsverstöße oder Missstände weitere Verarbeitungen von personenbezogenen Daten an, die sich auf den Austausch zwischen Hinweisgeber und interner Meldestelle beziehen, wie der Inhalt von Gesprächen oder schriftlichen Mitteilungen (z.B. E-Mails).

III. Rechtsgrundlage der Datenverarbeitung

Nach einer Meldung an die interne Meldestelle sind bei einem begründeten Verdachtsfall interne Untersuchungen durchzuführen. Im Rahmen dieser Untersuchungen werden in der Regel personenbezogene Daten verarbeitet. Diese Datenverarbeitung muss auf einer rechtlichen Grundlage durchgeführt werden. Dabei kommen folgende Rechtsgrundlagen in Betracht:

Nach Art. 6 Abs. 1 lit. c) DS-GVO ist diejenige Verarbeitung rechtmäßig, die zur Erfüllung einer rechtlichen Verpflichtung erforderlich ist. Interne Meldestellen sind gem. der §§ 13 bis 24 HinSchG rechtlich zur Aufrechterhaltung von Meldekanälen, Bearbeitung von Meldungen und dem Ergreifen von Folgemaßnahmen verpflichtet, so dass sie die dazu erforderliche Verarbeitung personenbezogener Daten auf Art. 6 Abs. 1 lit. c) DS-GVO gestützt werden kann.[2] Die Datenverarbeitung muss somit die Meldung und Aufklärung der gemeldeten Ver-

2 BT-Drs. 20/4909, S. 56; Thüsing/Fischer, § 10 Rn. 1; Baade/Hößl, DStR 2023, 1265 (1267).

stöße ermöglichen.[3] Im Rahmen der Verarbeitung müssen spezifische und angemessene Maßnahmen zur Wahrung der Interessen der betroffenen Personen gem. § 22 Abs. 2 BDSG getroffen werden.

Abweichend von Art. 9 Abs. 1 DS-GVO ist die Datenverarbeitung besonderer Kategorien personenbezogener Daten gem. Art. 9 Abs. 2 lit. g) DS-GVO durch eine Meldestelle zulässig, wenn dies zur Erfüllung ihrer Aufgaben erforderlich ist.[4] Auch in diesem Fall muss die Meldestelle gem. § 22 Abs. 2 BDSG spezifische und angemessene Maßnahmen zur Wahrung der Interessen der betroffenen Person vorsehen.

Weiterhin kommt § 26 Abs. 1 S. 1 BDSG als Rechtsgrundlage der Datenverarbeitung in Betracht. Dafür muss ein hinreichender Verdacht eines nicht unerheblichen Rechtsverstoßes bestehen.[5] Sofern die internen Ermittlungen den Verdacht einer Straftat behandeln, sind die weiteren Voraussetzungen des § 26 Abs. 1 S. 2 BDSG zu beachten. Demnach müssen tatsächliche Anhaltspunkte bestehen, die den Verdacht nahelegen, dass die betroffene Person im Beschäftigungsverhältnis eine Straftat begangen hat (vgl. § 152 Abs. 2 StPO).[6] Zudem muss die Verarbeitung zur Aufdeckung der Straftat erforderlich sein und das schutzwürdige Interesse der oder des Beschäftigten an dem Ausschluss der Verarbeitung darf das Interesse an der Strafverfolgung nicht überwiegen.[7]

IV. Informationspflichten, Art. 13 und 14 DS-GVO

Werden bei der betroffenen Person personenbezogene Daten erhoben, so teilt der Verantwortliche der betroffenen Person aktiv zum Zeitpunkt der Datenerhebung oder vor einer zweckändernden Weiterverarbeitung die gebotenen Informationen gem. Art. 13 Abs. 1 – 3 DS-GVO mit.[8] Demnach muss der Hinweisgeber insbesondere über den Zweck der Datenverarbeitung informiert werden.

Zumeist beinhaltet eine Meldung auch Informationen der beschuldigten Person, die als personenbezogene Daten verarbeitet werden. Werden personenbezogene Daten einer Person nicht bei dieser selbst erhoben, entsteht grundsätzlich eine Informationspflicht gegenüber dieser Person gem. Art. 14 DS-GVO.[9] Eine solche Informationspflicht ist jedoch gem. Art. 14 Abs. 5 lit. b) S. 1 DS-GVO ausgeschlossen, wenn die Erteilung der Information die Verwirklichung der Ziele der Datenverarbeitung ernsthaft beeinträchtigt.[10] Da das Ziel der Datenverarbeitung im Zuge des Meldeverfahrens unter anderem die Aufklärung des erhobenen Vorwurfs ist, stellt die Geheimhaltung des Vorwurfs gegenüber der beschuldigten Person zur lückenlosen Aufarbeitung der Meldung ein unabdingbares Erfordernis dar.

