MARKUS LANG

Datenschutzrechtliche Implikationen des Hinweisgeberschutzgesetzes

Datenschutzmanagement
Vertraulichkeitsgebot
Auskunft
Datenschutz-Folgenabschätzung
Meldestellen

Einrichtung und Betrieb eines Hinweisgebersystems unter Beachtung der datenschutzrechtlichen Vorgaben

■ Das Hinweisgeberschutzgesetz (HinSchG) ist am 2.7.2023 in Kraft getreten. Es sieht die Einrichtung sowie den Betrieb von Hinweisgebersystemen vor und unterwirft Meldestellen einem strengen, aber nicht ausnahmslosen Vertraulichkeitsgebot. Die Regelungen des HinSchG lassen nicht nur das Spannungsfeld von Hinweisgeber- und Datenschutz erkennen, sondern sind auch darüber hinaus datenschutzrechtlich relevant. Zum einen erstreckt sich der Anwendungsbereich dieses Gesetzes auf Verstöße gegen datenschutzgesetzliche Vorgaben. Zum anderen werden regelmäßig personenbezogene Daten von Hinweisgebern, möglichen Tätern und Dritten verarbeitet. In diesem Beitrag werden die datenschutzrechtlichen Implikationen des HinSchG aufgegriffen und die wesentlichen datenschutzrechtlichen Aspekte erläutert, die bei der Einrichtung und dem Betrieb eines Hinweisgebersystems nach HinSchG in der Praxis zu beachten sind.
Lesedauer: 22 Minuten

■ The German Whistleblower Protection Act (HinSchG) came into force on 2 July 2023. It provides for the establishment and operation of whistleblower systems and subjects reporting centres to a strict, but not absolute, confidentiality requirement. The provisions of the German Whistleblower Protection Act not only reveal the tension between whistleblower protection and data protection but are also relevant from a data protection perspective in other respects. On the one hand, the scope of application of this law extends to breaches of data protection regulations. On the other hand, personal data of whistleblowers, possible perpetrators and third parties are regularly processed. This article addresses the data protection implications of the German Whistleblower Protection Act and explains the key aspects of data protection law that need to be considered in practice when setting up and operating a whistleblower system in accordance with the German Whistleblower Protection Act.

I. Ausgangspunkt – Kernelemente des HinSchG

Das „Gesetz für einen besseren Schutz hinweisgebender Personen sowie zur Umsetzung der Richtlinie zum Schutz von Personen, die Verstöße gegen das Unionsrecht melden" ist nach einem langen und bemerkenswerten Gesetzgebungsverfahren beschlossen und am 2.6.2023 verkündet worden.[1] Mit dem Hinweisgeberschutzgesetz (HinSchG) und den korrespondierenden Anpassungen bestehender Regelungen soll die sog. Whistleblower-RL (RL (EU) 2019/1937)[2] umgesetzt und der bislang lückenhafte und unzureichende Schutz von hinweisgebenden Personen nachhaltig verbessert werden.[3] Um dieses Ziel zu erreichen, hat der Gesetzgeber im HinSchG insbesondere die Einrichtung und den Betrieb interner und externer Melde- bzw. Hinweisgebersysteme (§§ 12 ff., 19 ff. HinSchG), den Umgang mit Meldungen einschließlich eines Vertraulichkeitsgebots (§§ 8 ff. HinSchG) und Schutzmaßnahmen wie das Verbot von Repressalien (§§ 33 ff. HinSchG) geregelt.

Ein Kernelement des HinSchG ist die Verpflichtung zu einem internen Hinweisgebersystem. Beschäftigungsgeber iSv § 3 Abs. 9 HinSchG mit mehr als 50 Beschäftigten müssen eine Meldestelle einrichten und betreiben, § 12 HinSchG. Hierzu können Unternehmen mit 50 bis 249 Beschäftigten eine gemeinsame Stelle einrichten, § 14 Abs. 2 S. 1 HinSchG. Schließlich kann auch ein externer Dritter mit den Aufgaben der internen Meldestelle betraut werden, § 14 Abs. 1 S. 1 HinSchG.

II. Datenschutzrechtliche Implikationen

Die Regelungen des HinSchG sind in mehrfacher Hinsicht datenschutzrechtlich relevant. Zunächst erstreckt sich der Anwendungsbereich dieses Gesetzes gem. § 2 Abs. 1 Nr. 3 lit. p HinSchG auch auf Verstöße gegen die Vorgaben der DS-GVO. Es ist nicht entscheidend, ob es sich um einen Straftatbestand gem. § 42 BDSG oder um einen lediglich bußgeldbewehrten Verstoß gem. Art. 88 Abs. 4, Abs. 5 und Abs. 6 DS-GVO handelt. Weiterhin kommt es nicht auf die bei der Verhängung von Geldbußen umstrittene Frage des Verschuldens[4] an. Es muss sich lediglich um einen Verstoß iSv § 3 Abs. 2 HinSchG handeln, also ein rechtswidriges Handeln oder Unterlassen im Hinblick auf die Vorgaben der DS-GVO. Der Anwendungsbereich des HinSchG umfasst außerdem auch Verstöße gegen andere datenschutzrechtliche Vorgaben wie die des TTDSG, § 2 Abs. 1 Nr. 3 lit. o HinSchG.

Darüber hinaus betreffen die Kernelemente des HinSchG unweigerlich datenschutzrechtliche Aspekte. Beim Betrieb des Hinweisgebersystems werden regelmäßig personenbezogene Daten verarbeitet. Hierzu zählen Informationen einer Meldung wie die Angaben zu Hinweisgebern (sofern sie nicht anonym bleiben), zum Sachverhalt sowie zu beschuldigten und sonst betroffenen Personen wie zB Zeugen, aber auch personenbezogene Daten, die im weiteren Verlauf bei internen Ermittlungen erhoben werden. Nicht zuletzt vor diesem Hintergrund enthält Art. 17 S. 1 RL (EU) 2019/1937 die letztlich nur klarstellende Vorgabe, dass die Verarbeitung personenbezogener Daten zur Umsetzung der Whistleblower-RL in Einklang mit den Vorgaben

