www.compliance-berater.de

Compliance Berater

9 / 2023

Betriebs-Berater Compliance

24.8.2023 | 11.Jg
Seiten 333–380

EDITORIAL

Künstliche Intelligenz und Compliance | I

Prof. Dr. Stefan Behringer

AUFSÄTZE

Compliance-Lernkurve? Datenschutz-Bußgeldverfahren aus behördlicher Sicht | 333

Maria Christina Rost und Andreas Wigger

Internal Investigations und Datenschutz aus Sicht der Datenschutzaufsichtsbehörden | 340

Thomas Kahl und Jan Vogel

Datenschutzkonformes Tracking zu Werbe- und Marketingzwecken | 345

Laurin Maran

Zum Spannungsfeld von Hinweisgeberschutz und Datenschutzrecht | 351

Dr. Dominik Nikol

Datenschutzkonforme Ausgestaltung von Hinweisgebersystemen in Konzernkonstellationen | 356

Dr. Marius Haak und Jan Spittka

DSGVO-Zertifizierung – Das Europäische Datenschutzsiegel | 361

Timo Herold und Malte Tober

RECHTSPRECHUNG

EuGH: BKartA darf Datenschutz bei sozialem Netzwerk prüfen | 364

EuGH: Umfang des Anspruchs auf Kopie der personenbezogenen Daten | 375

Schwerpunktheft Datenschutz-Compliance

Fachmedien Recht und Wirtschaft | dfv Mediengruppe | Frankfurt am Main

CB-BEITRAG

Dr. Marius Haak, RA, und Jan Spittka, RA

Datenschutzkonforme Ausgestaltung von Hinweisgebersystemen in Konzernkonstellationen

Seit dem 2.7.2023 sind die ersten Unternehmen nach dem HinSchG dazu verpflichtet, eine interne Meldestelle zu betreiben, an die sich Beschäftigte bei vermeintlichen Rechtsverstößen wenden können. Der Gesetzgeber hat dabei für Unternehmen die Möglichkeit eröffnet, die interne Meldestelle „auch bei einer anderen Konzerngesellschaft" für mehrere Unternehmen einrichten zu können. Neben den Vorgaben des HinSchG müssen die Hinweisgebersysteme dabei DSGVO-konform umgesetzt werden. Dieser Beitrag gibt einen Überblick über die verschiedenen Ausgestaltungsmöglichkeiten von Hinweisgebersystemen in Konzernkonstellationen und ihre datenschutzrechtlichen Anforderungen.

I. Einrichtung und Ausgestaltung interner Meldestellen nach dem HinSchG

Beschäftigungsgeber ab 50 Beschäftigten[1] müssen gem. § 12 Abs. 1, Abs. 2 Hinweisgeberschutzgesetz („HinSchG") eine Stelle für interne Meldungen einrichten und betreiben, an die sich Beschäftigte bei Verstößen[2] wenden können.[3]

Die internen Meldestellen können gem. § 14 Abs. 1 HinSchG von einer bei dem Beschäftigungsgeber beschäftigten Person, einer aus mehreren beschäftigten Personen bestehenden Arbeitseinheit oder auch einem „Dritten" betrieben werden. Voraussetzung ist die Unabhängigkeit und Vertraulichkeit der internen Meldestelle, und auch eine personelle Kontinuität sollte vorliegen.[4]

In Konzernkonstellationen bedeutet dies Folgendes: jede einzelne Konzerngesellschaft, die unter den Anwendungsbereich des HinSchG fällt, kann entweder eine eigene interne Meldestelle einrichten oder es kann gemäß „dem konzernrechtlichen Trennungsprinzip […] auch bei einer anderen Konzerngesellschaft (zum Beispiel Mutter-, Schwester-, oder Tochtergesellschaft) eine unabhängige und vertrauliche Stelle als ‚Dritter' […] eingerichtet werden, die auch für mehrere selbstständige Unternehmen in dem Konzern tätig sein kann."[5]

Sowohl in der ersten als auch in der zweiten Alternative kann sich die jeweilige Gesellschaft, die die (konzernweite) interne Meldestelle betreibt, frei entscheiden, ob sie eine rein interne Lösung (z. B. Betrieb der internen Meldestelle durch den Leiter der Compliance-Abteilung[6]) oder eine externe Lösung wählt (z. B. externen Anwälten als Ombudspersonen die Aufgabe des Betreibens einer internen Meldestelle übertragen[7]). Also auch wenn die Konzernlösung gewählt wird, bedeutet dies nicht, dass die Konzerngesellschaft, die als „Dritter" für andere Gesellschaften die interne Meldestelle betreibt, dies zwingend in konzerninterner Eigenregie machen muss. Vielmehr kann sich die im Verhältnis zu der nach dem HinSchG verpflichteten Konzerngesellschaft (Beschäftigungsgeber) als „Dritte" auftretende Konzerngesellschaft bei dem Betrieb der konzernweiten internen Meldestelle ihrerseits eines externen „Dritten", z. B. einer Rechtsanwaltskanzlei, bedienen. In diesen Konstellationen agieren somit zwei „Dritte" i. S. d. HinSchG.

