HINWEISGEBER-RICHTLINIE

Inhaltsübersicht:

	Randnummer
1. Zweck der Hinweisgeber-Richtlinie	1-4
2. Gegenstand der Meldung	5
3. Meldeverfahren	6-12
3.1 Offene und direkte Meldung	6,7
3.2 Begründeter Verdacht	8,9
3.3 Konkret und schlüssig	10,11
3.4 Externe Meldungen	12
4. Missbrauch des Hinweisgebersystems	13-15
5. Verfahrensablauf nach Meldung	16-30
5.1 Grundsätze zum Umgang mit Verdachtsfällen	16-27
5.2 Mitwirkung bei der Sachverhaltsaufklärung	28-30
6. Schutz des Hinweisgebers und der bei der Aufklärung mitwirkenden Personen	31-37
6.1 Vertraulichkeit und Verschwiegenheit	31-33
6.2 Schutz vor Repressalien	34-37
7. Berichterstattung über Verdachtsfälle	38
8. Datenschutzrechtliche Hinweise	39-46

1. Zweck der Hinweisgeber-Richtlinie

Unsere **Allgemeine Verhaltensrichtlinie** ist ein zentraler Baustein der Unternehmensführung, in dem bedeutsame Regeln unserer Wertekultur festgelegt sind, die von allen Mitarbeitenden gemeinsam getragen und konsequent gelebt werden – besonders auch von unseren Führungskräften. Sie umfassen weit mehr als nur die Einhaltung von Recht und Gesetz, es ist für uns eine Frage der Haltung. Das betrifft uns alle bei LSV LECH-STAHL VEREDELUNG GMBH. 1

Es ist daher für uns alle ein Thema, dass es weiterhin auch so bleibt. Seriöse Hinweise helfen uns, Verstößen gegen Verhaltensanforderungen frühzeitig entgegenzuwirken und Schäden für unser Unternehmen, unsere Mitarbeiter und Mitarbeiterinnen sowie unsere Geschäftspartner zu vermeiden oder zumindest zu reduzieren. **Ergänzend** zu unseren regulären Informations- und Meldekanälen, wie beispielsweise Linienmanagement, Qualitätskontrollpersonal, Arbeitnehmervertretung, insbesondere Betriebsrat, bieten wir daher **die in dieser Hinweisgeber-Richtlinie beschriebene Möglichkeit einer Kontaktaufnahme**, um – auf Wunsch auch anonym – Verstöße gegen relevante gesetzliche Bestimmungen und sonstige Vorschriften zu melden. Unser Hinweisgeber-System dient zugleich zur Umsetzung des Gesetzes für einen besseren Schutz hinweisgebender Personen (Hinweisgeber-Schutzgesetz). 2

Primärer Ansprechpartner sollte dabei immer der Vorgesetzte[1] sein. Wenn – aus welchen Gründen auch immer – eine Meldung an den Vorgesetzten nicht möglich sein sollte, z.B. weil der Linienvorgesetzte/die Linienabteilung der Verursacher des anzusprechenden Problems ist, das anzusprechende Problem keine angemessene Aufmerksamkeit erhalten würde oder die eine Meldung beabsichtigende Person sich 3

[1]Ausschließlich aus Gründen der besseren Lesbarkeit wird auf die Verwendung der männlichen und weiblichen Form verzichtet.

dabei vielleicht so unsicher fühlt, so dass sie die Verwendung eines anderen vertraulichen Meldewegs wählen möchte, so ist frühzeitig **Kontakt mit dem Compliance Officer** aufzunehmen. Der Compliance Officer ist zugleich die **Interne Meldestelle** im Sinn des Hinweisgeber-Schutzgesetzes.