1 BGBl. 2023 I Nr. 140; zum Verlauf des Gesetzgebungsverfahrens s. nur BT-Drs. 20/3442, BT-Drs. 20/3709, BT-Drs. 20/4909, BT-Drs. 20/5991 und 20/5992 sowie BT-Drs. 20/6700.
2 RL (EU) 2019/1937 des Europäischen Parlaments und des Rates v. 23.10.2019 zum Schutz von Personen, die Verstöße gegen das Unionsrecht melden, ABl. v. 26.11.2019, L 305/17.
3 Begründung zum Entwurf eines Gesetzes für einen besseren Schutz hinweisgebender Personen sowie zur Umsetzung der Richtlinie zum Schutz von Personen, die Verstöße gegen das Unionsrecht melden, BT-Drs. 20/3442, 1.
4 Vgl. nur Wybitul ZD 2023, 187 (187 f.); Taeger/Gabel, DSGVO – BDSG – TTDSG/Moos/Schefzig, 4. Aufl. 2022, DSGVO Art. 83 Rn. 149 ff. und GA M. Campos Sánchez-Bordona SA v. 27.4.2023 – C-807/21 – Deutsche Wohnen SE.

der DS-GVO und der RL (EU) 2016/680[5] sowie der VO (EU) 2018/1725[6] erfolgen muss. Damit sind auch die ergänzenden Regelungen des BDSG und für den öffentlichen Bereich darüber hinaus die jeweiligen Landesdatenschutzgesetze sowie die bereichsspezifischen Datenschutzvorschriften zu beachten.

Die datenschutzrechtsrelevanten Aspekte betreffen insbesondere die Gestaltung und den Betrieb des Hinweisgebersystems. Eine Verarbeitung personenbezogener Daten bedarf auch in diesem Rahmen eines datenschutzrechtlichen Erlaubnistatbestands. Darüber hinaus sind die Fragen zu beantworten, ob eine Datenschutz-Folgenabschätzung durchzuführen ist und welche technischen und organisatorischen Maßnahmen (TOMs) ergriffen werden müssen. Weiterhin ist die Entscheidung zu treffen, ob betriebliche und behördliche Datenschutzbeauftragte als interne Meldestelle gem. § 12 Abs. 1 S. 1 HinSchG fungieren sollen bzw. dürfen. Schließlich besteht ein Spannungsverhältnis zwischen Hinweisgeberschutz und Datenschutz, das vom Gesetzgeber auch mit spezifischen Vorschriften wie §§ 8 und 9 HinSchG zur Vertraulichkeit grundsätzlich berücksichtigt wurde.[7]

III. Datenschutzrechtliche Grundlagen und Grenzen der Verarbeitung

1. Erlaubnistatbestand und Erforderlichkeit

Eine Verarbeitung personenbezogener Daten zum Betreiben eines Hinweisgebersystems nach den Vorgaben des HinSchG kann auf Art. 6 Abs. 1 S. 1 lit. c und Abs. 3 S. 1 DS-GVO iVm § 10 HinSchG gestützt werden, da eine rechtliche Pflicht erfüllt wird. Die Grenze wird durch das HinSchG gezogen, dem die gesetzlichen Pflichten im Einzelnen zu entnehmen sind.

Eine Verarbeitung durch interne und externe Meldestellen ist gem. § 10 HinSchG zulässig, soweit es zur Erfüllung ihrer Aufgaben gem. §§ 13 und 24 HinSchG erforderlich ist, also zum Betreiben der Meldekanäle, Durchführen der Verfahren und Ergreifen von Folgemaßnahmen. Die Erfüllung dieser – für interne Meldestellen in §§ 16–18 HinSchG und für externe Meldestellen in §§ 27–29 HinSchG konkretisierten – Aufgaben bildet den Maßstab für die Erforderlichkeit der Verarbeitung.

Erforderlichkeit ist zu bejahen, wenn die Verarbeitung für die Aufgabenerledigung geeignet ist und kein anderes, gleich wirksames, aber das Recht auf informationelle Selbstbestimmung weniger einschränkendes Mittel zur Verfügung steht. Die konkrete Verarbeitung muss dergestalt „conditio sine qua non" sein, dass die Aufgaben ohne die Verarbeitung nicht, nicht vollständig, nicht in der notwendigen Zeit oder nicht in rechtmäßiger Weise erfüllt werden können.[8] Das Tatbestandsmerkmal der Erforderlichkeit ist als unbestimmter Rechtsbegriff im Einzelfall auszulegen.

Es bestehen große Überschneidungen mit dem Gebot der Datenminimierung gem. Art. 5 Abs. 1 lit. c DS-GVO, das auch für Verarbeitungen iRd HinSchG zum Tragen kommt. Das Gebot der Datenminimierung verlangt Datensparsamkeit und Datenvermeidung. Es bezieht sich insbesondere auf die zu verarbeitenden Daten in quantitativer und qualitativer Hinsicht, die betroffenen Personen, die zeitliche Komponente und die Art und Häufigkeit der Verarbeitung.[9] Dem Grundsatz der Datenminimierung ist durch eine entsprechende Gestaltung des Hinweisgebersystems und der Verfahren Rechnung zu tragen, um die Erhebung und Verwendung personenbezogener Daten begrenzen zu können.

2. Besondere Kategorien personenbezogener Daten

Die Befugnis zur Verarbeitung besonderer Kategorien personenbezogener Daten folgt aus Art. 9 Abs. 2 lit. g DS-GVO iVm § 10 S. 2, S. 3 HinSchG.[10] Der Erlaubnistatbestand knüpft ebenfalls an die Erforderlichkeit der Verarbeitung an. Darüber hinaus müssen von der Meldestelle spezifische und angemessene Maßnahmen zur Wahrung der Interessen der betroffenen Person vorgesehen werden, § 10 S. 3 HinSchG; s. dazu unter VII.2.