Während der Dritte berechtigt ist, die technischen Meldekanäle und das Personal zur Entgegennahme und Bewertung von Meldungen zur Verfügung zu stellen sowie interne Untersuchungen in den betroffenen Konzernteilen durchzuführen, muss stets die nach dem HinSchG verpflichtete Konzerngesellschaft den Verstoß mit geeigneten Maßnahmen abstellen.[8] Zudem ist sie zur Kooperation mit dem beauftragten „Dritten" verpflichtet, etwa bei erforderlichen Folgemaßnahmen zur Überprüfung der Stichhaltigkeit einer Meldung.[9]

1 Zur besseren Lesbarkeit wird das generische Maskulinum verwendet. Die in diesem Aufsatz verwendeten Personenbezeichnungen beziehen sich – sofern nicht anders kenntlich gemacht – auf alle Geschlechter.

2 Verstöße sind Handlungen oder Unterlassungen im Rahmen einer beruflichen, unternehmerischen oder dienstlichen Tätigkeit, die rechtswidrig sind und Vorschriften oder Rechtsgebiete betreffen, die in den sachlichen Anwendungsbereich nach § 2 HinSchG fallen.

3 Beschäftigungsgeber ab 250 Beschäftigten trifft diese Pflicht seit dem 2.7.2023, Beschäftigungsgeber ab 50 Beschäftigten ab dem 17.12.2023.

4 Siehe BT-Drs. 20/3442, S. 79.

5 Siehe BT-Drs. 20/3442, S. 79; zur Kritik der Expertengruppe der Europäischen Kommission und der Reaktion des Schrifttums siehe *Dilling*, CCZ 2023, 91 ff.

6 Siehe BT-Drs. 20/3442, S. 79 (mit Hinweis auf Erwägungsgrund 56 der HinSch-RL).

7 Siehe BT-Drs. 20/3442, S. 79.

8 Siehe BT-Drs. 20/3442, S. 79.

9 Siehe BT-Drs. 20/3442, S. 79.

II. Relevante datenschutzrechtliche Grundlagen

Der Betrieb der Meldestelle nach dem HinSchG erfordert stets die Verarbeitung[10] personenbezogener Daten[11] i. S. d. Datenschutz-Grundverordnung (DSGVO), sei es über die Personen, die als mutmaßliche Täter Gegenstand der eingehenden Meldungen sind, über weitere in der Meldung erwähnte Personen, etwa Geschädigte oder Zeugen, und auch – soweit die Meldung nicht vollständig anonym erfolgt – über die hinweisgebende Person.

Die Verarbeitung personenbezogener Daten im Zusammenhang mit dem Betrieb einer internen Meldestelle unterliegt daher den Regeln der DSGVO. Verstöße gegen die DSGVO können hierbei zu erheblichen Konsequenzen, wie etwa Geldbußen nach Art. 83 DSGVO oder Schadenersatzansprüchen der betroffenen Personen nach Art. 82 DSGVO, führen.

1. Verteilung der datenschutzrechtlichen Verantwortlichkeit

Die Weichenstellung für die Zuordnung der datenschutzrechtlichen Pflichten ist die korrekte Bestimmung der Verantwortlichkeit unter der DSGVO. Hierbei wird grundsätzlich zwischen dem „Verantwortlichen“[12] und dem „Auftragsverarbeiter“[13] unterschieden. Verantwortlicher ist die Stelle, die über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. Auftragsverarbeiter ist demgegenüber eine Stelle, die zwar personenbezogene Daten verarbeitet, aber gerade nicht über die Zwecke und Mittel der Verarbeitung entscheidet, sondern rein im Auftrag des Verantwortlichen handelt. Beim Verantwortlichen wird weiter differenziert, ob die datenverarbeitende Stelle allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. Im letzteren Fall spricht man von gemeinsam für die Verarbeitung Verantwortlichen.

Gerade in Konstellationen, in denen die interne Meldestelle nicht von bzw. innerhalb der Stelle betrieben wird, die der Beschäftigungsgeber i. S. d. § 3 Abs. 9 HinSchG ist, sondern auf Dritte übertragen wird, stellt sich die Frage, wie das Verhältnis zwischen Beschäftigungsgeber und Drittem zu qualifizieren ist. Das HinSchG trifft keine Aussage zur datenschutzrechtlichen Einordnung Dritter, die der Beschäftigungsgeber gem. § 14 Abs. 1 S. 1 HinSchG mit den Aufgaben einer internen Meldestelle betraut hat. Die folgende Aussage aus der Gesetzesbegründung könnte bei oberflächlicher Betrachtung zwar dahingehend interpretiert werden, dass der Dritte immer als Auftragsverarbeiter einzustufen ist: „Soweit die interne Meldestelle zur Erfüllung der in ihrer Zuständigkeit liegenden Aufgaben personenbezogene Daten verarbeitet, soll vor allem bei internen Meldestellen, die von einer Einzelperson betrieben werden, diese nicht die für die Verarbeitung Verantwortliche im Sinne der datenschutzrechtlichen Vorschriften sein. Soweit externe Dritte im Rahmen einer Auftragsverarbeitung mit der Einrichtung und dem Betreiben der internen Meldestelle beauftragt werden, sind die Vorgaben für Auftragsverarbeitungen zu beachten, vergleiche Artikel 28 DSGVO.“[14]