Darüber hinaus ist gem. § 29 Abs. 1 S. 1 BDSG die Pflicht zur Information nach Art. 14 DS-GVO ausgeschlossen, soweit durch ihre Erfüllung Informationen offenbart würden, die ihrem Wesen nach, insbesondere wegen der

3 Ammon, PinG 2023, 67 (71).
4 BT-Drs. 20/4909, S. 56.
5 Gola/Heckmann/Gola/Pötters, § 26 Rn. 58.
6 Siehe Näheres in Schwartmann/Jaspers/Thüsing/Kugelmann/Schmidt/Thüsing, DS-GVO/BDSG, § 26 Rn. 31 ff.; Gola/Heckmann/Gola/Pötters, DS-GVO/BDSG, § 26 Rn. 58 ff.
7 Schwartmann/Jaspers/Thüsing/Kugelmann/Schmidt/Thüsing, DS-GVO/BDSG, § 26 Rn. 33; in Gola/Heckmann/Gola/Pötters, DS-GVO/BDSG, § 26 Rn. 61; Sydow/Marsch/Tiedemann, DS-GVO/BDSG, § 26 Rn. 35.
8 Schwartmann/Jaspers/Thüsing/Kugelmann/Schwartmann/Schneider, Art. 13 Rn. 38.
9 Schwartmann/Jaspers/Thüsing/Kugelmann/Schwartmann/Schneider, Art. 14 Rn. 1.
10 Schwartmann/Jaspers/Thüsing/Kugelmann/Schwartmann/Schneider, Art. 14 Rn. 74; Gola, RDV 2023, 213 (220).

überwiegenden berechtigten Interessen eines Dritten, geheim gehalten werden müssen.[11] Da das Geheimhaltungsinteresse der hinweisgebenden Person im Fall einer berechtigten Meldung das Informationsinteresse des Beschuldigten überwiegt, ist die Informationspflicht i.S.d. Art. 14 DS-GVO aufgrund § 29 Abs. 1 S. 1 BDSG ausgeschlossen.[12]

V. Transparenzpflichten nach dem HinSchG

Weiterhin sieht das HinSchG eigene Informationspflichten für Unternehmen vor. § 7 Abs. 3 S. 2 HinSchG verlangt, dass Beschäftigungsgeber für die Beschäftigten klare und leicht zugängliche Informationen **über die Nutzung des internen Meldekanals** bereitstellen müssen. Gem. § 13 Abs. 2 HinSchG besteht zudem für interne Meldestellen die Pflicht, für Beschäftigte klare und leicht zugängliche Informationen **über externe Meldestellen** und einschlägige Meldeverfahren von Organen, Einrichtungen oder sonstigen Stellen der Europäischen Union bereitzustellen. Diese Informationspflicht wird durch die Regelung des § 26 Abs. 4 HinSchG flankiert, indem externe Meldestellen die gebotenen Informationen selbst auf ihrer Website bereitstellen müssen.[13]

VI. Auskunftsanspruch, Art. 15 DS-GVO

Die betroffene Person hat gem. Art. 15 Abs. 1 und 3 DS-GVO das Recht, von dem Verantwortlichen eine Bestätigung darüber zu verlangen, dass sie betreffende personenbezogene Daten verarbeitet werden. Liegt eine Datenverarbeitung personenbezogener Daten vor, so hat die betroffene Person ein Recht auf Auskunft und ein Recht auf Kopie über diese personenbezogenen Daten.[14] Im Kontext des HinSchG ist vor allem die Frage relevant, ob die beschuldigte Person Auskunft über die Verarbeitung ihrer personenbezogenen Daten verlangen und insbesondere den Namen des Hinweisgebers erfahren kann.