3. Offenlegung von Daten und Vertraulichkeitsgebot

Sollen personenbezogene Daten offengelegt werden, wird eine Grenze für diese Verarbeitung nicht nur durch die Erforderlichkeit, sondern auch durch das Vertraulichkeitsgebot nach dem HinSchG gezogen. Das in §§ 8 und 9 HinSchG geregelte Vertraulichkeitsgebot ist ein wesentlicher Pfeiler des Hinweisgeberschutzes. Es umfasst die hinweisgebenden Personen, Personen, die Gegenstand der Meldung sind, und sonstige in der Meldung genannte Personen, zB beteiligte oder unbeteiligte Dritte wie Kollegen oder Vorgesetze. Bei den Ausnahmen vom Vertraulichkeitsgebot nach § 9 HinSchG wird nach den betroffenen Personen unterschieden. Beispielsweise dürfen Informationen zu Hinweisgebern im Gegensatz zu Informationen über die Identität von Personen, die Gegenstand einer Meldung sind, und von sonstigen in der Meldung genannten Personen für Folgemaßnahmen nur weitergegeben werden, wenn die hinweisgebende Person zuvor eingewilligt hat, § 9 Abs. 3, Abs. 4 Nr. 3 HinSchG. Hierbei sind die Vorgaben gem. § 26 Abs. 2 BDSG zu beachten, wo die Einwilligung im Beschäftigungsverhältnis geregelt ist. Der entsprechende Hinweis in § 9 Abs. 3 S. 3 HinSchG ist lediglich deklaratorischer Art[11] und damit entbehrlich, da die datenschutzrechtlichen Vorschriften grundsätzlich gelten und zu beachten sind.

Für die Meldestelle tätige Personen und ggf. unterstützendes Personal sollen nach der Intention des Gesetzgebers auf Vertraulichkeit verpflichtet und diesbezüglich geschult werden, soweit es erforderlich ist.[12] Eine entsprechende gesetzliche Regelung gibt es mit §§ 15 Abs. 2, 25 Abs. 2 S. 1 HinSchG zwar lediglich für die Schulung. Allerdings kann die Notwendigkeit einer spezifischen Verpflichtungserklärung sowohl zur Vertraulichkeit als auch zum spezifischen Datenschutz aus der Pflicht zu angemessenen TOMs zum Schutz personenbezogener Daten abgeleitet werden (s. dazu unter VII.).

---

5 RL (EU) 2016/680 des Europäischen Parlaments und des Rates v. 27.4.2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates (ABl. L 119 v. 4.5.2016, 89) mit den Berichtigungen, ABl. L 127 v. 23.5.2018, 9 und ABl. L 074 v. 4.3.2021, 36.

6 VO (EU) 2018/1725 des Europäischen Parlaments und des Rates v. 23.10.2018 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe, Einrichtungen und sonstigen Stellen der Union, zum freien Datenverkehr und zur Aufhebung der VO (EG) Nr. 45/2001 und des Beschlusses Nr. 1247/2002/EG, ABl. L 295 v. 21.11.2018, 39.

7 Begründung zum Entwurf eines Gesetzes für einen besseren Schutz hinweisgebender Personen sowie zur Umsetzung der Richtlinie zum Schutz von Personen, die Verstöße gegen das Unionsrecht melden, BT-Drs. 20/3442, 35 (Abschn. V) und 73 f.

8 Vgl. Taeger/Gabel, DSGVO – BDSG – TTDSG/Lang, 4. Aufl. 2022, BDSG § 3 Rn. 30.

9 So auch Ehmann/Selmayr, DS-GVO/Heberlein, 2018, DS-GVO Art. 5 Rn. 22; Gola/Heckmann, DS-GVO – BDSG/Pötters, 3. Aufl. 2022, DS-GVO Art. 5 Rn. 22 f.

10 Vgl. auch Beschlussempfehlung und Bericht des Rechtsausschusses, BT-Drs. 20/4909, 54.

11 Insofern zutreffend Begründung zum Entwurf eines Gesetzes für einen besseren Schutz hinweisgebender Personen sowie zur Umsetzung der Richtlinie zum Schutz von Personen, die Verstöße gegen das Unionsrecht melden, BT-Drs. 20/3442, 76.

12 Begründung zum Entwurf eines Gesetzes für einen besseren Schutz hinweisgebender Personen sowie zur Umsetzung der Richtlinie zum Schutz von Personen, die Verstöße gegen das Unionsrecht melden, BT-Drs. 20/3442, 74 (§ 8).

IV. Dokumentationspflicht und Löschen von Daten

Das HinSchG sieht eine Dokumentationspflicht vor. Alle eingehenden Meldungen sind in dauerhaft abrufbarer Weise unter Beachtung des Vertraulichkeitsgebots zu dokumentieren, § 11 HinSchG. Für telefonische oder persönlich vorgetragene Meldungen vor Ort sind besondere Vorgaben wie das Einwilligungserfordernis für eine Tonaufzeichnung und ein Wortlautprotokoll zu beachten, § 11 Abs. 2–4 HinSchG.

Die Dokumentation ist gem. § 11 Abs. 5 S. 1 HinSchG grundsätzlich drei Jahre nach Abschluss des Verfahrens zu löschen.[13] Das bedeutet, dass auch die iRe Meldung verarbeiteten personenbezogenen Daten grundsätzlich nach Ablauf dieser Frist zu löschen sind, da es sich hier um eine gesetzliche Aufbewahrungspflicht handelt, vgl. Art. 17 Abs. 3 lit. b DS-GVO.

Die Dokumentation darf im Einzelfall länger aufbewahrt werden, um die Anforderungen nach HinSchG oder anderen Rechtsvorschriften zu erfüllen, solange dies erforderlich und verhältnismäßig ist, § 11 Abs. 5 S. 2 HinSchG. Das kann nach Ansicht des Gesetzgebers zB der Fall sein, wenn ein weiterer Hinweis zu einem Sachverhalt erfolgt, zu dem ein Verfahren bereits abgeschlossen wurde.[14] Hier wird im Einzelfall zu prüfen sein, ob es sich tatsächlich um denselben Sachverhalt handelt und die Meldungen untrennbar verknüpft sind. Die maßgeblichen Kriterien der Erforderlichkeit und Verhältnismäßigkeit finden auch im Datenschutzrecht Anwendung. Der Ausnahmetatbestand ist jedenfalls nicht auf Fälle zur „Klärung erforderlicher weiterer rechtlicher Schritte wie Disziplinarverfahren und Einleitung von Strafverfahren" beschränkt, wie es die deutschen Datenschutzaufsichtsbehörden jedenfalls vor der RL (EU) 2019/1937 und dem HinSchG für eine über die Regelspeicherdauer hinausgehende Aufbewahrung von personenbezogenen Daten in Hinweisgebersystemen vertreten haben.[15]