Bei dieser Formulierung handelt es sich indes keineswegs um eine Festlegung, dass der Betreiber einer Meldestelle nicht Verantwortlicher, sondern stets Auftragsverarbeiter ist. Vielmehr werden lediglich allgemeine datenschutzrechtliche Grundsätze erläutert, nämlich, dass nicht die interne Meldestelle selbst oder gar eine konkret dort tätige natürliche Person der datenschutzrechtlich Verantwortliche ist, sondern das Rechtssubjekt, in dem die interne Meldestelle organisatorisch aufgesetzt ist. Soweit der externe Dritte tatsächlich als Auftragsverarbeiter einzustufen sein sollte, sind selbstverständlich die Voraussetzungen des Art. 28 DSGVO einzuhalten. Die Abgrenzung eines Verantwortlichen von einem Auftragsverarbeiter beim Betrieb der internen Meldestelle erfolgt daher allein nach der DSGVO.[15]

2. Erlaubnistatbestand für die Verarbeitung personenbezogener Daten

Die Verarbeitung personenbezogener Daten ist nur dann zulässig, wenn einer der in Art. 6 Abs. 1 UAbs. 1 DSGVO genannten Erlaubnistatbestände einschlägig ist. Werden sog. besondere Kategorien personenbezogener Daten i. S. d. Art. 9 Abs. 1 DSGVO oder die Verarbeitung personenbezogener Daten über strafrechtliche Verurteilungen und Straftaten i. S. d. Art. 10 DSGVO verarbeitet, müssen zusätzliche Anforderungen eingehalten werden.

Hier hat der deutsche Gesetzgeber mit § 10 HinSchG eine wichtige Grundlage dafür geschaffen, dass die für die Tätigkeit der Meldestelle erforderlichen personenbezogenen Daten ohne Einwilligung der betroffenen Personen verarbeitet werden dürfen. Sofern der Anwendungsbereich des § 10 S. 1 HinSchG, der festlegt, dass die Meldestellen befugt sind, personenbezogene Daten zu verarbeiten, soweit dies zur Erfüllung ihrer in den §§ 13 und 24 HinSchG bezeichneten Aufgaben erforderlich ist, für „letztlich überschaubar“ gehalten[16] oder dessen Inhalt als Hinweis „lediglich deklaratorischer Natur“ angesehen wird[17], weil die Verarbeitung direkt auf Art. 6 Abs. 1 UAbs. 1 lit. c DSGVO (Erfüllung rechtlicher Pflichten) gestützt werden könne, kann dem nicht zugestimmt werden. § 10 S. 1 HinSchG ist die entscheidende Schnittstelle zwischen Art. 6 Abs. 3 S. 1 DSGVO, der das Erfordernis einer spezifischen Rechtsgrundlage für Verarbeitungen im Rahmen des Art. 6 Abs. 1 UAbs. 1 lit. c DSGVO fordert, und den Pflichten des HinSchG.

Der Einstufung des § 10 S. 1 HinSchG als Rechtsgrundlage kann auch nicht entgegengehalten werden, dass die Norm keine spezifischen Anforderungen für die Verarbeitung auf präzise Art und Weise i. S. d. Art. 6 Abs. 2 DSGVO enthalte[18]. Anders als Art. 6 Abs. 3 S. 1 DSGVO enthält diese Vorschrift nämlich gerade keine konkreten Anforderungen an die Rechtsgrundlage, sondern an spezifische Anforderungen für die Verarbeitung sowie sonstige Maßnahmen. Das HinSchG enthält eine Vielzahl solcher Schutzmaßnahmen, wie etwa das Vertraulichkeitsgebot in § 8 HinSchG oder das „Need to know“-Prinzip in § 16 Abs. 2 HinSchG.

