Konferenz der unabhängigen
Datenschutzbehörden
des Bundes und der Länder

Orientierungshilfe der Datenschutzaufsichtsbehörden zu Whistleblowing-Hotlines:

Firmeninterne Warnsysteme und Beschäftigtendatenschutz

Die Orientierungshilfe zeigt den datenschutzrechtlichen Rahmen und Regelungsmöglichkeiten zu Whistleblowing-Hotlines auf. Sie soll es den Arbeitgebern und den Interessenvertretungen der Beschäftigten erleichtern, im Unternehmen klare Regelungen zum Umgang mit Whistleblowing-Hotlines zu erreichen.

[Anmerkung von Nicholas Vollmer:
Dieses Dokument stammt von November 2018 (das Dokument von Januar 2018 ist somit veraltet). In der Zwischenzeit (Mai 2022) hat Europa eine entsprechende Richtlinie beschlossen und der deutsche Gesetzgeber versucht sich an einem Hinweisgeberschutzgesetz... die Aussagen des hier vorliegenden Dokuments sind also mit Vorsicht zu genießen.]

Stand:
14. November 2018

Inhaltsverzeichnis

A Einführung

Firmeninterne Whistleblowing-Hotlines sind Angebote von Unternehmen an ihre Beschäftigten, ein nicht regelkonformes Verhalten anderer Beschäftigter dem Unternehmen zu melden. Mit der Meldung von Verstößen gegen Verhaltenspflichten geht die Verarbeitung von personenbezogenen Daten einher. Für jegliche automatisierte und nichtautomatisierte Verarbeitung von Beschäftigtendaten sind die Datenschutz-Grundverordnung (DS-GVO)[1] und § 26 Bundesdatenschutzgesetz (BDSG)[2] in Verbindung mit Art. 88 DS-GVO anzuwenden. Betroffene Personengruppen sind vor allem die Hinweisgeberinnen und Hinweisgeber sowie die beschuldigten Personen.

Die Aufsichtsbehörden beschränken sich auf die Beurteilung der datenschutzrechtlichen Zulässigkeit der personenbezogenen Datenverarbeitung bei Meldeverfahren unter Einsatz von firmeninternen Whistleblowing-Hotlines nach den Vorschriften der DS-GVO. Die Übermittlung von personenbezogenen Daten in Drittstaaten – beispielsweise aufgrund des US-amerikanischen Sarbanes-Oxley Act (SOX) – ist nicht Gegenstand der datenschutzrechtlichen Beurteilung der vorliegenden Orientierungshilfe.

Die Orientierungshilfe richtet sich in erster Linie an die Wirtschaft.

B Verstöße

Interne Verfahren zur Meldung von Missständen werden in der Regel aus dem Bedürfnis eingerichtet, zuverlässige Grundsätze der Unternehmensführung in den täglichen Betrieb der Unternehmen einzuführen. Verfahren zur Meldung von Missständen sind als zusätzlicher Mechanismus für die Beschäftigten gedacht, um Missstände intern über einen bestimmten Kanal zu melden. Sie ergänzen die regulären Informations- und Meldekanäle der Einrichtung, wie beispielsweise Arbeitnehmervertretungen, Linienmanagement, Qualitätskontrollpersonal oder interne Auditoren, die eigens dafür eingestellt sind, solche Missstände zu melden. Die Meldung von Missständen ist als Ergänzung zum internen Management zu sehen und nicht als Ersatz dafür. Bei der Einführung von unternehmensinternen Verhaltensregeln sind arbeitsrechtliche Erfordernisse zu berücksichtigen und Mitbestimmungsrechte des Betriebsrats zu wahren.

Verstöße, die über ein internes Verfahren als Missstand gemeldet werden, können sein:

1. Verhaltensweisen, die einen sich gegen das Unternehmensinteresse richtenden Straftatbestand erfüllen (insbesondere Betrug und Fehlverhalten in Bezug auf die Rechnungslegung sowie interne Rechnungslegungskontrollen, Wirtschaftsprüfungsdelikte, Korruption, Banken- und Finanzkriminalität, verbotene Insidergeschäfte),
2. Verhaltensweisen, die gegen Menschenrechte (beispielsweise Ausnutzung günstiger Produktionsbedingungen im Ausland durch in Kauf genommene Kinderarbeit), Umwelt-

[1] Amtsblatt der Europäischen Union vom 04.05.2016 – L 119/1 -
[2] Bundesgesetzblatt I vom 05.07.2017, S. 2097 ff.

schutzbelange oder gegen Vorschriften nach dem Allgemeinen Gleichbehandlungsgesetz (AGG) verstoßen,