V. Datenschutz-Folgenabschätzung

Vor dem Betrieb eines Hinweisgebersystems nach HinSchG ist nach wohl überwiegender Ansicht eine Datenschutz-Folgenabschätzung gem. Art. 35 DS-GVO durchzuführen.[16] Es ist vertretbar, von einem hohen Risiko für die Rechte und Freiheiten natürlicher Personen auszugehen, insbesondere weil Daten über potenziell strafrechtlich relevantes Verhalten verarbeitet werden können, die Vertraulichkeit in Bezug auf Hinweisgeber bzw. deren Anonymität auf Grund der Ausnahmetatbestände in § 9 HinSchG nicht in jedem Fall durchgängig gewahrt werden kann und bei einer Einbindung von Externen als Meldestelle oder der Einrichtung einer gemeinsamen Meldestelle sich das Risiko bei der Verarbeitung erhöht. Daher ist davon auszugehen, dass auch die Datenschutzaufsichtsbehörden die Verarbeitung auf Grund ihrer Art, ihres Umfangs, ihrer Umstände und ihrer Zwecke so bewerten, dass sie voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat. Bereits vor Inkrafttreten der RL (EU) 2019/1937 verlangten die deutschen Aufsichtsbehörden allgemein für „Verfahren zur Meldung von Missständen", dass eine Datenschutz-Folgenabschätzung durchgeführt werden muss.[17] Datenschutzaufsichtsbehörden in anderen EU-Ländern wie zB Italien haben sich bereits entsprechend positioniert und in mehreren Fällen u.a. auch wegen einer fehlenden Datenschutz-Folgenabschätzung für ein Hinweisgebersystem gemäß der RL (EU) 2019/1937 Bußgelder verhängt.[18]

Etwas anders sieht es zB in Österreich aus, wo der Bundesgesetzgesetzgeber zwar ebenfalls von der Notwendigkeit einer Datenschutz-Folgenabschätzung ausgeht.[19] Dabei vermögen die Annahme, dass das Regelbeispiel gem. Art. 35 Abs. 3 lit. b DS-GVO vorliegt, und die Begründung, „weil es potentiell auch zu einer (geographisch) umfangreichen Verarbeitung von personenbezogenen Daten kommen kann und diese auch die genannten Personen betreffen können, die besonders schutzwürdig sind", nicht zu überzeugen. Der Gesetzgesetzgeber hat allerdings von der Möglichkeit Gebrauch gemacht, eine Datenschutz-Folgenabschätzung iRd Gesetzgebungsverfahrens für das österreichische Hinweisgeberschutzgesetz (öHSchG)[20] auf abstrakter Ebene durchzuführen, § 8 Abs. 13 öHSchG.[21] Bei einer solchen – vorgezogenen – Datenschutz-Folgenabschätzung übernimmt der Gesetzgeber die Verantwortung für deren Durchführung. Die Regelungen in Art. 35 Abs. 1–7 DS-GVO finden gem. Art. 35 Abs. 10 DS-GVO keine Anwendung und Verantwortliche sind von der grundsätzlichen Pflicht zur Durchführung einer Datenschutz-Folgenabschätzung befreit.[22] Etwas anderes gilt lediglich, wenn der Gesetzgeber die Durchführung einer konkreten Datenschutz-Folgenabätzung explizit vorgesehen hat,[23] was gem. § 8 öHSchG nicht der Fall ist.

VI. Gemeinsame Verantwortlichkeit und Auftragsverarbeitung

Bei einer gemeinsamen Meldestelle zB in Konzernen oder Unternehmensgruppen und bei der Einschaltung Externer als interne Meldestelle, aber auch bei der Inanspruchnahme von Dienstleistern für die Bereitstellung und den Betrieb einer Anwendung für einen Online-Meldekanal (Software as a Service) sind datenschutzrechtliche Vereinbarungen zu schließen. Das können – je nach Konstellation – insbesondere Vereinbarungen über eine gemeinsame Verantwortlichkeit nach Art. 26 Abs. 1 S. 2 DS-GVO oder eine Auftragsverarbeitung gem. Art. 28 Abs. 2 DS-GVO sein. Im Fall einer gemeinsamen Verantwortlichkeit ist das Wesentliche der Vereinbarung der betroffenen Person zur Verfügung zu stellen, Art. 26 Abs. 2 S. 2 DS-GVO.[24]

---

13 Krit. zur Vereinbarkeit dieser Regelung mit Art. 18 Abs. 1 S. 2 RL (EU) 2019/1937 BeckOK Arbeitsrecht/Bruns, 68. Ed. 2.7.2023, HinSchG § 11 Rn. 9 f.; Thüsing/Musiol/Peisker ZGI 2023, 63 (64 f.).

14 Begründung zum Entwurf eines Gesetzes für einen besseren Schutz hinweisgebender Personen sowie zur Umsetzung der Richtlinie zum Schutz von Personen, die Verstöße gegen das Unionsrecht melden, BT-Drs. 20/3442, 77.

15 DSK, Orientierungshilfe zu Whistleblowing-Hotlines, 2018, abrufbar unter: https://www.datenschutzkonferenz-online.de/media/oh/20181114_oh_whistleblowing_hotlines.pdf, Abschn. E 6.

16 Vgl. nur Bayreuther NZA-Beil. 2022, 20 (22); Fehr ZD 2022, 256 (259).

17 DSK, Orientierungshilfe zu Whistleblowing-Hotlines, 2018, Abschn. E 9; unter Bezugnahme darauf nunmehr auch LfDI B-W, FAQ Hinweisgeberschutzgesetz, Frage 16, abrufbar unter: https://www.baden-wuerttemberg.datenschutz.de/faq-hinweisgeberschutzgesetz/.

18 Garante per la protezione dei dati personali (italienische Datenschutzaufsichtsbehörde), Registro dei provvedimenti n. 134 del 7 aprile 2022 (doc. web n. 9768363); Registro dei provvedimenti n. 235 del 10 giugno 2021 (doc. web n. 9685922).