Sofern man die Auffassung vertritt, dass auch die Verarbeitung personenbezogener Daten über (mögliche) Straftaten im Rahmen von Compliance-Untersuchungen unter Art. 10 DSGVO fällt,[19] stellt § 10 S. 1 HinschG (i. V. m. mit den flankierenden Schutzmaßnahmen nach dem HinSchG als geeignete Garantien für die Rechte und Freiheiten der betroffenen Personen) auch einen entsprechenden Erlaubnistatbestand nach Art. 10 Abs. 1 S. 1, 2. Var. DSGVO dar. § 10 S. 2 HinSchG ist unproblematisch eine Rechtsgrundlage für die

10 Siehe für die Definition Art. 4 Nr. 2 DSGVO.
11 Siehe für die Definition Art. 4 Nr. 1 DSGVO.
12 Siehe für die Definition Art. 4 Nr. 7 DSGVO.
13 Siehe für die Definition Art. 4 Nr. 8 DSGVO.
14 Gesetzesbegründung, BT-Drs. 20/3442, S. 79 f.
15 So i. E. auch *Rüdiger/Adelberg*, K&R 2023, 172, 172.
16 *Rüdiger/Adelberg*, K&R 2023, 172, 176.
17 *Baade/Hößl*, DStR 2023, 1265, 1267.
18 So *Rüdiger/Adelberg*, K&R 2023, 172, 177.
19 Siehe zum Streitstand *Nolde*, in: Taeger/Gabel, DSGVO BDSG TTDSG, 4. Aufl. 2022, Art. 10 Rn. 12 ff.; *Gola*, in: Gola/Heckmann, DSGVO – BDSG, 3. Aufl. 2022, Art. 10 Rn. 5.

Verarbeitung besonderer Kategorien personenbezogener Daten auf Grundlage der Art. 9 Abs. 2 lit. b DSGVO und Art. 9 Abs. 2 lit. g DSGVO.

3. Weitere datenschutzrechtliche Anforderungen

Darüber hinaus müssen Beschäftigungsgeber und Betreiber der internen Meldestelle auch die übrigen datenschutzrechtlichen Anforderungen der DSGVO einhalten, etwa Informations- und Auskunftspflichten (Art. 13, 14, 15 DSGVO), Löschpflichten (Art. 17 DSGVO), die Sicherheit der Verarbeitung (Art. 32 DSGVO) und die Durchführung einer Datenschutz-Folgenabschätzung (DSFA) (Art. 35 DSGVO).

III. Bewertung einzelner Konstellationen

Wie dargestellt, eröffnet § 14 HinSchG Beschäftigungsgebern die Möglichkeit, die interne Meldestelle in verschiedenen organisatorischen Konstellationen auszugestalten. Im Folgenden gehen wir auf drei mögliche Konstellationen im Rahmen der „Konzernlösung" und ihre unterschiedlichen datenschutzrechtlichen Anforderungen ein. Der Begriff „Konzernlösung" soll dabei verdeutlichen, dass in einem Konzern mehrere Gesellschaften nach dem HinSchG Verpflichtete sind, diese aber keine eigenen internen Meldestellen einrichten und betreiben, sondern eine Konzerngesellschaft die Aufgabe als konzernweite interne Meldestelle übernimmt.

1. Auslagerung der internen Meldestelle auf die Muttergesellschaft

a) Sachverhalt

Der Sachverhalt stellt sich hier wie folgt dar: Ein Konzern besteht aus einer Holding-Gesellschaft als Muttergesellschaft und mehreren Tochtergesellschaften. Während die Holding-Gesellschaft weniger als 50 Personen beschäftigt, haben sämtliche Tochtergesellschaften über 50 Beschäftigte und sind damit Beschäftigungsgeber i. S. d. HinSchG. Die Holding-Gesellschaft trifft die Entscheidung, für sämtliche Tochtergesellschaften als „Dritter" die interne Meldestelle einzurichten und zu betreiben. Als Meldekanal wird ein elektronisches Hinweisgebersystem gewählt, also eine Lösung in Textform (vgl. § 16 Abs. 3 S. 1 HinSchG). Während (lediglich) das technische System durch einen externen Dritten bereitgestellt wird, nimmt der Compliance-Verantwortliche der Holding-Gesellschaft sämtliche Meldungen entgegen und bewertet diese. Dieser führt zudem federführend die internen Untersuchungen in den betroffenen Konzernteilen durch und tauscht sich dabei ggf. zum Zwecke der Überprüfung der Stichhaltigkeit einer Meldung bzw. zum Zwecke der Abstellung von Verstößen mit den verantwortlichen Personen bei den Tochtergesellschaften aus. In diesem Zusammenhang übermittelt er auch im Rahmen der Meldung des Hinweisgebers und der Sachverhaltsaufarbeitung erhaltene personenbezogene Daten an die Tochtergesellschaft.