Dr. Lutz Steffen
Max Aicher GmbH & Co. KG
Teisenbergstraße 7
D-83395 Freilassing
E-Mail: l.steffen-HWS@max-aicher.de
Telefon: +49 8654 491 113
Mobile: +49 171 77 46 042

Der Compliance Officer ist **als Rechtsanwalt zur Vertraulichkeit verpflichtet** unter Berücksichtigung der Maßgaben dieser Richtlinie und prüft als unabhängige Instanz die eingehenden Meldungen. 4

2. Gegenstand der Meldung

Die Meldung von regelwidrigem Verhalten („Verstößen“) oder von einem Verdacht auf ein solches Fehlverhalten („Verdachtsfall“) gemäß dieser Richtlinie hat sich grundsätzlich auf Verhaltensweisen zu beschränken, die gegebenenfalls einen sich gegen das Unternehmensinteresse richtenden **Straftatbestand** erfüllen bzw. ein **schweres Vergehen** darstellen. Dies gilt insbesondere für folgende Delikte: 5

- Betrug,
- betrügerisches Fehlverhalten in Bezug auf die Rechnungslegung bzw. interne Rechnungslegungskontrollen,
- Korruption, Bestechung,
- Verbot der Geldwäsche,
- Verstöße gegen das Kartellrecht oder gegen das sonstige Wettbewerbsrecht,
- Offenlegung vertraulicher/firmeneigener Informationen gegenüber unbefugten Dritten („Geheimnisverrat“),
- Nutzung vertraulicher Informationen, von denen im Laufe der Arbeit Kenntnis erlangt wurde, zum persönlichen Vorteil („Insidergeschäfte“),
- Fälschung von Verträgen, Berichten oder Unternehmensdaten/-aufzeichnungen,
- Missbrauch von Unternehmensgütern, Diebstahl oder Veruntreuung,
- Umweltgefährdungen, Gemeingefahren, Gefahren für die Gesundheit bzw. Sicherheit unserer Belegschaft und ähnliche Fälle,
- Drogen- oder Alkoholmissbrauch sowie Diskriminierung oder sexuelle Belästigung am Arbeitsplatz,
- Verletzung sonstiger geltender Gesetze und Vorschriften, wodurch die Gesellschaft Strafen, Bußgeldern oder möglichem Regress ausgesetzt wird.

Sonstige Kategorien von Verstößen, die Gegenstand einer Meldung sein können, ergeben sich aus § 2 Hinweisgeber-Schutzgesetz.

3. Meldeverfahren

3.1 Offene und direkte Meldung

Alle Hinweisgeber[1] werden ermutigt, ihnen bekannte Missstände, Fehlverhalten, Gefährdungen etc. im Sinne dieser Richtlinie offen und direkt unter **Angabe ihrer erforderlichen Kontaktdaten** zu melden. 6

Wenn Sie Hinweise geben, sollte dies unter Bekanntgabe Ihrer Identität erfolgen. Interne Risikokommunikation sollte nicht anonym erfolgen, da dann keine Rückfragen möglich sind und das Vertrauen beeinträchtigt werden kann. Vor diesem Hintergrund sind **anonyme Hinweise** zwar grundsätzlich nicht erwünscht, werden jedoch ebenfalls zur Kenntnis genommen und untersucht. Sollten Hinweisgeber – aus welchen Gründen auch immer – überhaupt keinen Direktkontakt (z.B. über Telefon) wünschen, kann die Meldung auch anonymisiert über den dafür extra auf der Homepage eingerichteten Zugang erfolgen. 7

3.2 Begründeter Verdacht

Der Hinweisgeber sollte nur solche Fälle melden, bei denen er einen begründeten **Verdacht**, also einen die Möglichkeit wahrscheinlich machenden Anhaltspunkt hat, dass ein nach dieser Richtlinie relevanter Vorfall vorliegt. Er sollte sich bei seinen Meldungen immer auf die Richtlinie beziehen. 8

Nicht in allen Fällen wird für den Hinweisgeber klar erkennbar sein, ob eine bestimmte Handlung oder ein bestimmtes Verhalten entsprechend den Grundsätzen dieser Richtlinie gemeldet werden sollte. Der Hinweisgeber sollte dies vor seiner Meldung sorgfältig prüfen. Gleichwohl ist es vorzugswürdig, Verdachtsfälle gutgläubig zu melden, anstatt sie zu verschweigen. **Im Zweifelsfall** empfehlen wir, zunächst mit einem der in Ziffer 1 genannten Ansprechpartner den Fall abzustimmen, ohne dass der Name des Verdächtigen benannt wird. 9