Der Auskunftsanspruch steht jedoch mit dem Vertraulichkeitsgebot gem. § 8 HinSchG in einem Spannungsverhältnis.[15] Demnach haben Meldestellen die Vertraulichkeit der Identität der hinweisgebenden Personen (§ 8 Abs. 1 Nr. 1), der Personen, die Gegenstand der Meldungen sind (§ 8 Abs. 1 Nr. 2) und sonstige in der Meldung genannten Personen (§ 8 Abs. 1 Nr. 3) zu wahren. Der Anspruch auf Auskunftserteilung besteht gem. § 29 Abs. 1 S. 2 BDSG nicht, soweit durch die Auskunft Informationen offenbart würden, die nach einer Rechtsvorschrift oder ihrem Wesen nach, insbesondere wegen der überwiegenden berechtigten Interessen eines Dritten, geheim gehalten werden müssen.[16] Die berechtigten Interessen des Dritten überwiegen dann, wenn der Hinweisgeber eine berechtigte Meldung i.S.d. HinSchG abgegeben hat.[17] Meldet die hinweisgebende Person vorsätzlich oder grob fahrlässig unrichtige

11 Taeger/Gabel/Louven, § 29 BDSG Rn. 1.
12 BT-Drs. 20/5992, S. 59.
13 Ammon, PinG 2023, 67 (70).
14 Schwartmann/Jaspers/Thüsing/Kugelmann/Schwartmann/Klein/Peisker, DS-GVO/BDSG, Art. 15 Rn. 1.
15 Bayreuther, NZA-Beilage 2022, 20 (26).
16 Schwartmann/Jaspers/Thüsing/Kugelmann/Schwartmann/Klein/Peisker, DS-GVO/BDSG, Art. 15 Rn. 90; Bruns, NJW 2023, 1609 (1616).
17 Bayreuther, NZA-Beilage 2022, 20 (25).

Informationen über Verstöße, wird die Identität der hinweisgebenden Person gem. § 9 Abs. 1 HinSchG nicht geschützt. In diesem Fall ist der Auskunftsanspruch nicht gem. § 29 Abs. 1 S. 2 BDSG ausgeschlossen.[18]

VII. Verantwortlichkeit

Die Frage der datenschutzrechtlichen Verantwortlichkeit stellt sich im Rahmen des HinSchG insbesondere in den Fällen, in denen ein Dritter die Rolle der internen Meldestelle übernimmt (externalisierte interne Meldestelle). Das können zum Beispiel externe Dienstleister oder Rechtsanwälte sein.[19] Die Einstufung des Dritten in die verschiedenen datenschutzrechtlichen Rollen der Verantwortlichkeit ist insofern relevant, da mit ihnen unterschiedliche Anforderungen bestehen. So muss bspw. ein Vertrag über eine Auftragsdatenverarbeitung i.S.d. Art. 28 Abs. 3 S. 1 DS-GVO oder eine Vereinbarung zur gemeinsamen Verantwortlichkeit gem. Art. 26 Abs. 1 S. 2 DS-GVO geschlossen werden.[20]

Die Frage, ob die externalisierte Meldestelle als (gemeinsamer) Verantwortlicher oder Auftragsverarbeiter agiert, kann nicht pauschal beantwortet werden, sondern ist nach den jeweiligen Umständen des Einzelfalles zu bestimmen.[21] Die Weisungsgebundenheit sowie das Bestehen eines Entscheidungsspielraums sind die Abgrenzungskriterien zwischen Auftragsverarbeiter und Verantwortlichem.[22]

Oftmals werden von externen Dienstleistern Services angeboten, bei denen Meldekanäle für die Meldungen zur Verfügung, z.B. in Form eines digitalen Briefkastens, gestellt werden. Ein solcher Service stellt nur dann eine Auftragsverarbeitung dar, wenn die Meldungen ohne weitere Aufarbeitung durch den Dienstleister an die verantwortliche Stelle weitergeleitet werden. Ein digitaler Briefkasten stellt für sich allein keine externalisierte interne Meldestelle dar. Denn dieser führt die in den §§ 13 bis 24 HinSchG aufgeführten Aufgaben der internen Meldestelle nicht weiter aus. Er dient lediglich als Hilfswerkzeug zur digitalen Entgegennahme der Meldungen.