3. Verhaltensweisen, die unternehmensinterne Ethikregeln beeinträchtigen (beispielsweise Wal-Mart-Fall).[3]

C Datenströme beim Whistleblowing

Bei der Meldung von Verstößen gegen Verhaltensregeln werden personenbezogene Daten verarbeitet. Die Datenerhebung umfasst Angaben über die beschuldigte Person, die (angeblichen) Verhaltensverstöße sowie die entsprechenden Sachverhalte. Sofern ein Meldeverfahren regelt, dass Hinweise anonym erfolgen können, werden, falls Hinweisgeberinnen und Hinweisgeber sich nicht selbst anders äußern, keine personenbezogenen Daten über sie erhoben. Andernfalls kommen personenbezogene Angaben wie Name der meldenden Person, ihre Position im Unternehmen und gegebenenfalls auch die Umstände ihrer Beobachtung in Betracht. Je nach Ausgestaltung des Meldeverfahrens besteht die Möglichkeit der weiteren internen Verarbeitung durch die dafür vorgesehene Abteilung (beispielsweise Revision, Compliance). Bei verbundenen Unternehmen ist eine Übermittlung der personenbezogenen Daten an die Konzernmutter oder andere zum Konzern gehörende Unternehmen denkbar.

D Datenschutzrechtliche Zulässigkeit (Rechtsgrundlagen)

Die Verarbeitung personenbezogenen Daten ist nur rechtmäßig, wenn die DS-GVO, eine spezifischere Rechtsvorschrift oder eine Kollektivvereinbarung nach Art. 88 DS-GVO dies erlaubt oder die betroffene Person eingewilligt hat (Art. 6 Abs. 1 lit a DS-GVO).

D 1 Vertragsverhältnis gemäß Art. 6 Abs. 1 lit. b DS-GVO

Art. 6 Abs. 1 lit. b DS-GVO ist nicht anzuwenden, weil das Beschäftigungsverhältnis bei der von der Unternehmensleitung veranlassten oder ihr zuzurechnenden Datenerhebung nicht unmittelbar betroffen ist. Beurteilungsgrundlage sind vielmehr Art. 6 Abs. 1 lit. c und lit. f DS-GVO.

D 2 Rechtliche Verpflichtung gemäß Art. 6 Abs. 1 lit. c DS-GVO

Eine rechtliche Verpflichtung zur Einrichtung einer firmeninternen Whistleblowing-Hotline ergibt sich für den Bankensektor aus § 25a Abs. 1 Satz 6 Nr. 3 Gesetz über das Kreditwesen (KWG). Auch im Zusammenhang mit der Korruptionsbekämpfung bestehen rechtliche Verpflichtungen zur Einrichtung von verstärkten Kontrollmechanismen. Klarstellend wird darauf

[3] vgl. Mitbestimmung des Betriebsrates: Beschluss des LAG Düsseldorf vom 14.11.2005 – 10 TaBV 46/05 –

hingewiesen, dass hierbei nur rechtliche Verpflichtungen aus dem Unionsrecht oder dem Recht eines Mitgliedsstaates in Betracht kommen.

D 3 Abwägung nach Art. 6 Abs. 1 lit. f DS-GVO

D 3.1 Erforderlichkeit zur Wahrung der berechtigten Interessen des Unternehmens

Die Einrichtung von Verfahren zur Meldung von Missständen kann zur Verwirklichung des berechtigten Interesses für erforderlich gehalten werden. Solche Interessen haben die für die Verarbeitung Verantwortlichen sowie Dritte, denen die Daten übermittelt werden. Das Ziel der Gewährleistung der finanziellen Sicherheit auf den internationalen Finanzmärkten und insbesondere die Verhütung von Betrug und Fehlverhalten in Bezug auf die Rechnungslegung, interne Rechnungslegungskontrollen, Fragen der Wirtschaftsprüfung sowie die Bekämpfung von Korruption, Banken- und Finanzkriminalität oder Insider-Geschäften kann ein berechtigtes Interesse des Arbeitgebers darstellen, das die Verarbeitung personenbezogener Daten mittels Verfahren zur Meldung von Missständen in diesen Bereichen rechtfertigt. Eine Datenverarbeitung zur Wahrung dieses Interesses wäre jedoch nur zulässig, sofern die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, nicht überwiegen.

D 3.2 Interessen, Grundrechte und Grundfreiheiten der betroffenen Person

Bei einem Verfahren zur Meldung von Missständen besteht die Gefahr der Viktimisierung (eine Person „zum Opfer machen“) und Stigmatisierung (Zuschreibung von Merkmalen und Eigenschaften, die diskreditierbar sind) der belasteten Person. Eine Prüfung schutzwürdiger Interessen dieser Person wird bei konkreten, auf relevante Verfehlungen hinweisenden Verdachtsmomenten besonders sorgfältig vorzunehmen sein.