3.3 Konkret und schlüssig

Jeder Hinweis sollte so konkret wie möglich erfolgen. Der Hinweisgeber sollte dem Empfänger **möglichst detaillierte Informationen** über den zu meldenden Sachverhalt vorlegen, so dass dieser die Angelegenheit richtig einschätzen kann. In diesem Zusammenhang sollten die Hintergründe, der Tathergang und der Grund der Meldung sowie Namen, Daten, Orte und sonstige Informationen benannt werden. Sofern vorhanden, sollten Dokumente vorgelegt werden. Persönliche Erfahrungen, mögliche Vorurteile oder subjektive Auffassungen sollten als solche kenntlich gemacht werden. 10

Allein aufgrund dieser Richtlinie besteht **keine Verpflichtung** des Hinweisgebers zu eigenen Ermittlungen. 11

3.4 Meldungen von außerhalb des Unternehmens

Sofern Meldungen bei dem Unternehmen eingehen von außerhalb stehenden Personen, z.B. Kunden, Lieferanten, kann dies erhebliche Auswirkungen auf den betrieblichen Ablauf haben. Sie sind daher **sorgfältig zu prüfen**. 12

4. Missbrauch des Hinweisgebersystems

Bitte berücksichtigen Sie, dass Verdächtigungen und Anschuldigungen gegen eine Person für diese schwerwiegende Konsequenzen nach sich ziehen können. Wir halten Sie daher dazu an, das **Hinweisgeber-System verantwortungsvoll zu nutzen**. Eine Meldung sollte in gutem Glauben erfolgen. Ergibt die Überprüfung des Hinweises, dass bspw. kein begründeter Verdacht besteht oder die Fakten 13

nicht ausreichen, um einen Verdacht zu erhärten, haben Hinweisgeber, die einen Hinweis gutgläubig melden, keine disziplinarischen Maßnahmen zu befürchten.

Anderes gilt für Hinweisgeber, die das Hinweisgebersystem bewusst für falsche Meldungen missbrauchen; diese müssen mit disziplinarischen Maßnahmen rechnen. Auch eine Beeinträchtigung des Hinweisgebersystems durch bspw. Manipulation, Vertuschung oder der Bruch von Absprachen betreffend die Vertraulichkeit können **disziplinarische Maßnahmen** nach sich ziehen. Als Maßnahmen kommen bspw. Abmahnungen oder Kündigungen in Betracht. Daneben kann dies zivilrechtliche oder strafrechtliche Folgen nach sich ziehen. 14

Gutgläubig sind Hinweise, wenn der Hinweisgeber einen vernünftigen Grund zur Annahme hat, dass die von ihm zu meldenden Tatsachen korrekt sind, seinem eignen Kenntnisstand nicht widersprechen und nach seiner auf dieser Grundlage gebildeten Überzeugung einen Umstand darstellen, der unmittelbar oder mittelbar zu einem Schaden oder anderweitigen Nachteil für das Unternehmen, die Unternehmensgruppe, die Belegschaft, Geschäftspartner etc. führen kann. 15

5. Verfahrensablauf nach Meldung

5.1 Grundsätze zum Umgang mit Verdachtsfällen

Jede Meldung wird vertraulich und unter Berücksichtigung der geltenden Datenschutzgesetze behandelt. Hinweise werden nur zum **Zwecke** der Ermittlung und etwaigen Ahndung von Verstößen verwendet. Nach dem Eingang einer Meldung erfolgt durch die Stelle, die die Meldung entgegennimmt, eine erste Überprüfung der Hinweise, insbesondere, ob Beweise vorliegen, die die übermittelten Informationen bekräftigen oder widerlegen. 16

Ist die **entgegennehmende Stelle** der Auffassung, dass weitere Ermittlungen erfolgen sollten, dokumentiert sie dies und leitet die Informationen an die im Unternehmen zuständige Stelle weiter. Diese führt im Anschluss die internen Ermittlungen durch. 17