Soweit ein externer Dienstleister die Meldungen der hinweisgebenden Personen sammelt und in Form eines Berichts an das Unternehmen weiterleitet, steht dem Dienstleister dabei ein eigener Ermessensspielraum zu. Die Einbindung eines externen Dienstleisters stellt daher keine Auftragsverarbeitung nach Art. 28 DS-GVO dar. Auch ein **Rechtsanwalt** ist nicht als Auftragsverarbeiter einzustufen, da er aufgrund seines Berufes keinen Weisungen unterliegt und ihm ein eigener Entscheidungsspielraum hinsichtlich der Datenverarbeitung zusteht.[23]

Werden Meldungen eines Hinweisgebers durch den Dienstleister auf deren Plausibilität geprüft und dem Beschäftigungsgeber ohne Einwirkungsmöglichkeit zur Verfügung gestellt, kann nicht von einer Gemeinsamkeit der Zweckbestimmung gesprochen werden.[24] In diesem Fall sind Beschäftigungsgeber und Dritter zwei unabhängige Verantwortliche.

18 Taeger/Gabel/Louven, § 29 Rn. 6.
19 Rüdiger/Adelberg, K&R 2023, 172 (173).
20 Schwartmann/Jaspers/Thüsing/Kugelmann/Kremer, Art. 28 Rn. 93; Schwartmann/Jaspers/Thüsing/Kugelmann/Kremer, Art. 26 Rn. 68. Näheres zu den (Mindest-) Inhalten dieser Vereinbarung, vgl. Schwartmann/Jaspers/Thüsing/Kugelmann/Kremer, Art. 26 Rn. 75 ff.
21 Rüdiger/Adelberg, K&R 2023, 172 (175).
22 Schwartmann/Jaspers/Thüsing/Kugelmann/Kremer, Art. 26 Rn. 59.
23 Rüdiger/Adelberg, K&R 2023, 172 (173f.).
24 Beispiel nach Rüdiger/Adelberg, K&R 2023, 172 (174).

Handlungsempfehlung:
Mangels Weisungsgebundenheit sind externe Dienstleister im Rahmen ihrer Tätigkeit als externalisierte interne Meldestelle nicht als Auftragsverarbeiter einzuordnen. Die Dienstleister und verantwortlichen Stellen sind zwei unabhängige Verantwortliche i.S.d. DS-GVO.

VIII. Dokumentation

Die Personen, die in einer Meldestelle für die Entgegennahme von Meldungen zuständig sind, dokumentieren alle eingehenden Meldungen in dauerhaft abrufbarer Weise unter Beachtung des Vertraulichkeitsgebots (§ 8), vgl. § 11 Abs. 1 HinSchG. Bei telefonischen Meldungen oder Meldungen mittels einer anderen Art der Sprachübermittlung darf eine dauerhaft abrufbare Tonaufzeichnung des Gesprächs oder dessen vollständige und genaue Niederschrift (Wortprotokoll) nur mit Einwilligung der hinweisgebenden Person erfolgen.[25] Liegt eine solche Einwilligung nicht vor, ist die Meldung durch eine von der für die Bearbeitung der Meldung verantwortlichen Person zu erstellende Zusammenfassung ihres Inhalts (Inhaltsprotokoll) zu dokumentieren, § 11 Abs. 2 HinSchG.

IX. Aufbewahrungsfrist

Die Dokumentation wird drei Jahre nach Abschluss des Verfahrens gelöscht, § 11 Abs. 5 S. 1 HinSchG. Die Dokumentation kann länger aufbewahrt werden, um die Anforderungen nach diesem Gesetz oder nach anderen Rechtsvorschriften zu erfüllen, solange dies erforderlich und verhältnismäßig ist, § 11 Abs. 5 S. 2 HinSchG.

X. Erforderlichkeit einer Datenschutz-Folgenabschätzung

Hat eine Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge, so führt der Verantwortliche vorab eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten durch, Art. 35 Abs. 1 S. 1 DS-GVO.[26]

Eine Meldung über den internen Meldekanal beinhaltet meist hochsensible Daten des Hinweisgebers (sofern er seine Meldung nicht anonym abgibt), des Beschuldigten und ggf. eines Zeugen oder Dritten. Die unsachgem.e Handhabung dieser Daten kann für die Beteiligten verheerende Folgen nach sich ziehen. Daher unterliegt das Verfahren zur Meldung von Missständen nach dem HinSchG wegen des besonders hohen Risikos für die Rechte und

25 Thüsing/Fischer, § 11 Rn. 11.

26 DSK, Orientierungshilfe der Datenschutzaufsichtsbehörden zu Whistleblowing-Hotlines: Firmeninterne Warnsysteme und Beschäftigtendatenschutz, S. 12, abrufbar unter: https://www.datenschutzkonferenz-online.de/media/oh/20181114_oh_whistleblowing_hotlines.pdf.