Die Verarbeitung von personenbezogenen Daten, die mit der Aufdeckung von Verstößen der in den Abschnitten **B 1** und **B 2** beschriebenen Kategorien (sogenannte „harte Faktoren“) in Zusammenhang stehen, kann als zulässig angesehen werden. In der Regel wird die Interessenabwägung zugunsten des berechtigten Interesses des Unternehmens ausfallen, da die Meldung solcher Verstöße rechtliche Konsequenzen durch beispielsweise Strafverfolgung, Schadensersatzforderungen und Imageschaden vermeiden hilft, wenn das Verfahren im Übrigen datenschutzgerecht ausgestaltet ist (Kapitel **E**).

Bei Verhaltensweisen entsprechend der Kategorie **B 3** (sogenannte „weiche Faktoren“) ist die Zulässigkeit ebenso nur im Einzelfall zu beurteilen. Hierbei ist zu berücksichtigen, dass bestimmte Verhaltensweisen von vornherein nicht in eine Beurteilung oder Interessenabwägung einbezogen werden dürfen.[4]

Grundsätzlich ist bei Fallgruppe **B 3** anzunehmen, dass die schutzwürdigen Interessen der Betroffenen überwiegen. Dabei sind auch arbeitsrechtliche Grundsätze zu beachten. Für die

[4] s. LAG Düsseldorf, Beschluss vom 14.11.2005, NZA 2006,63. Nach Ansicht des Gerichts ist der Regelungskomplex „Private Beziehungen/ Liebesbeziehungen“ wegen Verstoßes gegen Art. 1 und 2 GG grundgesetzwidrig und damit unwirksam.

„weichen Faktoren“ der internen Verhaltensregeln (beispielsweise „Freundlichkeit bei der Kundenbetreuung“) fehlt es zumeist schon an einer klar umrissenen Definition, um einen Verstoß einwandfrei identifizieren zu können. Außerdem ist ein Zusammenhang zwischen dem Verstoß und einem erheblichen Schaden für das Unternehmen (vergleichbar der in den Abschnitten **B 1** und **B 2** beschriebenen Kategorien) nicht erkennbar, so dass schon Zweifel an einem berechtigten Interesse des Verantwortlichen bestehen. Daher dürfte in diesen Fällen im Grundsatz davon auszugehen sein, dass überwiegende Interessen der betroffenen Person bestehen und eine Verarbeitung personenbezogener Daten insoweit unzulässig ist.

D 4 Spezifischere Vorschriften gemäß Art. 88 DS-GVO

Eine spezifischere Vorschrift im Sinne des Art. 88 DS-GVO ist § 26 Abs. 1 Satz 2 BDSG. Danach dürfen zur Aufdeckung von Straftaten personenbezogene Daten von Beschäftigten nur dann verarbeitet werden, wenn zu dokumentierende tatsächliche Anhaltspunkte den Verdacht begründen, dass die betroffene Person im Beschäftigungsverhältnis eine Straftat begangen hat, die Verarbeitung zur Aufdeckung erforderlich ist und das schutzwürdige Interesse der oder des Beschäftigten an dem Ausschluss der Verarbeitung nicht überwiegt, insbesondere Art und Ausmaß im Hinblick auf den Anlass nicht unverhältnismäßig sind.

Des Weiteren muss der Verantwortliche geeignete Maßnahmen treffen, um sicherzustellen, dass insbesondere die in Art. 5 DS-GVO dargelegten Grundsätze für die Verarbeitung personenbezogener Daten eingehalten werden (§ 26 Abs. 5 BDSG). Die Vorschrift des § 26 Abs. 1 Satz 2 BDSG ist jedoch nur anwendbar, wenn es sich um die Aufdeckung von Straftaten im Beschäftigungskontext handelt (Verhaltensweisen nach Abschnitt **B 1**).

Nach § 26 Abs. 4 Satz. 1 BDSG können Kollektivvereinbarungen, das heißt Tarifverträge und Betriebsvereinbarungen, Grundlage für die Verarbeitung personenbezogener Daten im Beschäftigungsverhältnis sein. Bei der Abfassung einer solchen Vereinbarung sind die Vorgaben der DS-GVO zu beachten. So muss eine Betriebsvereinbarung, die Verhaltensregeln beinhaltet, gemäß Art. 5 Abs. 1 lit. b DS-GVO die Datenerhebung und -weiterverarbeitung eindeutig regeln. Die bloße Beschreibung einer Aufgabe oder eines Zwecks reicht nicht aus, auch wenn zu deren Erledigung personenbezogene Beschäftigtendaten verarbeitet werden müssen.