Hat der **Compliance Officer** (s. bei Rn. 3) die Meldung entgegengenommen, prüft und dokumentiert er, ob die vorgetragenen Bedenken hinreichend fundiert sind, um eine Untersuchung einzuleiten. Hierbei sind insbesondere auch die Ergebnisse einer vorangegangenen Konsultation zu berücksichtigen. Im Zweifel ist davon auszugehen, dass eine Untersuchung angezeigt ist. 18

Der Compliance Officer **bestätigt dem Hinweisgeber**, sofern dessen Meldung nicht anonym erfolgt ist, innerhalb von sieben Kalendertagen den Eingang seiner Meldung, **teilt ihm** das weitere Vorgehen **mit** und **unterrichtet den Hinweisgeber** spätestens drei Monate nach der Eingangsmeldung über den Stand der Angelegenheit. 19

Die Schwere und die Folgen eines möglichen Verstoßes sowie eine mögliche Gefahr im Verzug geben den Rahmen für zu ergreifende Maßnahmen vor. Sachlich fundierte Hinweise leitet der Compliance Officer in der Regel an die zuständige Geschäftsführung weiter zur Veranlassung der gegebenenfalls erforderlichen weiteren Sachverhaltsaufklärung und Entscheidung über das angemessene Vorgehen einschließlich der Information einzuschaltender Personen und etwaiger Eilmaßnahmen. Der Compliance Officer wird den **Namen des Hinweisgebers** nur dann dem Unternehmen mitteilen, wenn dieser seine vorherige Freigabe erteilt hat. 20

Auch wenn der Compliance Officer mit Zustimmung des Hinweisgebers und unter Entbindung von der anwaltlichen Verschwiegenheitspflicht **anonymisierte Berichte** an das Unternehmen verfasst, achtet er darauf, dass der in Rede stehende Sachverhalt nicht so strukturiert ist, dass allein seine Mitteilung Rückschlüsse auf den Hinweisgeber zulässt. Soweit dies aufgrund einer detailreichen Schilderung zu befürchten ist - diese Frage sollte mit dem Hinweisgeber ausdrücklich erörtert werden - muss dieser auf das **Risiko einer Enttarnung** hingewiesen werden. Ihm muss auch klar sein, welches Restrisiko er je nach Sachverhalt und der Kenntnis anderer dazu eingeht. Ggf. können Details eines Sachverhalts im Bericht an das Unternehmen weggelassen werden, wenn (nur) dadurch der Schutz der Identität gewährleistet werden kann. 21

Für die nach allgemeinen Grundsätzen durchzuführende Untersuchung ist die **Angemessenheit der Mittel** zu wahren. Diese allgemeinen Untersuchungsgrundsätze beinhalten insbesondere: Ist die **Hinzuziehung von Personalkräften** erforderlich, sind diese einzugrenzen auf solche, die nachprüfbar zuständig, fachlich befähigt, zuverlässig und formal zugelassen sind sowie keine Interessenskonflikte bei der Ausübung aufweisen; sie sind zur Verschwiegenheit, insbesondere auf das Datengeheimnis verpflichtet. **Prüfschritte** und gegebenenfalls **Interviews** sind zu dokumentieren. Zur Dokumentation der ermittelten Informationen werden **nur die erforderlichen Daten erhoben und verarbeitet**. Bei zielgerichteten Ermittlungen ist stets **abzuwägen** zwischen den Interessen des Unternehmens, den Chancen und Risiken der Aufdeckung möglicher Verdachtsfälle und den denkbaren Folgen eines unberechtigten Verdachts. Zweckspezifische **Pseudonyme** werden eingesetzt, wo die Verarbeitung von personenbezogenen Daten zur Erreichung des jeweiligen Untersuchungsziels nicht unbedingt erforderlich ist. Untersuchungen berücksichtigen immer auch mögliche **entlastende Tatsachen**. Belastete Personen erhalten durch **Anhörung** zum gegebenen Zeitpunkt Gelegenheit zu den Vorwürfen Stellung zu nehmen. Die Einhaltung der Festlegung zur Nutzung zugelassener Ressourcen, insbesondere **Kommunikationskanäle**, wird kontrolliert. 22