Freiheiten natürlicher Personen einer Datenschutz-Folgenabschätzung.[27]

Handlungsempfehlung:
Es ist zwingend eine Datenschutz-Folgenabschätzung vorzunehmen.

XI. Einhaltung der Grundsätze aus Art. 25 und 32 DS-GVO

Nach den Grundsätzen des Art. 25 Abs. 1 DS-GVO treffen Verantwortliche Maßnahmen, die den Datenschutz bereits bei der Entwicklung von Prozessen und Systemen integrieren („Datenschutz durch Technikgestaltung") und standardmäßig nur die für den jeweiligen Zweck notwendigen personenbezogenen Daten verarbeiten („Datenschutz durch datenschutzfreundliche Voreinstellungen"). Dies erfordert die Implementierung geeigneter technischer und organisatorischer Maßnahmen, um die Einhaltung der Datenschutzprinzipien von Anfang an und dauerhaft sicherzustellen.

Bei der Erstellung eines Hinweisgebersystems sollten daher folgende Punkte sichergestellt sein.

>> **Datenminimierung**: Es sollten nur die Daten erhoben werden, die für die Bearbeitung der Meldung erforderlich sind.
>> **Zugriffsbeschränkung**: Der Zugang zu den Meldungen sollte auf eine kleine, notwendige Gruppe von Personen beschränkt werden, um den Schutz der sensiblen Informationen zu gewährleisten.
>> **Pseudonymisierung und Verschlüsselung**: Die Identität des Hinweisgebers sollte durch Pseudonymisierung geschützt und alle Daten sollten verschlüsselt gespeichert werden, um unbefugten Zugriff zu verhindern.
>> **Transparenz**: Hinweisgeber sollten über die Verarbeitung ihrer Daten informiert werden, einschließlich der Zwecke, der rechtlichen Grundlage und der Rechte, die ihnen zustehen.
>> **Sicherheitsmaßnahmen**: Es sollten technische und organisatorische Maßnahmen ergriffen werden, um die Sicherheit der Daten während der Übermittlung und Speicherung zu gewährleisten, wie z.B. die Nutzung sicherer Kommunikationskanäle (Ende-zu-Ende-Verschlüsselung).
>> **Datenschutzfreundliche Voreinstellungen**: Standardmäßig sollten die strengsten Datenschutzoptionen aktiviert sein, z.B. dass Meldungen anonym abgegeben werden können, wenn der Hinweisgeber dies wünscht.

XII. Datenschutzbeauftragte als interne Meldestelle

Gem. § 15 Abs. 1 S. 1 HinSchG müssen die mit einer internen Meldestelle betrauten Personen bei der Ausübung ihrer Tätigkeit unabhängig sein. Allerdings dürfen diese Personen neben ihrer Tätigkeit als interne Meldestelle auch andere Aufgaben und Pflichten übernehmen, vgl. § 15 Abs. 1 S. 2 HinSchG. Dabei ist sicherzustellen, dass derartige Aufgaben und Pflichten nicht zu Interessenkonflikten mit der Tätigkeit

27 So auch Bayreuther, PinG 2023, 67 (71); Fehr, ZD 2022, 256 (259).

als interne Meldestelle führen, § 15 Abs. 1 S. 3 HinSchG.

Auch der Datenschutzbeauftragte kann neben seiner Tätigkeit als Überwachungs- und Kontrollinstanz andere Aufgaben im Unternehmen übernehmen, Art. 38 Abs. 6 S. 1 DS-GVO.[28] Jedoch darf er, wie auch die Person der internen Meldestelle, diese Aufgaben nur übernehmen, wenn zu seiner Tätigkeit als Datenschutzbeauftragter keine Interessenkonflikte entstehen.[29] Es stellt sich somit die Frage, ob der Datenschutzbeauftragte als interne Meldestelle eingesetzt werden kann oder ob dieser Einsetzung Interessenkonflikte entgegenstehen.