19 Datenschutz-Folgenabschätzung zum Bundesgesetz über das Verfahren und den Schutz bei Hinweisen auf Rechtsverletzungen in bestimmten Rechtsgebieten (Hinweisgeberschutzgesetz – öHSchG), S. 1, abrufbar unter: https://www.ris.bka.gv.at/Dokumente/Begut/BEGUT_31042F40_74E2_4CBF_8E24_899D1A8EF37C/Materialien_0003_4AC23FCB_626B_4A0E_921A_559F160A09D4.pdf.

20 Bundesgesetz über das Verfahren und den Schutz bei Hinweisen auf Rechtsverletzungen in bestimmten Rechtsbereichen (HinweisgeberInnenschutzgesetz – öHSchG), zB öBGBl. I Nr. 6/2023 v. 24.2.2023.

21 Datenschutz-Folgenabschätzung zum Bundesgesetz über das Verfahren und den Schutz bei Hinweisen auf Rechtsverletzungen in bestimmten Rechtsgebieten (Hinweisgeberschutzgesetz – öHSchG), S. 1, abrufbar unter: https://www.ris.bka.gv.at/Dokumente/Begut/BEGUT_31042F40_74E2_4CBF_8E24_899D1A8EF37C/Materialien_0003_4AC23FCB_626B_4A0E_921A_559F160A09D4.pdf.

22 Zur Datenschutz-Folgenabschätzung im Zuge der Gesetzgebung Roßnagel/Geminn/Johannes ZD 2019, 435.

23 Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht/Karg, 2019, DSGVO Art. 35 Rn. 56; Roßnagel/Geminn/Johannes ZD 2019, 435 (436); unentschieden Sydow/Marsch, DS-GVO BDSG/Schwendemann, 3. Aufl. 2022, DS-GVO Art. 35 Rn. 20.

24 Dazu Taeger/Gabel, DSGVO – BDSG – TTDSG/Lang, 4. Aufl. 2022, DSGVO Art. 26 Rn. 95 ff.

VII. Technische und organisatorische Maßnahmen

1. Allgemeine Vorgaben

Für die Verarbeitung personenbezogener Daten in einem Hinweisgebersystem gelten hinsichtlich der TOMs die allgemeinen Vorschriften und Vorgaben gem. Art. 24, 25 und 32 DS-GVO. Da die Daten rechtswidriges und auch strafbares Verhalten einerseits und die Identität u.a. hinweisgebender Personen sowie möglicher Täter andererseits umfassen können, sollte der Fokus insbesondere auf den Zugriffsrechten und dem korrespondierenden Berechtigungskonzept, der Protokollierung, der Möglichkeit eines Einsatzes von Verschlüsselungsverfahren und dem Prozess für die Löschung der Daten liegen.

2. Spezifische und angemessene Maßnahmen für besondere Kategorien personenbezogener Daten

Werden besondere Kategorien personenbezogener Daten verarbeitet, sind von der Meldestelle gem. § 10 S. 3 HinSchG spezifische und angemessene Maßnahmen zur Wahrung der Interessen der betroffenen Person zu ergreifen. Mit dieser Regelung setzt der Gesetzgeber die Vorgaben von Art. 9 Abs. 2 lit. g DS-GVO um, wonach die gesetzliche Ausnahmeregelung für eine Verarbeitung besonderer Kategorien personenbezogener Daten entsprechende Maßnahmen vorzusehen hat.

Die Maßnahmen für eine Verarbeitung besonderer Kategorien personenbezogener Daten müssen „spezifisch" sein, also konkret festgelegt werden und die besonderen Umstände der Verarbeitung im Einzelfall widerspiegeln.[25] Die Maßnahmen müssen auch verhältnismäßig sein. Sie sind im Wege einer einzelfallbezogenen Abwägung zu ermitteln und zu treffen. Dabei sind zum einen der Stand der Technik und die Implementierungskosten und zum anderen Art, Umfang, Umstände und Zwecke der Verarbeitung sowie die Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen zu berücksichtigen, § 10 S. 3 HinSchG iVm § 22 Abs. 2 S. 2 BDSG. Die in § 22 Abs. 2 S. 2 BDSG aufgelisteten Regelbeispiele[26] wie zB Pseudonymisierung sind als mehr oder weniger konkretisierte Themenfelder nur begrenzt hilfreich. Dennoch müssen Vorkehrungen getroffen werden, die bei wertender Betrachtung diesen Kriterien entsprechen.[27] Die wesentlichen Aspekte und Gründe der Abwägungs- und Auswahlentscheidung sollten nicht zuletzt wegen der Rechenschaftspflicht gem. Art. 5 Abs. 2 DS-GVO dokumentiert werden.

VIII. Datenschutzrechte der betroffenen Personen

Die datenschutzrechtlichen Informations- und Auskunftsrechte sowie die korrespondierenden Plichten der Verantwortlichen gem. Art. 13, 14 und 15 DS-GVO werden durch das in § 8 HinSchG geregelte Vertraulichkeitsgebot begrenzt. Diese Einschränkung der Offenlegung ist eine zulässige Ausnahme, soweit Informationen offenbart würden, die ihrem Wesen nach oder nach einer Rechtsvorschrift geheim gehalten werden müssen. Sie ist datenschutzgesetzlich verankert in Art. 14 Abs. 5 lit. c DS-GVO und Art. 23 Abs. 1 lit. i DS-GVO iVm § 29 Abs. 1 S. 1, S. 2 BDSG.