Über die **abschließende Beurteilung** des Sachverhalts und die im Einzelfall zu treffenden Maßnahmen entscheiden die nach dem ggf. Eskalationsprozess zuständigen Stellen. Die gesetzlichen Rechte des Betriebsrats bleiben unberührt. 23

Der Vorgang unter Einschluss des Ergebnisses der Untersuchung und der getroffenen Entscheidung wird **dokumentiert**. Dabei kann auf andere Unterlagen Bezug genommen werden. 24

Die Geschäftsführung informiert den Compliance Officer über das **Ergebnis der Untersuchung**. 25

Der **Compliance Officer informiert den Hinweisgeber** zeitnah über eine Einstellung des Verfahrens wegen nicht ausreichender Fundierung oder über das Ergebnis der Untersuchung. 26

Nicht mehr benötigte **personenbezogene Daten** werden in der Regel innerhalb von zwei Monaten nach Abschluss der Ermittlungen **gelöscht**. Sind diese Bestandteil einer Dokumentation gemäß § 11 Hinweisgeber-Schutzgesetz, werden sie zusammen mit der Dokumentation in der Regel drei Jahre nach Abschluss des Verfahrens gelöscht. 27

5.2 Mitwirkung bei der Sachverhaltsaufklärung

Bei jeder **Weitergabe von Informationen** ist zu prüfen, ob die Offenlegung der Information zur Aufklärung unerlässlich ist. 28

Alle **Mitarbeiter und Mitarbeiterinnen** sind angehalten, bei der Sachverhaltsaufklärung mit der zuständigen Stelle kooperativ zusammenzuarbeiten. Dies umfasst insbesondere die Vorlage von vollständigen Geschäftsunterlagen sowie die Erteilung von Auskünften zu geschäftlichen Vorgängen. Über ihre Mitwirkung sind sie zur **Vertraulichkeit** verpflichtet. 29

Wer eine Untersuchung durch die Vernichtung oder Beschädigung von betrieblichen Unterlagen oder anderen möglichen **Beweismitteln** beeinträchtigt, oder wer versucht, mögliche **Zeugen** zu beeinflussen, begeht eine schwerwiegende Pflichtverletzung (z.B. Unterdrückung beweiserheblicher Daten, Versuch der Anstiftung zur Falschaussage). 30

6. Schutz des Hinweisgebers und der bei der Aufklärung mitwirkenden Personen

6.1 Vertraulichkeit und Verschwiegenheit

Der Schutz eines Hinweisgebers wird durch die **vertrauliche Behandlung seiner Identität** gewährleistet. Sofern er seine Kontaktdaten mitteilt, werden diese unter Berücksichtigung der datenschutzrechtlichen Vorgaben und darüber hinaus beim Compliance Officer als Rechtsanwalt nach Maßgabe der berufsrechtlichen Verschwiegenheitspflicht gespeichert und genutzt. 31

Grundsätzlich wird sein Name nicht bekannt gegeben; Abweichendes kann gelten, wenn der Hinweisgeber die Offenlegung seiner Identität gestattet oder eine entsprechende Rechtspflicht, z.B. möglicherweise gegenüber ermittelnden Behörden oder in einem sich eventuell anschließenden Gerichtsverfahren, besteht. Dies kann insbesondere dann gelten, wenn die Offenlegung unerlässlich ist, damit die von der Meldung betroffenen Personen ihr Recht auf Anhörung wahrnehmen können. Eine solche der vertraulichen Behandlung entgegenstehende Rechtspflicht zur Offenlegung ist allerdings äußerst unwahrscheinlich, falls der Hinweisgeber seine Identität gegenüber dem Compliance Officer als Rechtsanwalt offenbart hat. **Der Hinweisgeber wird in jedem Fall vorab von der Offenlegung seiner Identität unterrichtet**. Bis zu einer solchen Offenlegung der Identität des Hinweisgebers hat der Hinweisgeber das Recht, seine in der bewussten Preisgabe seiner Identität gegenüber der entgegennehmenden Stelle zu sehende Einwilligung in die Verarbeitung seiner personenbezogenen Daten durch diese verantwortliche Stelle jederzeit zu widerrufen. Die **Einwilligung des Hinweisgebers** in die Offenlegung durch Übermittlung seiner Identität durch die verantwortliche Stelle ist nachzuweisen (Art. 7 DSGVO[2]). 32