Erwägungsgrund 56 der HinSch-RL[30] führt exemplarisch einige Personen eines Unternehmens auf, die die Rolle der internen Meldestelle wahrnehmen könnten. Zwar wird dort unter anderem auch der Datenschutzbeauftragte als zulässige Person genannt, der zugleich die Rolle der internen Meldestelle bekleiden kann.[31] Jedoch besteht sowohl bei KMU als auch bei großen Unternehmen eine erhöhte Gefahr von Interessenkonflikten.

1. Zeitlicher Umfang

Zunächst könnte der zeitliche Umfang der beiden Tätigkeiten zu einem Interessenkonflikt führen. Der Beschäftigungsgeber ist gem. Art. 38 Abs. 2 DS-GVO dazu verpflichtet, dem Datenschutzbeauftragten alle „erforderlichen Ressourcen“ zur Erfüllung seiner Aufgaben zur Verfügung zu stellen. Dazu gehört auch das Bereitstellen von genügend zeitlichen Ressourcen.[32] Es ist also zu befürchten, dass die gleichzeitige Wahrnehmung beider Ämter zu einer Vernachlässigung eines Amtes führt. Dies stellt einen Interessenkonflikt dar, sodass die gleichzeitige Ausübung der Ämter unzulässig ist. In einem größeren Unternehmen ist somit durchgehend zu prüfen, ob dem Datenschutzbeauftragten bzw. der internen Meldestelle genügend zeitliche Ressourcen zur Aufgabenerfüllung eingeräumt werden.[33]

Außerdem besteht im Fall einer zeitlichen Überlastung des Datenschutzbeauftragten bzw. der internen Meldestelle die Gefahr, dass das interne Meldeverfahren nur langsam vorangeht und so die hinweisgebende Person den Weg über eine externe Meldestelle sucht. Dies führt dazu, dass die jeweiligen Missstände im Unternehmen nicht intern gelöst werden können, sondern direkt ein behördliches (Bußgeld-) Verfahren droht.

2. Verschwiegenheit

Weiterhin könnte das unterschiedlich gelagerte Niveau an Verschwiegenheitspflichten in DS-GVO und HinSchG einen Interessenkonflikt bei der zeitgleichen Ausübung beider Ämter hervorrufen. Nach Art. 38 Abs. 5 DS-GVO ist der Datenschutzbeauftragte bei der Erfüllung seiner Aufgaben an die Wahrung der Geheimhal-

28 Schwartmann/Jaspers/Thüsing/Kugelmann/Jaspers/Reif, Art. 38 Rn. 28.39; Franck, GDD-Ratgeber Datenpannen, S. 61 f.
29 Schwartmann/Jaspers/Thüsing/Kugelmann/Jaspers/Reif, Art. 38 Rn. 28.
30 RL (EU) 2019/1937.
31 Dies bezieht sich jedoch nur - wie auch die Gesetzesbegründung der Bundesregierung - auf die Ausübung beider Ämter in kleineren Unternehmen, vgl. BT-Drs. 20/3442, S. 78; Kritisch dazu: Kühling/Buchner/Bergt/Herbort, Art. 38 Rn. 42a; Fehr, ZD 2022, 256 (256); Stuke/Fehr, BB 2021, 2740; Leibold, ZD-Aktuell 2022, 01333; LfDI BW, FAQ – Hinweisgeberschutzgesetz, https://www.baden-wuerttemberg.datenschutz.de/faq-hinweisgeberschutzgesetz/; nicht so streng Gola, RDV 2023, 213 (219 f.).
32 Schwartmann/Jaspers/Thüsing/Kugelmann/Jaspers/Reif, Art. 38 Rn. 10.
33 So auch LfDI BW, FAQ – Hinweisgeberschutzgesetz, https://www.baden-wuerttemberg.datenschutz.de/faq-hinweisgeberschutzgesetz/.

tung oder der Vertraulichkeit gebunden, wobei die nähere Ausgestaltung dieser Verpflichtung dem Unionsrecht bzw. Recht der Mitgliedstaaten überlassen ist.[34] Der deutsche Gesetzgeber machte von dieser Gestaltungsmöglichkeit in Form von § 6 Abs. 5 S. 2 BDSG Gebrauch. Dieser statuiert, dass der Datenschutzbeauftragte zur Verschwiegenheit über die Identität der betroffenen Person sowie über Umstände, die Rückschlüsse auf die betroffene Person zulassen, verpflichtet ist, soweit er nicht davon befreit ist.