Bei der Erfüllung der datenschutzrechtlichen Informations- und Auskunftspflichten sowie der Gestaltung der entsprechenden Prozesse müssen sowohl das Vertraulichkeitsgebot als auch dessen Ausnahmen gem. § 9 HinSchG beachtet werden. Andernfalls besteht die Gefahr, die datenschutzrechtlichen Pflichten zu verletzen, weil das Vertraulichkeitsgebot nach HinSchG im konkreten Einzelfall gar nicht greift. Von der Informationspflicht und dem Auskunftsrecht wird zB regelmäßig auch der Hinweisgeber als Quelle der personenbezogenen Daten der betroffenen Person umfasst sein, Art. 14 Abs. 2 lit. f, 15 Abs. 1 lit. g DS-GVO. Hinweisgeber werden nach § 8 Abs. 1 HinSchG zwar vor einer Offenlegung geschützt. Das gilt gem. § 9 Abs. 1 HinSchG jedoch nicht bei vorsätzlich oder grob fahrlässig unrichtigen Informationen über Verstöße. Die Berücksichtigung und Anwendung der einschlägigen Vorschriften können im Einzelfall eine herausfordernde Aufgabe sein. Das zeigt auch die Diskussion darüber, ob der datenschutzrechtliche Auskunftsanspruch mangels expliziter Ausnahmeregelung im HinSchG den Hinweisgeberschutz zu unterlaufen droht.[28] Hierzu ist anzumerken, dass insbesondere beim Verweis auf die Rechtsprechung des LAG Baden-Württemberg[29] und des BGH[30] zu wenig berücksichtigt wird, dass mit § 8 HinSchG eine gesetzliche Regelung vorliegt und damit die erste Alternative von § 29 Abs. 1 S. 2 BDSG zum Tragen kommt.[31] Das ändert freilich nichts daran, dass die Ausnahmetatbestände gem. § 9 HinSchG schwierige Folgefragen der Darlegungs- und Beweislast im Gerichtsverfahren aufwerfen.[32] Jedenfalls sollte nicht zuletzt mit Blick auf die Rechenschaftspflicht gem. Art. 5 Abs. 2 DS-GVO bei jeder Information bzw. Nicht-Information von betroffenen Personen und bei jeder Bearbeitung eines Auskunftsanspruchs konkret dokumentiert werden, welche Informationen wie zB die Identität des Hinweisgebers als Quelle der personenbezogenen Daten aus welchen Gründen (nicht) offengelegt wurden.

IX. Datenschutzbeauftragte als interne Meldestelle

Die mit den Aufgaben einer internen Meldestelle betrauten Personen sollen nicht nur über die notwendige Fachkunde verfügen, § 15 Abs. 2 HinSchG. Sie müssen zudem bei der Ausübung ihrer Tätigkeit unabhängig sein. Etwaige weitere Aufgaben dürfen zu keinem Interessenkonflikt führen, § 15 Abs. 1 HinSchG. Unter diesen Voraussetzungen sind auch Doppelfunktionen zulässig, was nach Auffassung des Gesetzgebers zumindest in kleineren Unternehmen auch für Datenschutzbeauftragte der Fall sein soll. In der Gesetzesbegründung wird auf Erwägungsgrund 56 RL (EU) 2019/1937 verwiesen,[33] wo neben Datenschutzbeauftragten auch die Leitung der Bereiche Compliance und Personal sowie der Finanzvorstand genannt werden. Diese Ansicht wurde bislang nur vereinzelt kritisch betrachtet.[34] Dabei ist es fraglich, wie die Position des bundesdeutschen und europäischen Gesetzgebers mit der Vermeidung von Interessenkonflikten bei Datenschutzbeauftragten zusammenpasst.

Nach Art. 38 Abs. 6 DS-GVO ist es grundsätzlich möglich, dass Datenschutzbeauftragte auch andere Aufgaben übernehmen können (Satz 1). Es muss jedoch zwingend sichergestellt werden, dass es nicht zu Interessenkonflikten kommt (Satz 2). Die

25 Vgl. zu der insoweit entsprechenden Regelung in § 22 Abs 2 S. 1 BDSG Piltz, BDSG, 2018, BDSG § 22 Rn. 29; Gola/Heckmann, DS-GVO – BDSG/Heckmann/Scheurer, 3. Aufl. 2022, BDSG § 22 Rn. 57.

26 Piltz, BDSG, 2018, BDSG § 22 Rn. 31; Gola/Heckmann, DS-GVO – BDSG/Heckmann/Scheurer, 3. Aufl. 2022, BDSG § 22 Rn. 59.

27 Vgl. BAG NZA 2019, 1055 Rn. 52 = ZD 2020, 46 (gekürzt) mAnm Tiedemann; Taeger/Gabel, DSGVO – BDSG – TTDSG/Rose, 4. Aufl. 2022, BDSG § 22 Rn. 60.

28 So Dzida/Seibt NZA 2023, 657 (665); vgl. auch Lühning ZD 2023, 136 (137) (140).

29 LAG Baden-Württemberg NZA-RR 2019, 242 Rn. 177 ff. = ZD 2019, 276 (gekürzt) mAnm Wybitul.

30 BGH ZD 2022, 326 Rn. 15 ff.

31 Vgl. bei Dzida/Seibt NZA 2023, 657 (665); wohl auch Lühning ZD 2023, 136 (137) (140); dagegen zutreffend Mohn NZA 2022, 1159 (1166 f.).

32 Mohn NZA 2022, 1159 (1166 f.).

33 Begründung zum Entwurf eines Gesetzes für einen besseren Schutz hinweisgebender Personen sowie zur Umsetzung der Richtlinie zum Schutz von Personen, die Verstöße gegen das Unionsrecht melden, BT-Drs. 20/3442, 78, 80.

34 ZB Leibold ZD-Aktuell 2022, 01333, Abschn. 6; s.a. Fehr ZD 2022, 256, die ohne weitergehende Begr. unter Verweis auf Stuke/Fehr BB 2021, 2740 hiervon abrät.

Frage, ob ein Interessenkonflikt vorliegt, muss nach der Rechtsprechung des EuGH im Einzelfall unter Würdigung aller relevanten Umstände, insbesondere der Organisationsstruktur des Verantwortlichen bzw. Auftragsverarbeiters, und im Licht aller anwendbaren Rechtsvorschriften sowie etwaiger interner Vorschriften beantwortet werden.[35] Dabei ist zu beachten, dass Art. 38 Abs. 6 DS-GVO die funktionelle Unabhängigkeit von Datenschutzbeauftragten wahren und damit die Wirksamkeit der Bestimmungen der DS-GVO gewährleisten soll.[36]