Zusätzlich muss eine Betriebsvereinbarung angemessene und besondere Maßnahmen zur Wahrung der menschlichen Würde, der berechtigten Interessen und der Grundrechte der betroffenen Personen, insbesondere im Hinblick auf die Transparenz der Verarbeitung, die Übermittlung personenbezogener Daten innerhalb einer Unternehmensgruppe oder eine Gruppe von Unternehmen, die eine gemeinsame Wirtschaftstätigkeit ausüben, und die Überwachung am Arbeitsplatz umfassen. (§ 26 Abs. 4 Satz 2 BDSG in Verbindung mit Art. 88 Abs. 2 DS-GVO).

D 5 Einwilligung der betroffenen Person gemäß Art. 6 Abs. 1 lit. a DS-GVO

Die Wirksamkeit einer Einwilligung im Rahmen eines solchen Verfahrens muss insbesondere an die Kriterien der Freiwilligkeit und Information über die Datenverarbeitung anknüpfen. § 26 Abs. 2 Satz 1 BDSG gibt vor, dass für die Beurteilung der Freiwilligkeit der Einwilligung insbesondere die im Beschäftigungsverhältnis bestehende Abhängigkeit der beschäftigten Person sowie die Umstände, unter denen die Einwilligung erteilt wird, zu berücksichtigen sind.

Die besondere Bedeutung der Freiwilligkeit der Einwilligung wird schon allgemein in Art. 7 Abs. 4 DS-GVO ausdrücklich betont. Anforderungen an eine wirksame Einwilligung finden sich in Art. 7 DS-GVO sowie Erwägungsgrund (EG) 32, 42 und 43. Insbesondere ist die Einwilligung nur dann freiwillig, wenn die betroffene Person eine echte oder freie Wahl hat und somit in der Lage ist, die Einwilligung zu verweigern oder zurückzuziehen, ohne Nachteile zu erleiden.

Gleichwohl kann die Verarbeitung personenbezogener Daten für firmeninterne Warnsysteme aufgrund der Rechtsvorschriften des Art. 6 Abs. 1 lit. f DS-GVO und des § 26 Abs. 1 Satz 2 BDSG grundsätzlich nicht auf die Einwilligung gestützt werden, sondern nur auf diese Vorschriften. Einzige Ausnahme ist die Einwilligung einer Hinweisgeberin oder eines Hinweisgebers, soweit die betroffene Person ihre Identität gewollt oder bewusst dem Arbeitgeber oder der externen Stelle preisgegeben möchte (siehe Abschnitt **E 3**).

E Datenschutzgerechte Gestaltung eines Meldeverfahrens mittels Hotline

E 1 Grundsätze

Personenbezogene Daten müssen für festgelegte, eindeutige und legitime Zwecke erhoben und dürfen nicht in einer damit nicht zu vereinbarenden Weise weiterverarbeitet werden (Art. 5 Abs. 1 lit. b DS-GVO). Darüber hinaus müssen die verarbeiteten Daten den Zwecken entsprechen, für die sie erhoben und/oder weiterverarbeitet werden, dafür erforderlich sein und sich auf das notwendige Maß beschränken. Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen trifft der Verantwortliche sowohl zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung als auch zum Zeitpunkt der eigentlichen Verarbeitung geeignete technische und organisatorische Maßnahmen – beispielsweise Pseudonymisierung – die dafür ausgelegt sind, die Datenschutzgrundsätze – etwa Datenminimierung – wirksam umzusetzen und die notwendigen Garantien in die Verarbeitung aufzunehmen, um den Anforderungen der DS-GVO zu genügen und die Rechte der betroffenen Personen zu schützen (Art. 25 Abs. 1 DS-GVO).

Der Verantwortliche muss Maßnahmen treffen, die sicherstellen, dass nicht zutreffende oder unvollständige Daten gelöscht oder berichtigt werden. Informationen an die betroffene Person zu dem mit einer Whistleblowing-Hotline verfolgten Zweck müssen in klarer, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache übermittelt werden. Missverständnisse, jede auch nur geringfügige oder lediglich vermutete Unregelmäßigkeit sei zu melden, sollten vermieden werden. Klar sein muss, dass kein Interesse an unkonkretisierten Beschuldigungen besteht.