b) Datenschutzrechtliche Anforderungen

Die Pflicht zur Einrichtung interner Meldestellen trifft in dieser Konstellation die Tochtergesellschaften. Weil die DSGVO kein Konzernprivileg kennt,[20] ist die Holding-Gesellschaft im Verhältnis zu ihren Tochtergesellschaften datenschutzrechtlich so zu behandeln, wie eine externe Stelle. Ein Auftragsverarbeitungsverhältnis, bei dem die jeweilige Tochtergesellschaft als Verantwortlicher über die Zwecke und Mittel der Verarbeitung entscheidet und die Holding-Gesellschaft lediglich ausführt und daher die Daten allein im Auftrag der Tochtergesellschaft verarbeitet, scheidet hier aus. Die Holding-Gesellschaft erbringt keine, für die Auftragsverarbeitung typische datenverarbeitende Hilfsfunktion[21], wie etwa die alleinige Bereitstellung der technischen Infrastruktur oder die botenhafte Entgegennahme und weitgehend ungeprüfte Weiterleitung der eingehenden Meldungen, wie in einem Callcenter. Vielmehr übernimmt sie den vollständigen Betrieb der internen Meldestelle für die Tochtergesellschaft. Dies umfasst u. a. die Prüfung, ob der gemeldete Verstoß in den sachlichen Anwendungsbereich nach § 2 HinSchG fällt, die Prüfung der Stichhaltigkeit der eingegangenen Meldung sowie das Ergreifen angemessener Folgemaßnahmen nach § 18 HinSchG. Dies sprengt die Grenzen der Auftragsverarbeitung, da hier juristische Prüfungen vorgenommen werden müssen und Maßnahmen im eigenen Ermessen ergriffen werden.

Ist die Holding-Gesellschaft damit also grundsätzlich alleinig Verantwortlicher und die Tochtergesellschaften treffen nur dann datenschutzrechtliche Pflichten, wenn ihnen die Holding-Gesellschaft personenbezogene Daten weitergibt? Oder liegen in dieser Konstellation die Voraussetzungen für eine gemeinsame Verantwortlichkeit vor? Mangels gefestigter Rechtsprechung verbietet sich jede pauschalierte Betrachtung. Es kommt immer auf die Umstände des Einzelfalles an. Allerdings bestehen in dieser Konstellation starke Anhaltspunkte für eine gemeinsame Verantwortlichkeit zwischen der jeweils nach HinSchG originär verpflichteten Tochtergesellschaft und der Holding-Gesellschaft. Betrachtet man eine Entscheidung des AG Mannheim zum datenschutzrechtlichen Verhältnis zwischen einer Wohnungseigentümergesellschaft und ihrem Verwalter, bei der das Gericht eine gemeinsame Verantwortlichkeit angenommen hat,[22] so zeigen sich wesentliche Parallelen zur Auslagerung der internen Meldestelle auf einen Dritten. Wie bei der WEG besteht für die Einrichtung einer internen Meldestelle keine Pflicht zur Einschaltung eines Dritten. Entscheidet sich der Beschäftigungsgeber aber dazu, einen Dritten, im vorliegenden Fall die Holding-Gesellschaft, mit den Aufgaben der internen Meldestelle zu betrauen, entbindet dies den Beschäftigungsgeber gem. § 14 Abs. 1 S. 2 HinSchG nicht von der Pflicht, selbst geeignete Maßnahmen zur Abstellung eines Verstoßes zu ergreifen. Der Beschäftigungsgeber bleibt also, wie die WEG, letztendlich in der Pflicht. Gleichzeitig hat der Dritte als Betreiber der internen Meldestelle nunmehr gem. §§ 17, 18 HinSchG eigene Pflichten, denen er nachkommen muss. Insofern lässt sich bei Anwendung der durch das AG Mannheim unter Berücksichtigung der einschlägigen Rechtsprechung des EuGH[23] entwickelten Grundsätze durchaus argumentieren, dass eine gemeinsame Entscheidung über die Zwecke und Mittel der Verarbeitung vorliegt, da der Beschäftigungsgeber mit der Betrauung des Dritten mit dem Betrieb der internen Meldestelle über das „Wie" und „Warum" der Datenverarbeitung entscheidet und der Dritte sodann in der Folge über das konkrete „Wie" und „Warum" der Erhebung und Verarbeitung bestimmt. Hierbei ist weiter zu berücksichtigen, dass der EuGH bislang zu einem weiten Verständnis der gemeinsamen Verantwortlichkeit

20 *Schantz*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 6 Abs. 1 DSGVO Rn. 116.

21 AG Mannheim, 11.9.2019 – 5 C 1733/19 – WEG; siehe allgemein zu datenschutzrechtlicher Verantwortlichkeit bei Aufgabenübertragung *Spittka,* in: Taeger, Den Wandel begleiten, 2020, S. 41 ff.

22 AG Mannheim, 11.9.2019 – 5 C 1733/19 – WEG.

23 EuGH, 10.7.2018 – C-25/17; EuGH, 29.7.2019 – C-40/17.

tendiert, um einen wirksamen und umfassenden Schutz der betroffenen Personen zu gewährleisten.[24] So ist noch nicht einmal erforderlich, dass jeder der gemeinsam Verantwortlichen überhaupt Zugriff auf die verarbeiteten personenbezogenen Daten hat.[25]

Die Tochtergesellschaften sind zueinander, z. B. für den Fall, dass Sie im Rahmen einer unternehmensübergreifenden Untersuchung einer Meldung personenbezogene Daten austauschen, in der Regel jeweils allein Verantwortliche, da hier gerade nicht die durch den Auslagerungsvorgang ausgelöste gemeinsame Bestimmung über Zwecke und Mittel vorliegt. Der Austausch personenbezogener Daten zwischen Holding-Gesellschaft und jeweiliger Tochtergesellschaft kann – soweit er tatsächlich für die Erfüllung der Aufgaben der internen Meldestelle erforderlich ist – auf Art. 6 Abs. 1 UAbs. 1 lit. c DSGVO i. V. m. § 10 S. 1 HinSchG und für besondere Kategorien personenbezogener Daten auf Art. 9 Abs. 2 lit. b und g DSGVO i. V. m. § 10 S. 2 HinSchG gestützt werden. Sofern eine unternehmensübergreifende Ermittlung erforderlich ist, kann die Holding-Gesellschaft die Daten auch mit mehreren Tochtergesellschaften teilen.