Gleiches gilt für **Personen, die an der Aufklärung des Verdachts mitgewirkt haben**. 33

6.2 Schutz vor Repressalien

LSV LECH-STAHL VEREDELUNG GMBH schützt die Interessen der Hinweisgeber. Jede Person, die **in gutem Glauben** ein Anliegen in Verbindung mit Fehlverhalten am Arbeitsplatz vorbringt oder an der Aufklärung eines entsprechenden Verdachts mitwirkt, muss nicht aufgrund der Meldung bzw. der Mitwirkung mit negativen Konsequenzen rechnen (z.B. Abstufung oder Entlassung). Abweichendes kann gelten, wenn die Person in den aufzuklärenden Vorfall verwickelt ist; zeigt sich jedoch die betreffende Person selbst an, so wird dies bei möglichen Personalmaßnahmen zu Gunsten des Betroffenen berücksichtigt. 34

[2]Datenschutz-Grundverordnung.

Sollte ein Hinweisgeber oder jemand, der an der Aufklärung eines Verdachts mitwirkt, der Auffassung sein, dass er deshalb benachteiligt, diskriminiert, belästigt oder ähnliches wurde, hat er dies seinem jeweiligen **Vorgesetzten mitzuteilen**. 35

Alternativ kann ein solcher Vorfall entsprechend Ziffer 1 über die dort vorgesehenen Meldewege mitgeteilt werden. Jegliche Benachteiligung, Diskriminierung, Belästigung oder ähnliches des Hinweisgebers oder einer mitwirkenden Person wird seitens des Unternehmens nicht geduldet. Das Unternehmen prüft die Umstände des jeweiligen Falles und kann vorübergehende oder dauerhafte Maßnahmen ergreifen, um den Hinweisgeber bzw. die mitwirkende Person zu schützen und die Interessen des Unternehmens zu wahren. Das Unternehmen informiert die Betroffenen schriftlich über das Ergebnis der jeweiligen Untersuchung. 36

Jeder Mitarbeiter oder Vorgesetzte, der einen Hinweisgeber oder eine Person, die an der Aufklärung eines entsprechenden Verdachts mitwirkt, aufgrund der Meldung oder der Mitwirkung entlässt, herabstuft, belästigt oder diskriminiert oder ähnliches, muss mit **disziplinarischen Maßnahmen** rechnen, die im äußersten Fall zu seiner Entlassung führen können. 37

7. Berichterstattung über Verdachtsfälle

Der Compliance Officer erstattet halbjährlich einen **Tätigkeitsbericht**. In diesen sind aufzunehmen: 38

- die im Berichtszeitraum von ihm neu erfassten Fälle mit kurzer Angabe zur Art des Vorwurfs,
- die Erledigung von Fällen mit kurzer Angabe zur Art der Erledigung sowie
- nicht erledigte Fälle aus den Vorperioden mit kurzer Angabe zum Stand der Ermittlungen.

Empfänger des Berichts ist die Geschäftsführung.