E 2 Betroffener Personenkreis

Nach dem Grundsatz der Datenminimierung gemäß Art. 5 Abs. 1 lit. c DS-GVO hat der Verantwortliche zu prüfen, inwieweit der für eine Meldung in Betracht kommende Personenkreis bei einer Whistleblowing-Hotline möglichst eingegrenzt und konkret bestimmt werden kann. Das Unternehmen, das ein Verfahren zur Meldung von Missständen einführt, sollte ebenfalls sorgfältig prüfen, ob es angebracht wäre, die Zahl der Personen zu begrenzen, die über das Verfahren gemeldet werden können, insbesondere in Anbetracht der Schwere der gemeldeten mutmaßlichen Verstöße. Entscheidend kommt es dabei jedoch auf die Umstände im Einzelfall an.

E 3 Anonymer oder personenbezogener Hinweis

Anonymität begünstigt gegenüber der namentlichen Nennung von ‚Ross und Reiter' eher Missbrauch und Denunziantentum. Einer durch anonymen Hinweis gemeldeten Person bleibt keine Möglichkeit, sich gegen eine etwaige Verleumdung in einem rechtsstaatlichen Verfahren zur Wehr zu setzen. Ein von vornherein auf die Erhebung personenbezogener Daten über Whistleblower abstellendes Verfahren hat jedoch den Nachteil, dass auch bei gewünschten Hinweisen ein Abschreckungseffekt besteht. Hinweisgeberinnen und Hinweisgeber müssen nämlich damit rechnen, ihren Arbeitsplatz zu verlieren, wenn sie unter Offenbarung ihrer Identität Missstände in ihrem Unternehmen aufdecken. Nach § 626 Abs. 1 Bürgerliches Gesetzbuch (BGB) ist die fristlose Kündigung eines Arbeitsvertrags erlaubt, wenn dem Kündigenden (hier: Arbeitgeber) die Fortsetzung des Dienstverhältnisses aus einem „wichtigen Grund" nicht zugemutet werden kann.

Der Europäische Gerichtshof für Menschenrechte (EGMR) stellte 2011 fest, dass der Staat der Pflicht unterliege, die Wahrnehmbarkeit der Meinungsfreiheit auch im privaten Verhältnis von Arbeitgeber und Arbeitnehmer zu schützen. Der gutgläubig agierende Arbeitnehmer habe prinzipiell das Recht, strafbare Handlungen auch seines Arbeitgebers zur Anzeige zu bringen. Jede Person, die Informationen preisgibt, müsse nach den Umständen des Einzelfalls prüfen, ob die Informationen zutreffend und verlässlich sind. Von dem gutgläubigen Erstatter einer Strafanzeige könne aber vernünftigerweise nicht erwartet werden, vorherzusehen, ob die strafrechtlichen Ermittlungen auch zu einer Anklage führen werden.[5]

[5] EGMR Nr. 28274/08 (5. Kammer) – Urteil vom 21.07.2011

Die Informationsfreiheitsbeauftragten in Deutschland verlangen, dass Whistleblowern die vertrauliche Behandlung des Hinweises zugesagt werden muss, ebenso einen gesetzlich geregelten effektiven Schutz von Whistleblowern, die über Rechtsverstöße im öffentlichen und nicht öffentlichen Bereich berichten.[6] Der Europarat hat in seiner Empfehlung zum Whistleblowerschutz am 30.04.2014 ihre Mitgliedstaaten aufgefordert, einen gesetzlichen Rahmen zu schaffen, der Menschen schützt, die auf Verletzungen und Gefährdungen des Öffentliches Interesses im Zusammenhang mit ihrer Arbeit hinweisen.[7]

Gleichwohl gibt es derzeit in Deutschland keinen gesetzlich geregelten oder wirksamen Whistleblowerschutz, ausgenommen § 25a Abs. 1 Satz 6 Nr. 3 KWG.

Zudem gibt es keine gesicherten Erkenntnisse, ob und in welchem Umfang Hinweise auf Missstände in einem Unternehmen unbegründet waren. Nach den Erfahrungen der Datenschutz-Aufsichtsbehörden haben sich - auch anonyme - Hinweise über Datenschutzverstöße regelmäßig nicht als unbegründet erwiesen.

In Abwägung der genannten Interessen ist das folgende Vorgehen zu empfehlen:

Verfahren zur Meldung von Missständen stellen sicher, dass Hinweise regelmäßig anonym erfolgen. Für die Verarbeitung von Angaben zur Identität der Hinweisgeberin oder des Hinweisgebers gibt es keine Rechtsgrundlage (Kap. **D 5** letzter Absatz). Soweit eine Person eine Meldung mit Hilfe eines solchen Verfahrens unter bewusster oder gewollter Darlegung ihrer Identität machen möchte, sollte sie bei der ersten Kontaktaufnahme mit dem System vorher darauf hingewiesen werden, dass ihre Identität während aller internen oder außergerichtlichen Schritte des Verfahrens vertraulich behandelt wird, allerdings auch, dass die beschuldigte Person über die Identität der Hinweisgeberin oder des Hinweisgebers grundsätzlich spätestens einen Monat nach der Meldung informiert werden muss (Art. 14 Abs. 3 lit. a DS-GVO, näher hierzu unter **4.1**).