Vor diesem Hintergrund und unter Berücksichtigung der einem Datenschutzbeauftragten nach Art. 39 Abs. 1 lit. b DS-GVO obliegenden Aufgaben wie der Überwachung der Einhaltung der Datenschutzvorschriften etc. dürfen Datenschutzbeauftragten keine Aufgaben oder Pflichten übertragen werden, die sie dazu veranlassen würden, die Zwecke und Mittel der Verarbeitung personenbezogener Daten bei dem Verantwortlichen oder Auftragsverarbeiter festzulegen. Das stünde im Widerspruch zur gesetzlichen Vorgabe, dass Datenschutzbeauftragte die Überwachung dieser Zwecke und Mittel unabhängig durchführen müssen.[37] Ein Interessenkonflikt iSv Art. 38 Abs. 6 S. 2 DS-GVO ist daher vor allem dann anzunehmen, wenn Datenschutzbeauftragte sich im Rahmen ihrer anderen Tätigkeit selbst kontrollieren müssten. Das wird insbesondere der Fall sein, wenn der weitere Aufgabenbereich eine interne Verantwortung für die Datenschutzkonformität von Verarbeitungen mit sich bringt. Es ist im Einzelfall zu prüfen, ob insofern eigene Entscheidungskompetenzen im Hinblick auf Mittel und Zwecke der Datenverarbeitung bestehen.[38]

Für interne Meldestellen nach HinSchG ist zu festzustellen, dass deren Aufgaben und Kompetenzen einen besonderen Bezug zu datenschutzrechtlichen Fragestellungen aufweisen. Interne Meldestellen müssen die Meldekanäle gem. § 16 HinSchG betreiben und die Verfahren nach § 17 HinSchG durchführen. Das umfasst u.a. die Anfrage weiterer Informationen und die Rückmeldung an Hinweisgeber. Weiterhin muss eine interne Meldestelle auch Folgemaßnahmen iSd § 3 Abs. 7 HinSchG ergreifen. Hierzu zählen nach § 18 HinSchG insbesondere interne Untersuchungen, Kontaktaufnahmen zu Betroffenen und betroffenen Organisationseinheiten sowie der Abschluss und die Abgabe von Verfahren für weitere Untersuchungen an interne Organisationseinheiten oder Behörden. Dabei verarbeitet die interne Meldestelle eine Vielzahl personenbezogener Daten, die auch potenziell strafbares Verhalten umfassen können. Weiterhin hat sie für die Dokumentation von Meldungen in Form von Tonaufzeichnungen gem. § 11 Abs. 1, Abs. 3 HinSchG eine Einwilligung einzuholen. Nicht zuletzt muss die interne Meldestelle bei einer Verarbeitung besonderer Kategorien personenbezogener Daten spezifische und angemessene Maßnahmen zur Wahrung der Interessen der betroffenen Person treffen. Diese Aufgabe wird in § 10 S. 3 HinSchG explizit der internen Meldestelle zugewiesen. Ungeachtet der mit diesen Aufgaben und Kompetenzen einhergehenden internen Verantwortung für die Datenschutzkonformität unterliegt eine interne Meldestelle bzw. deren Verarbeitung personenbezogener Daten der Kontrolle durch den Datenschutzbeauftragten. Daher sprechen die gesetzlichen Aufgaben einer internen Meldestelle gem. §§ 16–18 HinSchG und deren datenschutzrechtliche Implikationen für die Gefahr einer Interessenkollision.

Nach der Rechtsprechung des EuGH ist ein strenger Prüfungsmaßstab angezeigt.[39] Bei der Frage eines Interessenkonflikts ist darauf zu fokussieren, dass Art. 38 Abs. 6 DS-GVO die funktionelle Unabhängigkeit von Datenschutzbeauftragten wahren und damit die Wirksamkeit der Bestimmungen der DS-GVO gewährleisten soll.[40] Es müssen zwar nicht nur die gesetzlichen Vorgaben, sondern auch interne Regelungen und die Organisationsstruktur des Verantwortlichen bzw. Auftragsverarbeiters berücksichtigt werden.[41] Nur so lässt sich feststellen, ob Datenschutzbeauftragten zusätzliche Aufgaben und Funktionen übertragen werden, die eine interne Festlegung der Zwecke und Mittel der Verarbeitung personenbezogener Daten mit sich bringen, wie es der Europäische Datenschutzausschuss (EDSA) gerade auch für hierarchisch nachgeordnete Positionen bereits dargelegt hat.[42]

Dieser umfassende Ansatz setzt nicht nur Grenzen, sondern eröffnet zugleich Handlungsoptionen, die internen Regelungen und Organisationsstruktur so zu gestalten, dass kein Interessenkonflikt entsteht. Im Hinblick auf die interne Meldestelle nach HinSchG ist jedoch zu beachten, dass deren Aufgaben und Kompetenzen gesetzlich im Detail geregelt sind und insoweit keine oder nur sehr begrenzte Gestaltungsmöglichkeiten bestehen, um der Gefahr bereits vorgezeichneter Interessenkonflikte zu begegnen. Das gilt – zumindest soweit es um die vom Gesetzgeber in den Blick genommenen kleineren Unternehmen geht – insbesondere für die Empfehlung, die Aufgaben und Rollen strikt zu trennen sowie entsprechende Rahmenbedingungen zu schaffen.[43] Gerade kleinere Unternehmen verfügen in der Praxis häufig nicht über die personelle Stärke und Flexibilität, die für ein solches Vorgehen notwendig sind, um möglichen Interessenkonflikten vorbeugen zu können. Vielmehr wird bzw. soll regelmäßig lediglich eine Person die Aufgaben des Datenschutzbeauftragten und der internen Stelle wahrnehmen, ohne auf Stellvertreter oder weitere Mitarbeiter zurückgreifen zu können.

X. Fazit

Das HinSchG ist in hohem Maße datenschutzrelevant. Das gilt nicht zuletzt wegen des Spannungsfelds von Hinweisgeber- und Datenschutz, das u.a. beim Vertraulichkeitsgebot gem. § 8 HinSchG und dem Grundsatz der Transparenz gem. Art. 5 Abs. 1 lit. a DS-GVO mit den Ausprägungen in Form von Informationspflicht (Art. 13 und 14 DS-GVO) und Auskunftsrecht (Art. 15 DS-GVO) deutlich wird. Es gibt eine Vielzahl datenschutzrechtlicher Implikationen, die in der Praxis zu beachten sind. Sie betreffen vor allem die Gestaltung und den Betrieb des Hinweisgebersystems, den Schutz von Hinweisgebern, möglichen Tätern sowie Dritten, die Offenlegung von Verstößen und die Dokumentation.