8. Datenschutzrechtliche Hinweise

Mit der Meldung von Verstößen gegen Verhaltenspflichten geht die **Verarbeitung von personenbezogenen Daten** einher. Betroffene Personengruppen sind vor allem die Hinweisgeber sowie die belasteten Personen. Die Datenerhebung umfasst Angaben über die belastete Person, die (angeblichen) Verhaltensverstöße sowie die entsprechenden Sachverhalte. Bezüglich des Hinweisgebers kommen der Name der meldenden Person, ihre Position im Unternehmen, ihre Kontaktdaten, insbesondere Telefonnummer, unter der sie bei eventuellen Rückfragen erreicht werden will, und gegebenenfalls auch die Umstände ihrer Beobachtung in Betracht. 39

Die Verarbeitung der personenbezogenen Daten stützt sich vornehmlich auf die Erforderlichkeit zur Wahrung der berechtigten Interessen des Unternehmens als **Ermächtigungsgrundlage** (Art. 6 Abs. 1 lit. f DSGVO). 40

Die Verarbeitung von personenbezogenen Daten, die mit der **Aufdeckung von Verstößen der in Abschnitt Ziffer 2 beschriebenen Kategorien** in Zusammenhang stehen, wird als zulässig angesehen[3]; die gebotene Interessenabwägung fällt zugunsten des berechtigten Interesses des Unternehmens aus, da die Meldung solcher Verstöße rechtliche Konsequenzen durch beispielsweise Strafverfolgung, Schadensersatzforderungen und Imageschaden vermeiden hilft. 41

[3]DSK, Orientierungshilfe der Datenschutzaufsichtsbehörden zu Whistleblowing-Hotlines, Stand: 14.11.2018, Abschnitt D 3.2.

Die Pflicht zur **Information der belasteten Person**, insbesondere von der Speicherung, der Art der Daten, der Zweckbestimmung der Verarbeitung und der Identität des Verantwortlichen und gegebenenfalls des Hinweisgebers (Art. 14 Abs. 1, 2 DSGVO), besteht so lange nicht, wie 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 (Art. 14 Abs. 5 lit. b DSGVO). Eine dauerhafte Geheimhaltung dürfte aber ausgeschlossen sein. Folglich muss die Information - auch hinsichtlich der Identität des Hinweisgebers - dann nachgeholt werden, sobald der Grund für den Aufschub entfallen ist. Ohne eine solche Berechtigung zum Aufschub müsste die Information innerhalb eines Monats nach Erlangung der personenbezogenen Daten gegeben werden (Art. 14 Abs. 3 lit. a DSGVO). 42

Eine wirksamere Einschränkung der Informationspflicht besteht, wenn personenbezogene Daten gemäß dem Recht der Mitgliedstaaten dem **Berufsgeheimnis** unterliegen und daher vertraulich behandelt werden müssen (Art. 14 Abs. 5 lit. d DSGVO). Bei unmittelbarer Meldung an den Compliance Officer, der ein Rechtsanwalt ist, unterliegt die Identität des Hinweisgebers der berufsrechtlichen Verschwiegenheitspflicht[4]. 43

Eine Pflicht zur Information besteht ferner nicht, soweit durch ihre Erfüllung Informationen offenbart würden, die wegen der **überwiegenden berechtigten Interessen** eines Dritten, also **des Hinweisgebers**, geheim gehalten werden müssen (§ 29 Abs. 1 Satz 1 BDSG[5]). 44

Spiegelbildlich dazu besteht der **Auskunftsanspruch der belasteten Person** nicht, soweit durch die Auskunft Informationen offenbart würden, die nach einer Rechtsvorschrift oder ihrem Wesen nach, insbesondere wegen der überwiegenden berechtigten Interessen eines Dritten, geheim gehalten werden müssen (§ 29 Abs. 1 Satz 2 BDSG). 45

Das Recht auf bzw. die Pflicht zur **Löschung personenbezogener Daten** nach Zweckerfüllung (Art. 17 Abs. 1 lit. a DSGVO) gilt nicht für den Compliance Officer an Rechtsanwalt, weil die gesetzlichen Aufbewahrungspflichten eines Anwalts vorgehen (Art. 17 Abs. 3 lit. b DSGVO). 46

[4]Buchert, Ombudsmann und Hinweisgebersysteme, Rn. 35, 38ff. in: Hauschka ua., Corporate Compliance, 3. Aufl. 2016.
[5]Bundesdatenschutzgesetz.