Auch das HinSchG sieht besondere Verschwiegenheits- und Geheimhaltungspflichten vor. So müssen die Meldestellen die Identität der hinweisgebenden Person, der Personen, die Gegenstand der Meldungen oder sonstig in der Meldung genannt sind, vertraulich behandeln, vgl. § 8 Abs. 1 HinSchG. Allerdings gilt diese Verschwiegenheitspflicht nach dem HinSchG nicht uneingeschränkt. Denn nach § 9 Abs. 1 HinSchG gilt diese nicht, wenn die hinweisgebende Person vorsätzlich oder grob fahrlässig unrichtige Informationen über Verstöße meldet. Im Vergleich zur DS-GVO, nach der eine solche Ausnahme auf die Vertraulichkeit in Bezug auf die personenbezogenen Daten der betroffenen Personen nicht angewendet werden kann, besteht somit ein unterschiedliches Geheimhaltungsniveau. Denkbar sind demnach Fälle, in denen die interne Meldestelle rechtmäßig unter Berufung auf § 9 Abs. 2 - 4 HinSchG die Identität der hinweisgebenden Person preisgibt und somit gegen das der DS-GVO innewohnende Vertraulichkeitsgebot verstößt. Dieses unterschiedliche Geheimhaltungsniveau zwischen DS-GVO und HinSchG könnte bei gleichzeitiger Ausübung beider Ämter ebenfalls einen Interessenkonflikt darstellen.[35]

3. Faktische Selbstkontrolle

Zudem besteht bei der gleichzeitigen Ausübung beider Rollen die akute Gefahr einer faktischen Selbstkontrolle des Datenschutzbeauftragten. Aus Art. 37 Abs. 1 lit. b) i.V.m. Art. 39 Abs. 1 lit. b) DS-GVO ergibt sich, dass die primäre Aufgabe des Datenschutzbeauftragten darin liegt, die verantwortliche Stelle zu überwachen.[36] Daraus folgt zwangsläufig, dass Datenschutzbeauftragter und verantwortliche Stelle nicht dieselbe Person sein dürfen, da ansonsten ein Interessenkonflikt in Form einer faktischen Selbstkontrolle vorläge.[37] Die interne Meldestelle legt das jeweilige Meldeverfahren im Unternehmen (§ 17 HinSchG) sowie angemessene Folgemaßnahmen (§ 18 HinSchG) fest. Sie bestimmt die Zwecke und Mittel der Datenverarbeitung und ist somit als verantwortliche Stelle im Sinne des Art. 4 Nr. 7 DS-GVO einzustufen. Die gleichzeitige Ausübung beider Stellen führte somit zu einer faktischen Selbstkontrolle.[38] Da Meldungen nach dem HinSchG nicht selten sensible Daten i.S.v. Art. 10 DS-GVO beinhalten und die im Rahmen der internen Ermittlungen durchgeführten Datenverarbeitungen mit Blick auf den damit verbundenen Eingriff in das Persönlichkeitsrecht einer besonders sorgfältigen Prüfung bedürfen, ist dies besonders proble-

34 Schwartmann/Jaspers/Thüsing/Kugelmann/Jaspers/Reif, DS-GVO/BDSG, Art. 38 Rn. 35 m.w.N.

35 So auch Leibold, ZD-Aktuell 2022, 01333.

36 Schwartmann/Jaspers/Thüsing/Kugelmann/Schmidt/Thüsing, DS-GVO/BDSG, Art. 39 Rn. 14.

37 Näheres dazu Schwartmann/Jaspers/Thüsing/Kugelmann/Jaspers/Reif, DS-GVO/BDSG, Art. 38 Rn. 36; GDD-Ratgeber Datenpannen, S. 34 ff.

38 Ähnlich Cornelius, PinG 2022, 244 (247); LfDI BW, FAQ – Hinweisgeberschutzgesetz, https://www.baden-wuerttemberg.datenschutz.de/faq-hinweisgeberschutzgesetz/; Ehmann/Selmayr/Heberlein, DS-GVO, Art. 38 Rn. 27 sieht zwar Konfliktpotenzial, geht aber davon aus, dass durch organisatorische Maßnahmen entgegengewirkt werden kann.

matisch.[39] Diese Selbstkontrolle stellt einen Interessenkonflikt nach Art. 38 Abs. 6 S. 2 DS-GVO dar. Eine gleichzeitige Ausübung beider Rollen ist somit unzulässig.