Wenn die Hinweisgeberin oder der Hinweisgeber trotz dieser Hinweise ihre Identität bewusst und gewollt preisgeben möchte und die Angaben verarbeitet werden sollen, kommt eine Einwilligung dieser Person in Frage. Daher ist die betroffene Person vor der Einwilligung über ihr Recht nach Art. 7 Abs. 2 DS-GVO in Kenntnis zu setzen, dass sie die Einwilligung widerrufen kann, dies jedoch nur bis zu einem Monat nach erfolgter Meldung wirksam möglich ist. Die Einwilligung der betroffenen Person in die Preisgabe ihrer Identität ist nach Art. 7 Abs. 1 DS-GVO vom Arbeitgeber oder der externen Stelle nachzuweisen. Gleichwohl ist der Arbeitgeber oder die externe Stelle trotz dieser Einwilligung verpflichtet, geeignete technische und organisatorische Maßnahmen zu treffen, die diese auch nur vorübergehende Vertraulichkeit der Identität der betroffenen Person gewährleisten (siehe **Nr. 4** und **5**).

[6] Entschließungen der 18. und 27. Konferenz der Informationsfreiheitsbeauftragten vom 24.06.2009 und 28.11.2013

[7] https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805c5ea5

E 4 Unterrichtungs- und Auskunftspflichten

Der Verantwortliche muss, wenn personenbezogene Daten bei betroffenen Personen erhoben werden, diese nach Art. 13 DS-GVO insbesondere über die Zweckbestimmung der Erhebung, Verarbeitung oder Nutzung personenbezogener Daten unterrichten. Dies gilt nicht, wenn und soweit die betroffene Person bereits über die Informationen verfügt (Art. 13 Abs. 4 DS-GVO). Sofern Betriebsvereinbarungen über das Meldeverfahren mit Regelungen zur personenbezogenen Datenverarbeitung abgeschlossen wurden, hat sie das Unternehmen so auszulegen, dass sämtliche Beschäftigten, auch die neu eingestellten, in der Lage sind, sich ohne besondere Umstände mit dem Inhalt vertraut zu machen (§ 77 Abs. 2 Betriebsverfassungsgesetz - BetrVG).[8]

E 4.1 Information der beschuldigten Person

Werden personenbezogene Daten für die Meldung von Missständen ohne Kenntnis der betroffenen Person erhoben, ist diese nach Art. 14 DS-GVO insbesondere von der Speicherung, der Art der Daten, der Zweckbestimmung Verarbeitung und der Identität des Verantwortlichen und gegebenenfalls der Hinweisgeberin oder des Hinweisgebers zu informieren.

Wenn das Risiko erheblich wäre, dass eine solche Unterrichtung die Fähigkeit des Unternehmens zur wirksamen Untersuchung des Vorwurfs oder zur Sammlung der erforderlichen Beweise gefährden würde, kann die zu erfolgende Information der beschuldigten Person so lange aufgeschoben werden, wie diese Gefahr besteht. Grundlage hierfür ist Art. 14 Abs. 5 lit. b DS-GVO, wonach die Information nicht erteilt werden muss, wenn die Verwirklichung der Ziele der Verarbeitung zumindest ernsthaft beeinträchtigt würde. Andernfalls müsste die Information nach spätestens einem Monat gegeben werden (Art. 14 Abs. 3 lit. a DS-GVO). Eine dauerhafte Geheimhaltung dürfte angesichts einer möglichen Beeinträchtigung der Persönlichkeitsrechte der beschuldigten Person und seiner Verteidigungsrechte ausgeschlossen sein. Als Maßnahme zum Schutz der berechtigten Interessen der beschuldigten Person nach Art. 14 Abs. 5 lit. b DS-GVO muss die Information daher dann nachgeholt werden, sobald der Grund für den Aufschub entfallen ist.

