

## EU-Whistleblower-Richtlinie: Handlungsbedarf für Unternehmen

Mit der Umsetzung der EU-Whistleblowing-Richtlinie<sup>1</sup> (WBRL) in nationales Recht werden Unternehmen ab 50 Mitarbeitenden verpflichtet, interne Meldekanäle einzurichten. Zu den Verpflichteten der EU-Whistleblowing-Richtlinie gehören sowohl Akteure des privaten Sektors wie auch Unternehmen der öffentlichen Hand. Hinweisgebenden soll auf diese Weise die Weitergabe von Informationen zu Gesetzesverstößen im Unternehmen ermöglicht und erleichtert werden. Der Anwendungsbereich der WBRL bezieht sich auf Verstöße gegen (ausgewählte) EU-rechtliche Vorschriften. Es ist allerdings zu erwarten, dass die Umsetzung der WBRL in deutsches Recht so erfolgen wird, dass Gegenstand von Meldungen neben allen Verstößen gegen Straftatbestände oder Ordnungswidrigkeiten auch die Nichteinhaltung weiterer ausgewählter Rechtsvorschriften wie etwa solche zur Bekämpfung von Terrorismusfinanzierung, zur Vergabe von öffentlichen Aufträgen und zum Schutz personenbezogener Daten sein werden. Ein erster Entwurf eines Hinweisgeberschutzgesetzes (HinwGebSchG-E) aus dem Jahr 2021, der noch unter der vorherigen Bundesregierung entstand, aber nicht in die parlamentarischen Beratungen gelangte, legt dies nahe.



<sup>1</sup> Richtlinie (EU) 2019/1937 des Europäischen Parlaments und des Rates vom 23. Oktober 2019 zum Schutz von Personen, die Verstöße gegen das Unionsrecht melden.

Dass sich die Einrichtung von Hinweisgebersystemen lohnt, zeigt eine Studie<sup>2</sup> der Fachhochschule Graubünden FHGR und der EQS Group: Im Rahmen der Studie wurde ermittelt, dass bei 30,5 % der befragten Unternehmen in Deutschland im Jahr 2021 ein Gesamtschaden von über EUR 100.000 durch Missstände entstanden sei<sup>3</sup>. Hinweisgebersysteme können solche Missstände im Keim ersticken und den Eintritt von finanziellen Schäden und Reputationsverlust vermeiden.

## Verfahren für interne Meldungen

Nach den Vorgaben der WBRL sollen neben Mitarbeitenden auch Gesellschafter, Lieferanten, Kunden und bestimmte Geschäftspartner Verstöße über unternehmensinterne Kanäle melden können.

Ferner können die Meldekanäle von einer hierfür benannten internen Person oder Abteilung betrieben oder extern von einem Dritten, bspw. einer Ombudsperson, einem externen kommerziellen Anbieter von Meldeplattformen, Gewerkschafts- oder Arbeitnehmervertreter, bereitgestellt werden.

Die Ausgestaltung der Kanäle muss gewährleisten, dass die Vertraulichkeit der Identität des Hinweisgebenden gewahrt wird, der Eingang der Meldung dem Hinweisgebenden innerhalb von sieben Tagen bestätigt wird, eine unparteiische Person oder Abteilung für die Folgemaßnahmen zu den Meldungen zuständig ist, die benannte Person/Abteilung ordnungsgemäße Folgemaßnahmen ergreift, der Hinweisgebende innerhalb einer Frist von drei Monaten ab Bestätigung des Eingangs bzw. nach Ablauf der Frist der Bestätigung eine Rückmeldung erhält, und klare und leicht zugängliche Informationen über die Verfahren für externe Meldungen erteilt werden.

## Ressourcennutzung in Unternehmensgruppen

Bei Konzernstrukturen reicht eine ausschließliche Einrichtung der Hinweisgeberstelle auf Ebene einer Konzernobergesellschaft nicht aus. Grundsätzlich muss jede verpflichtete juristische Person ihren eigenen Meldekanal aufweisen.

<sup>2</sup> Whistleblowing-Report 2021 der Fachhochschule Graubünden (FHGR) in Kooperation mit der EQS Group, Februar 2022.

<sup>3</sup> Unter Gesamtschaden werden „alle finanziellen Aufwendungen verstanden, die bei den untersuchten Unternehmen als Folge von Missständen sowie durch deren Aufdeckung und Bearbeitung im Jahr 2020 verursacht wurden, wobei neben materiellen auch immaterielle Konsequenzen vollumfänglich dazuzählen“, vgl. Whistleblowing-Report 2021 der Fachhochschule Graubünden (FHGR) in Kooperation mit der EQS Group, Februar 2022, S. 18.

Ausnahmen gelten jedoch für private Unternehmen mit 50 bis 249 Arbeitnehmenden; diese können für die Entgegennahme von Meldungen und für möglicherweise durchzuführende Untersuchungen unbeschadet einer Konzernzugehörigkeit Ressourcen teilen. Zusätzlich sieht die WBRL vor, dass sich die Unternehmen auch eines Dritten bedienen dürfen, um die Meldungen entgegenzunehmen. In der Praxis wird deshalb nach Lösungen gesucht, wie trotz der restriktiven Vorgaben der WBRL – die die EU-Kommission in zwei Stellungnahmen zur Jahresmitte 2021 nochmals ausdrücklich bestätigt hat – eine Meldestellenressource durch mehrere rechtliche Einheiten genutzt werden kann. Ein wichtiges Element für eine Mehrfachnutzung von Ressourcen ist die Bereitstellung einer Landing Page für den Hinweisgebenden, die eine Auswahl (z. B. per Button) desjenigen Unternehmens ermöglicht, zu dem eine Meldung abgegeben werden soll.