4. Fazit

Die aufgezeigten Interessenkonflikte und Risiken verdeutlichen, dass durch die Einbindung einer weiteren Person und die klare Benennung der einzelnen Pflichten diese Risiken umgangen bzw. verringert werden können. Insbesondere wegen der faktischen Selbstkontrolle wird die klare personelle Trennung von Datenschutzbeauftragtem und interner Meldestelle empfohlen.

Literatur

Kommentare

>> Thüsing (Hrsg.), Hinweisgeberschutzgesetz, München 2024

Aufsätze

Ammon, Das Hinweisgeberschutzgesetz für Unternehmen – Umsetzung der EU-Whistleblower-Richtlinie, PinG 2023, S. 67; Baade/Hößl, Arbeits- und compliancerechtlicher Handlungsbedarf unter dem neuen Hinweisgeberschutzgesetz (Teil II), DStR 2023, S. 1265; Bayreuther, Whistleblowing und das neue Hinweisgeberschutzgesetz, NZA-Beilage 2022, S. 20; Bruns, Das neue Hinweisgeberschutzgesetz, NJW 2023, S. 1609; Cornelius, Interessenkonflikte bei betrieblichen Datenschutzbeauftragten, PinG 2022, S. 244; Fehr, Whistleblowing und Datenschutz – ein unlösbares Spannungsfeld? Praktischer Diskurs der EU-Whistleblower-RL und der DS-GVO im Kontext des Hinweisgebermanagements, ZD 2022, S. 256; Gola, Hinweisgeberschutz nach dem HinSchG, dem LkSG und weiteren bereichsspezifischen Melderegelungen – ein Überblick, RDV 2023, S. 213; Leibold, Überblick: Betrieblicher Datenschutzbeauftragter als interne Meldestelle i.S.d. HinSchG-E – ein Interessenkonflikt?, ZD-Aktuell 2022, 01333; Rüdiger/Adelberg, Datenschutzrechtliche Herausforderungen des neuen Hinweisgeberschutzgesetzes, K&R 2023, S. 172; Stuke/Fehr, Whistleblowing und seine betrieblichen Fallstricke – Eine Handlungsempfehlung für ein professionelles Hinweisgebermanagement, BB 2021, 2740.

Aufsichtsbehörden

>> Datenschutzkonferenz, Orientierungshilfe der Datenschutzaufsichtsbehörden zu Whistleblowing-Hotlines: Firmeninterne Warnsysteme und Beschäftigtendatenschutz

>> LfDI BW, FAQ – Hinweisgeberschutzgesetz

39 Ähnlich Cornelius, PinG 2022, 244 (248); auch Kascherus, ZD 2024, 429 (432).

Mitglied werden? Mehr Informationen?

https://www.gdd.de/service/mitglied-werden oder eine E-Mail an: info@gdd.de

Eine Mitgliedschaft bietet wesentliche Vorteile:

>> Mitglieder-Nachrichten mit aktuellen Fachinformationen in Form eines monatlichen Newsletters
>> Bezug der Fachzeitschrift RDV (Recht der Datenverarbeitung)
>> Beratung bei konkreten Einzelfragen
>> Zugriff auf Rechtsprechungs- und Literaturarchiv in der GDDcommunity
>> Online-Service „DataAgenda Plus“ (Muster, Checklisten, RDV ONLINE Archiv, Arbeitspapiere etc.)
>> Mitarbeit in Erfahrungsaustausch- und Arbeitskreisen
>> Teilnahme an den kostenfreien GDD-Informationstagen sowie Vergünstigungen bei Seminaren u.v.m.

Schließen Sie sich unseren mehr als 3.600 Mitgliedern an. Eine Mitgliedschaft erhalten Sie schon ab 150,- EUR/Jahr für Privatpersonen und ab 300,- EUR/Jahr für Firmen.

Diese Praxishilfe wurde erstellt durch:

Clemens Loke
Referent, GDD e.V., Bonn

Satz: C. Kopp, GDD-Geschäftsstelle, Bonn
Stand: Version 1.0 (Februar 2025)

Herausgeber:
Gesellschaft für Datenschutz und Datensicherheit (GDD e.V.)
Heinrich-Böll-Ring 10
53119 Bonn

Tel.: +49 2 28 96 96 75-00
www.gdd.de
info@gdd.de