Eine Pflicht zur Benachrichtigung besteht auch nicht, wenn personenbezogene Daten gemäß dem Unionsrecht oder dem Recht der Mitgliedstaaten dem Berufsgeheimnis, einschließlich einer satzungsmäßigen Geheimhaltungspflicht, unterliegen und daher vertraulich behandelt werden müssen. (Art. 14 Abs. 5 lit. d DS-GVO). Das Gleiche gilt, wenn diese Pflicht durch Rechtsvorschriften der Union oder der Mitgliedstaaten zum Zweck des Schutzes der betroffenen Person oder Rechte und Freiheiten anderer Personen beschränkt wird (Art. 23 Abs. 1 lit. i DS-GVO). Eine derartige Regelung enthält das BDSG jedoch nicht. Die Vorschrift des § 29 Abs.1 Satz 1 Bundesdatenschutzgesetz (BDSG) schränkt die Informationspflichten des Arbeitgebers oder einer externen Stelle hinsichtlich der Identität der Hinweisgeberin oder des Hinweisgebers wirksam ein. Danach besteht eine Pflicht zur Information nicht, soweit durch ihre Erfüllung Informationen offenbart würden, die wegen der überwiegenden berechtigten Interessen eines Dritten geheim gehalten werden müssen.

[8] Fitting, Anm. 25 zu § 77 BetrVG

E 4.2 Auskunft

Nach Art. 15 DS-GVO hat die betroffene Person, sowohl die Hinweisgeberin oder der Hinweisgeber als auch die beschuldigte Person, Anspruch auf Auskunft der zu ihrer Person gespeicherten Daten, auch soweit sie sich auf Herkunft und Empfänger beziehen. Der Auskunftsanspruch der beschuldigten Person kollidiert hinsichtlich der Identität der meldenden Person grundsätzlich mit einer für das Meldeverfahren vorgesehenen anonymen Meldung (siehe dazu Abschnitt **E 3**). Allerdings besteht keine Auskunftsverpflichtung, wenn diese durch Rechtsvorschriften der Union oder der Mitgliedstaaten zur Verhütung oder Aufdeckung von Straftaten oder zum Zweck des Schutzes der betroffenen Person oder Rechte und Freiheiten anderer Personen beschränkt wird (Art. 23 Abs. 1 lit. d und lit. i DS-GVO). Diese Beschränkung regelt § 29 Abs.1 Satz 2 BDSG, wonach das Recht auf Auskunft nicht besteht, soweit durch die Auskunft Informationen offenbart würden, die wegen der überwiegenden berechtigten Interessen eines Dritten geheim gehalten werden müssen.

E 5 Weitergabe an Dritte

Grundsätzlich ist eine Weitergabe personenbezogener Daten der beschuldigten Person an Dritte nicht zulässig. Akteneinsichtsrechte in einem etwaigen Strafverfahren bleiben unberührt. Personenbezogene Daten der beschuldigten Person können nach Art. 6 Abs. 1 lit. f DS-GVO in Verbindung mit § 24 Abs. 1 Nr. 1, letzte Alternative BDSG zur Verfolgung von Straftaten übermittelt werden.

E 6 Berichtigung, Sperrung und Löschung

Nach Art. 5 Abs. 1 lit. d DS-GVO müssen personenbezogene Daten sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein. Es sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke der Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden. Art. 18 DS-GVO gibt der betroffenen Person unter bestimmten Voraussetzungen zudem das Recht, die Einschränkung der Verarbeitung zu verlangen. Grundsätzlich sollten Daten innerhalb von zwei Monaten nach Abschluss der Untersuchung gelöscht werden. Eine darüber hinausgehende Speicherung ist nur für die Dauer der Klärung erforderlicher weiterer rechtlicher Schritte wie Disziplinarverfahren oder Einleitung von Strafverfahren zulässig. Personenbezogene Daten im Zusammenhang mit Meldungen, die von der Organisationseinheit, die für die Bearbeitung der Meldung zuständig ist, als grundlos erachtet werden, sollten unverzüglich gelöscht werden.

E 7 Widerspruch

Die betroffene Person hat nach Art. 21 Abs. 1 DS-GVO das Recht, aus Gründen, die sich aus ihrer besonderen Situation ergeben, jederzeit gegen die Verarbeitung sie betreffender personenbezogener Daten, die aufgrund von Art. 6 Abs. 1 lit. e oder f DS-GVO erfolgt, Widerspruch einzulegen; dies gilt auch für ein auf diese Bestimmungen gestütztes Profiling. Der Verantwortliche verarbeitet die personenbezogenen Daten nicht mehr, es sei denn, er kann

zwingende schutzwürdige Gründe für die Verarbeitung nachweisen, die die Interessen, Rechte und Freiheiten der betroffen Person überwiegen oder die Verarbeitung dient der Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen.