Folge der gemeinsamen Verantwortlichkeit ist, dass die Holding-Gesellschaft mit der jeweiligen Tochtergesellschaft gem. Art. 26 Abs. 1 S. 2 DSGVO in einer Vereinbarung in transparenter Form festlegen muss, wer von ihnen welche Verpflichtung unter der DSGVO erfüllt, insbesondere was die Wahrnehmung der Rechte der betroffenen Person angeht, und wer welchen Informationspflichten gemäß den Art. 13, 14 DSGVO nachkommt. Hier haben die Parteien zwar einen gewissen Gestaltungsspielraum. Art. 26 Abs. 2 S. 1 DSGVO verlangt jedoch, dass die Vereinbarung die jeweiligen tatsächlichen Funktionen und Beziehungen der gemeinsam Verantwortlichen gegenüber betroffenen Personen gebührend widerspiegelt. Das Wesentliche der Vereinbarung muss den betroffenen Personen gem. Art. 26 Abs. 2 S. 2 DSGVO zur Verfügung gestellt werden. Die betroffenen Personen können aber weiter ihre Rechte im Rahmen der DSGVO gem. Art. 26 Abs. 3 DSGVO bei und gegenüber jedem einzelnen Verantwortlichen geltend machen. Die Plicht zur Einhaltung der Sicherheit der Verarbeitung nach Art. 32 DSGVO sowie zur Durchführung der DSFA trifft jeden der gemeinsam Verantwortlichen. Jedoch können und sollten diese in der Vereinbarung nach Art. 26 DSGVO die Pflichten intern der Stelle zuweisen, welche sie am besten erfüllen kann und Informations- und Unterstützungsplichten vereinbaren.

Wird das elektronische Hinweisgebersystem in technischer Hinsicht von einem externen Dienstleister bereitgestellt und kann nicht ausgeschlossen werden, dass dieser Dritte auch Zugriff auf die in dem System verarbeiteten Daten hat, liegt eine Auftragsverarbeitung nach Art. 4 Nr. 8, 28 DSGVO vor. In diesem Fall muss der gemeinsame Verantwortliche, der den externen Dienstleister beauftragt, einen Vertrag, die sog. Auftragsverarbeitungsvereinbarung (AVV), mit den Mindestinhalten des Art. 28 Abs. 3 DSGVO abschließen. Es ist nicht erforderlich, dass jeder der gemeinsam Verantwortlichen eine AVV mit dem Dienstleister abschließt. Es ist jedoch aus Gründen der Rechenschaftspflicht nach Art. 5 Abs. 2 DSGVO ratsam, dass sich alle gemeinsam Verantwortlichen mit der Beauftragung einverstanden erklären.

2. Vollständige Auslagerung der internen Meldestelle an externen Dritten

a) Sachverhalt

Der Sachverhalt stellt sich in dieser Konstellation wie unter Ziffer III.1.a. dar, jedoch mit den folgenden Abweichungen: Das elektronische Hinweisgebersystem wird nicht nur in technischer Hinsicht von einem externen Dritten bereitgestellt, sondern dieser externe Dritte (hier: eine Rechtsanwaltskanzlei) nimmt auch sämtliche Meldungen entgegen, bewertet diese und führt interne Sachverhaltsuntersuchungen durch. Er wird direkt von den einzelnen verpflichteten Beschäftigungsgebern, den Tochtergesellschaften, mandatiert, um für diese ein einheitliches internes Hinweisgebersystem einzurichten und zu betreiben. Wenn er – was regelmäßig der Fall sein dürfte – bei den internen Untersuchungen auf die Zusammenarbeit mit dem Konzern angewiesen ist, ist jedoch der Compliance-Verantwortliche der Holding-Gesellschaft sein Hauptansprechpartner. An diesen berichtet der externe Dritte auch die Ergebnisse der Bewertung der eingegangenen Meldungen. Der Compliance-Verantwortliche geht bei Bedarf auf die verantwortlichen Personen bei den Tochtergesellschaften zu, etwa wenn Verstöße abgestellt werden müssen.