Neben der datenschutzrechtlichen Einordnung und Bewertung dieser Vorgaben ist auch deren datenschutzrechtskonforme Umsetzung in der Praxis eine Herausforderung. Hierzu müssen die entsprechenden Prozesse sowie datenschutzrechtskonforme Strukturen geschaffen und in das Datenschutzmanagement integriert werden. Darüber hinaus sind weitere Anpassungen beim Datenschutzmanagement erforderlich. Es muss zB das Verzeichnis der Verarbeitungstätigkeiten gem. Art. 30 DS-GVO ergänzt werden. Das umfasst sowohl die Verarbeitungen beim

35 EuGH ZD 2023, 234 Rn. 45 f.; dazu Lang NZA 2023, 269.
36 EuGH ZD 2023, 234 Rn. 41 f.; dazu Lang NZA 2023, 269.
37 EuGH ZD 2023, 234 Rn. 42 ff.; dazu Lang NZA 2023, 269.
38 EDSA, Endorsement 1/2018 v. 25.5.2018, S. 1 iVm Art. 29-Datenschutzgruppe, Leitlinien in Bezug auf Datenschutzbeauftragte („DSB") v. 5.4.2017, Dok. 16/DE, WP 243 rev.01, Abschn. 3.5; BfDI (Hrsg.), Die Datenschutzbeauftragten in Behörden und Betrieben, Stand 2020, Abschn. 1.4; Kühling/Buchner, DS-GVO/BDSG/Bergt, 3. Aufl. 2020, DS-GVO Art. 38 Rn. 39 f.; Taeger/Gabel, DSGVO – BDSG – TTDSG/Scheja, 4. Aufl. 2022, DSGVO Art. 38 Rn. 75.
39 Lang NZA 2023, 269 (274).
40 EuGH ZD 2023, 234 Rn. 42, 46.
41 EuGH ZD 2023, 234 Rn. 44 f.
42 EDSA, Endorsement 1/2018 v. 25.5.2018, S. 1 iVm Art. 29-Datenschutzgruppe, Leitlinien in Bezug auf Datenschutzbeauftragte („DSB") v. 5.4.2017, Dok. 16/DE, WP 243 rev.01, Abschn. 3.5.
43 BvD e.V., Stellungnahme zum „Entwurf eines Gesetzes für einen besseren Schutz hinweisgebender Personen sowie zur Umsetzung der Richtlinie zum Schutz von Personen, die Verstöße gegen das Unionsrecht melden" (HinSchG-E) v. 4.5.2022, S. 2 f., abrufbar unter: https://www.bmj.de/SharedDocs/Gesetzgebungsverfahren/DE/Hinweisgeberschutz.html; Hoffmann ZD-Aktuell 2023, 01107.

Betrieb des Hinweisgebersystems als auch die Verarbeitungen iRv Folgemaßnahmen. Dabei sind die spezifischen Besonderheiten des HinSchG zu beachten, zB in Bezug auf die Rechtsgrundlage für Tonaufzeichnungen bei telefonischer oder persönlicher Meldung vor Ort (Einwilligung gem. § 11 Abs. 2–4 HinSchG). Soweit Querbezüge zu bzw. Schnittstellen mit anderen Prozessen bestehen, sind diese Prozesse und deren Dokumentation entsprechend anzupassen, zB die Erteilung einer Auskunft gem. Art. 15 DS-GVO.

Um ein Hinweisgebersystem datenschutzkonform zu gestalten, müssen die datenschutzgesetzlichen Anforderungen systematisch berücksichtigt und umgesetzt werden. Es sollte ein Datenschutzkonzept entwickelt bzw. bestehende Konzepte sollten ergänzt werden, um die datenschutzrechtlichen Risiken zu minimieren. Dabei sind die Vorgaben des HinSchG und der DS-GVO sowie des BDSG gleichermaßen zu berücksichtigen. Eine der Herausforderungen ist die unterschiedliche Regelungstiefe datenschutzrelevanter Aspekte im HinSchG. Während einige Fragen wie die der Erforderlichkeit einer Verarbeitung im Detail nicht beantwortet werden, enthalten andere Regelungen wie zB zum Vertraulichkeitsgebot in §§ 8 und 9 HinSchG konkrete und klare Vorgaben, die im Hinblick auf die datenschutzgesetzlichen Informationspflichten und Auskunftsrechte zu beachten sind. Bei einem bereits vorhandenen Hinweisgebersystem ist der Anpassungsbedarf für das Datenschutzkonzept auf Grund des HinSchG unter Berücksichtigung der datenschutzrechtlichen Implikationen zu prüfen. Die insoweit notwendigen Änderungen werden regelmäßig u.a. die datenschutzrechtlichen Erlaubnistatbestände sowie die Informationspflichten und Auskunftsrechte betreffen.

Schließlich ist zu entscheiden, ob betriebliche und behördliche Datenschutzbeauftragte als interne Meldestelle eingesetzt werden. Eine solche Doppelfunktion ist mit Blick auf Art. 38 Abs. 6 S. 2 DS-GVO grundsätzlich und insbesondere dann nicht zu empfehlen, wenn lediglich ein und dieselbe Person diese Aufgaben wahrnehmen soll.

Schnell gelesen ...

- Die Regelungen des HinSchG und das Datenschutzrecht haben nicht nur Berührungspunkte, sondern erhebliche Schnittmengen.
- Datenschutzrechtlich besonders relevant sind das Vertraulichkeitsgebot, die Dokumentationspflicht sowie die Vorgaben in Bezug auf die TOMs.
- Das Vertraulichkeitsgebot nach HinSchG beschränkt die datenschutzrechtlichen Informations- und Auskunftsrechte, was bei der Gestaltung der Prozesse im Detail besonders zu berücksichtigen ist.
- Datenschutzbeauftragte sollten jedenfalls dann nicht als interne Meldestelle eingesetzt werden, wenn die mit beiden Funktionen verbundenen Aufgaben von lediglich ein und derselben Person wahrgenommen werden können.

Dr. Markus Lang
ist selbstständiger Rechtsanwalt in Düsseldorf sowie zertifizierter Datenschutzbeauftragter und Datenschutzauditor.