E 8 Beteiligung der Datenschutzbeauftragten

Bei Whistleblowing-Systemen handelt es sich um Verfahren, bei denen nach Art. 38 Abs. 1 DS-GVO die Datenschutzbeauftragten ordnungsgemäß und frühzeitig in alle mit dem Schutz personenbezogener Daten zusammenhängenden Fragen einzubinden sind.

E 9 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 (Datenschutz-Folgenabschätzung nach Art. 35 Abs. 1 DS-GVO). Ein Verfahren zur Meldung von Missständen unterliegt wegen des besonders hohen Risikos für die Rechte und Freiheiten natürlicher Personen einer Datenschutz-Folgenabschätzung.

E 10 Beauftragung externer Stellen

Wenn Unternehmen externe Dienstleister mit einem Teil der Verwaltung des Systems zur Meldung von Missständen beauftragen, behalten sie dennoch die Verantwortung für die daraus hervorgehenden Verarbeitungen, soweit diese als Auftragsverarbeiter im Sinne des Art. 28 Abs. 1 DS-GVO tätig werden. Der Auftragsverarbeiter muss dabei im Auftrag des Verantwortlichen hinreichend Garantien dafür bieten, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen der DS-GVO erfolgt und den Schutz der Rechte der betroffenen Personen gewährleistet. Der hierfür abzuschließende Vertrag sieht gemäß Art. 28 Abs. 3 Satz 2 lit. a DS-GVO unter anderem vor, dass der Auftragsverarbeiter die personenbezogenen Daten nur auf dokumentierte Weise des Verantwortlichen verarbeitet - auch in Bezug auf die Datenübermittlung an ein Drittland.

Andernfalls liegt bei der Beauftragung externer Stellen im Rahmen einer Funktionsübertragung eine Übermittlung vor, deren Zulässigkeit nach Art. 6 Abs. 1 lit. f DS-GVO zu beurteilen ist. Je nach Ausgestaltung des Meldeverfahrens ist zwischen dem berechtigten Interesse der verantwortlichen Stelle und den Interessen oder Grundrechten und Grundfreiheiten der betroffenen Personen abzuwägen. Die Zulässigkeit der Übermittlung an externe Stellen ist ebenfalls Gegenstand der Datenschutz-Folgenabschätzung nach Art. 35 DS-GVO.

Nach Art. 35 Abs. 1 DS-GVO entscheidet der für Datenverarbeitung Verantwortliche über die Durchführung einer Datenschutz-Folgenabschätzung. Wenn eine externe Stelle damit beauf-

tragt werden soll, kann davon ausgegangen werden, dass dies angesichts ihrer Komplexität (beispielsweise Erfordernisse nach Art. 35 Abs. 7 DS-GVO) nur im Rahmen einer Funktionsübertragung möglich ist.

Die Beauftragung einer externen Stelle außerhalb der Unternehmensorganisation (Konzernverbund) kann sich bei Beachtung der datenschutzrechtlichen Vorschriften im Übrigen als vorteilhaft erweisen, weil möglicherweise eine gewisse, das Missbrauchsrisiko verringernde Hemmschwelle entsteht.

E 11 Technische und organisatorische Maßnahmen

Um die Vorgaben des Art. 32 DS-GVO zu erfüllen, sind geeignete technische und organisatorische Maßnahmen zu treffen. Dies gilt insbesondere wegen der zugesicherten Vertraulichkeit und für die Löschungsverpflichtung. Bei interner Datenverarbeitung ist zu empfehlen, dass die Whistleblowing-Hotline nicht innerhalb der Personalverwaltung organisiert und betrieben wird. Um zu gewährleisten, dass Unbefugte Datenverarbeitungssysteme nicht nutzen können, bieten sich neben einem Berechtigungskonzept und einer Passwortrichtlinie auch Verschlüsselungsverfahren im Hinblick auf die Sensibilität der Daten an.[9] Zu den Maßnahmen gehören auch Protokollierung von Dateneingaben und Löschroutinen.

F Ergebnis

Das Meldeverfahren mittels firmeninterner Whistleblowing-Hotlines lässt sich unter besonderer Berücksichtigung des von dem Unternehmen verfolgten Zwecks und der Einrichtungsmodalitäten datenschutzgerecht gestalten und betreiben. Für Unternehmen, die solche Warnsysteme beabsichtigen einzurichten, empfiehlt sich eine rechtzeitige Abstimmung mit allen zu Beteiligenden (beispielsweise Innenrevision, Beauftragte der Geschäftsleitung, Datenschutzbeauftragte, Betriebsvertretung). Zur Klärung von Zweifelsfragen stehen auch die Datenschutzbehörden zur Verfügung.

[9] BSI-IT-Grundschutzhandbuch