b) Datenschutzrechtliche Anforderungen

Dieses Szenario entspricht datenschutzrechtlich grundsätzlich der Auslagerung der internen Meldestelle auf die Muttergesellschaft, mit dem Unterschied, dass die Dienstleistung der internen Meldestelle und die Bereitstellung der technischen Infrastruktur hier in einer Hand liegen. Auch hier ist zunächst festzuhalten, dass sich mangels gefestigter Rechtsprechung eine pauschalierte Betrachtung verbietet. Ein wesentlicher Aspekt ist die gruppeninterne organisatorische Ausgestaltung.

aa) Kein internes Business-Process-Outsourcing

Unter Anwendung der unter Ziffer III.1.b. herausgearbeiteten Grundsätze könnte bei entsprechender organisatorischer Ausgestaltung eine gemeinsame Verantwortlichkeit zwischen der jeweiligen Tochtergesellschaft, die Beschäftigungsgeber ist, und dem externen Dritten, der mit den Aufgaben der internen Meldestelle betraut wird, vorliegen. In diesem Verhältnis wäre dann die Vereinbarung zur gemeinsamen Verantwortlichkeit abzuschließen. Wichtig ist, dass die Einstufung des externen Dienstleisters als (gemeinsam) Verantwortlichen unabhängig davon erfolgt, ob die Tätigkeit eine anwaltliche oder nur eine solche zur Umsetzung der §§ 17, 18 HinSchG ist. Bereits letzte überschreitet die Grenzen der Auftragsverarbeitung, sofern nicht einfach Meldungen anhand strenger Entscheidungsbäume und weitgehend ungeprüft an den Beschäftigungsgeber weitergeleitet werden. Dies entspricht aber nicht der Idee der Tätigkeit einer externen Meldestelle i. S. d. HinSchG.

Es stellt sich sodann die Frage nach der Rolle der Holding-Gesellschaft, da diese hier häufig nur die Funktion übernimmt, der zentrale Ansprechpartner für den externen Dritten (Ombudsperson) zu sein, sei es im Rahmen der Einrichtung des Hinweisgebersystems oder bei der Durchführung von Folgemaßnahmen. Sie ist jedoch selbst kein verpflichteter Beschäftigungsgeber nach dem HinSchG und auch nicht interne Meldestelle in dem Sinne, dass bei ihr Meldungen eingehen. Daher finden die Erlaubnistatbestände des § 10 HinSchG grundsätzlich keine direkte Anwendung.

Haben die jeweiligen Tochtergesellschaften die Compliance-Funktion jedoch im Rahmen konzerninterner Abreden ordnungsgemäß auf die Holding-Gesellschaft outgesourct, kann die Übermittlung personenbezogener Daten durch den externen Dritten an die Holding-Gesell-

24 EuGH, 5.6.2018 – C-210/16; EuGH, 10.7.2018 – C-25/17; EuGH, 29.7.2019 – C-40/17.

25 EuGH, 10.7.2018 – C-25/17; EuGH, 29.7.2019 – C-40/17.

schaft wiederum auf die vorgenannten Erlaubnistatbestände gestützt werden, da es für die Erfüllung der in § 13 HinSchG aufgeführten Aufgaben durch die interne Meldestelle (dem Dritten) auch erforderlich ist, die Stelle im Konzern einzubinden, die vom Beschäftigungsgeber mit der Durchführung der Compliance-Untersuchungen beauftragt wurde. In diesem Fall dürfte das Verhältnis zwischen externem Dritten und Holding-Gesellschaft jedoch grundsätzlich das einer separaten und keiner gemeinsamen Verantwortlichkeit sein, im Verhältnis zwischen Holding-Gesellschaft und Tochtergesellschaften dürfte jedoch wieder eine gemeinsame Verantwortlichkeit vorliegen.
Fraglich ist, ob die Tatsache, dass auch die technische Infrastruktur für die Meldungen bereitgestellt wird, zusätzlich den Abschluss einer AVV mit dem externen Dritten erforderlich macht. In der vorliegenden Konstellation stellt die technische Infrastruktur lediglich das Mittel dar, mit dem der externe Dritte arbeitet und ist damit untrennbar mit der ausgelagerten Tätigkeit als interne Meldestelle verbunden. Es läge daher eine künstliche Aufsplittung eines einheitlichen Lebenssachverhalts in Auftragsverarbeitung und eigene Verantwortlichkeit, ohne dass wirklich eine Doppelfunktion vorläge. Es bleibt also bei der gemeinsamen Verantwortlichkeit zwischen Tochtergesellschaft und externem Dritten. Der Datenaustausch in diesem Verhältnis kann auf Art. 6 Abs. 1 UAbs. 1 lit. c DSGVO i. V. m. § 10 S. 1 HinSchG und ggf. Art. 9 Abs. 2 lit. b und g DSGVO i. V. m. § 10 S. 2 HinSchG gestützt werden.

bb) Internes Business-Process-Outsourcing
Weiter könnte man die vorliegende Konstellation auch so ausgestalten, dass die Holding-Gesellschaft als Dritter i. S. d. § 14 Abs. 1 S. 1 HinSchG agiert und ihrerseits den externen Dritten mit der Einrichtung und dem Betrieb des Hinweisgebersystems unterbeauftragt. In diesem Fall läge einerseits eine gemeinsame Verantwortlichkeit zwischen der jeweiligen Tochtergesellschaft und der Holding-Gesellschaft vor und davon separat eine gemeinsame Verantwortlichkeit zwischen Holding-Gesellschaft und externem Dienstleister, da hier ein Business-Process-Outsourcing (BPO) vorliegt. In dem Verhältnis Tochtergesellschaft zu externem Dienstleister muss in dieser Konstellation weder eine Auftragsverarbeitungsvereinbarung noch eine Vereinbarung gem. Art. 26 DSGVO abgeschlossen werden.

3. Teilweise Auslagerung der internen Meldestelle an externen Dritten

a) Sachverhalt
Der Sachverhalt stellt sich in dieser Konstellation wie unter Ziffer III. 2. a. dar, jedoch mit den folgenden Abweichungen: Der Hinweisgeber kann vor der Abgabe einer Meldung frei entscheiden, ob er seinen Hinweis bei dem Compliance-Verantwortlichen der Holding-Gesellschaft oder dem externen Dritten (hier: die Ombudsperson) abgeben möchte. Je nach Wahl entscheidet sich, wer für die Entgegennahme, Bewertung und Aufklärung des Hinweises zuständig ist.

b) Datenschutzrechtliche Anforderungen
In der vorliegenden Konstellation haben die Tochtergesellschaften defacto zwei Dritte mit der Aufgabe der internen Meldestelle beauftragt, einen konzerninternen und einen externen Dritten. Auch wenn § 14 Abs. 1 S. 1 HinSchG die Formulierung „ein Dritter" und damit den Singular verwendet, dürfte dem nichts entgegenstehen, soweit die Funktionsfähigkeit der internen Meldestelle nicht unterlaufen wird.

In diesem Szenario hat der externe Dritte eine wirkliche Doppelfunktion. Soweit sich der Hinweisgeber dazu entscheidet, die Meldung an die beim externen Dritten verortete Ombudsperson abzugeben, gelten die datenschutzrechtlichen Grundsätze Ziffer III. 2. b. bb. (da in diesen Konstellationen wohl regelmäßig ein internes BPO hinsichtlich der bei dem externen Dritten eingehenden Meldungen handeln dürfte). Wenn sich der Hinweisgeber jedoch entscheidet an den Compliance-Verantwortlichen der Holding-Gesellschaft zu melden, stellt der externe Dritte für diese Meldungen lediglich die technische Infrastruktur zur Verfügung und agiert als Auftragsverarbeiter für die Holding-Gesellschaft wie in Ziffer III. 1. b. Hier ist die Aufteilung in (gemeinsam) Verantwortlicher und Auftragsverarbeiter sachlich begründet.

VI. Fazit

Die Einrichtung und der Betrieb einer internen Meldestelle ist für Unternehmen nicht nur hinsichtlich der Umsetzung der Anforderungen des HinSchG eine erhebliche Herausforderung. Datenschutz und IT-Sicherheit müssen stets mitgedacht, implementiert und dokumentiert werden. Dies gilt umso mehr, wenn der Betrieb der internen Meldestelle von dem Beschäftigungsgeber auf andere Konzernunternehmen oder externe Dienstleister ausgelagert wird. Dennoch lassen sich alle Konstellationen in datenschutzkonformer Weise ausgestalten. Wichtig ist es, die datenschutzrechtlichen Beziehungen zwischen den beteiligten Stellen im jeweiligen Einzelfall korrekt einzuordnen, da hier die entscheidende Weichenstellung zur Einhaltung der DSGVO getroffen wird. Hiervon ausgehend muss ein angemessenes Risikomanagementsystem implementiert werden, das sowohl das HinSchG als auch die DSGVO berücksichtigt und alle erforderlichen Akteure einbezieht. Denn jenseits aller negativen Konsequenzen, die ein DSGVO-Verstoß mit sich bringt, wird nur ein datenschutzkonformes und sicheres Hinweisgebersystemen auf Dauer von potenziellen Whistleblowern angenommen werden.

AUTOREN

Rechtsanwalt **Dr. Marius Haak** *ist als Strafverteidiger in der Kanzlei PARK | Wirtschaftsstrafrecht. in Dortmund tätig und verantwortet dort die Dezernate Datenschutzstrafrecht und Außenwirtschaftsstrafrecht. Ferner unterstützt er Unternehmen bei der Implementierung von Hinweisgebersystemen sowie internen Untersuchungen und berät diese zu Criminal Compliance-Fragen.*

Jan Spittka *ist Rechtsanwalt und Partner bei Clyde & Co in Düsseldorf. Er leitet dort die deutsche Datenschutz- und Cybersecurity-Praxis und vertritt Unternehmen regelmäßig gegenüber Datenschutzbehörden und in Gerichtsverfahren.*