Zukünftig kann sich zudem bei kleineren Unternehmen – auch unter dem Gesichtspunkt effektiver Ressourcennutzung – die Frage stellen, ob das Hinweisgebersystem zugleich auch als Meldestelle nach dem Lieferkettensorgfaltspflichtengesetz (LkSG) genutzt werden kann. Die gesetzlichen Regelungen (WBRL und LkSG) stehen dem nicht entgegen. Allerdings unterscheiden sich die beiden Meldewege hinsichtlich des Kreises verpflichteter Unternehmen (Mitarbeiteranzahl), möglicher Hinweisgebender und der melderelevanten Themen. Man muss also im Einzelfall sehen, ob eine Zusammenfassung der Meldewege in einer Stelle praktikabel ist. Es wird jedenfalls – wegen der unterschiedlichen Größenanforderungen – deutlich mehr Hinweisgebersysteme als Meldestellen nach LkSG geben.

## Auswahl von Meldestellenadministratoren

Für die Entgegennahme von Meldungen kommen grundsätzlich alle in Betracht. Die WBRL spricht von „unparteiischen Personen oder Abteilungen“, die zu benennen sind. Das HinwGebSchG-E nennt zudem als Voraussetzung, dass die verantwortlichen Personen ihre Tätigkeit „unabhängig“ ausüben. In der Regel werden die Compliance-Beauftragten geeignete Meldestellenadministratoren sein, aber auch an die Datenschutzbeauftragten oder andere Sonderbeauftragte im Unternehmen ist zu denken. Daneben qualifizieren sich auch die in den Bereichen Recht oder Interne Revision tätigen Personen.

## IT-Produkte zum Betrieb einer Meldestelle

Auf dem Markt finden sich zahlreiche Anbieter für digitale Produkte zum Betrieb eines Meldesystems. Diese unterscheiden sich unter anderem hinsichtlich der Kundenzielgruppen (Mittelstandsprodukte, Produkte für Großunternehmen mit vielen tausend Mitarbeitenden oder am anderen Ende auch kleine, einfache Lösungen für kleinere Unternehmen), den Funktionalitäten (Eingabemöglichkeit von Text, Hochladen von Anhängen auf der Landing Page, Voice Recording), der Bedienbarkeit (Anpassung von Back- und Frontend, Zusatzfunktionen im Bereich der Kommunikation mit dem Hinweisgebenden, Konfigurationsmöglichkeiten und anderes) und nicht zuletzt auch in der Preisgestaltung. Sinnvoll ist es, bei der Auswahl eines Produkts an die datenschutzrechtlichen Anforderungen (dazu sogleich) zu denken und den Datenschutzbeauftragten des Unternehmens und die für die Meldestelle verantwortlichen Personen – wenn diese bereits feststehen – in den Auswahlprozess einzubeziehen.

## Mitbestimmung des Betriebsrats

Bei der Einrichtung von Hinweisgebersystemen sollten die Betriebsräte frühzeitig einbezogen werden. Der Betrieb eines Hinweisgebersystems mittels einer IT-gestützten Lösung dürfte (siehe oben) die Regel sein. In diesem Fall kommt in Betracht, dass es sich um eine mitbestimmungspflichtige Maßnahme nach § 87 Abs. 1 Nr. 6 BetrVG handelt. Daneben kann das Mitbestimmungsrecht nach § 87 Abs. 1 Nr. 1 BetrVG zum sog. „Ordnungsverhalten“ zu beachten sein, wenn der Arbeitgeber ein Hinweisgebersystem verpflichtend im Unternehmen einführen möchte.

Zu erwägen ist als eine mögliche Gestaltung, in einer Richtlinie/Policy mitbestimmungsfreie Inhalte zum Hinweisgebersystem zusammenzufassen, z. B. die Darstellung der Unternehmensphilosophie und der Gesetzeslage, und daneben alle mitbestimmungspflichtigen Elemente in einer Betriebsvereinbarung zu regeln. Kernelemente einer solchen Betriebsvereinbarung sind dann etwa der Ablauf einer Meldung, die zuständigen Ansprechpersonen und die Grundzüge der weiteren Bearbeitung von Hinweisen.

## Datenschutzkonforme Ausgestaltung

Die Einrichtung eines Meldesystems hat datenschutzkonform, also in Übereinstimmung mit der Datenschutz-Grundverordnung (DSGVO) zu erfolgen. Dies erfordert u. a. eine frühestmögliche Einbindung des Datenschutzbeauftragten.

## Unternehmen als Verantwortliche i.S.d. DSGVO

Die Unternehmen handeln bei der Einführung und dem Betrieb eines Hinweisgebersystems in der Regel als datenschutzrechtlich „Verantwortliche“. Die Verantwortlichkeit umfasst neben formalen Anforderungen (siehe Checkliste unten) auch die inhaltliche Verantwortung für die Einhaltung der Vorschriften der Datenverarbeitung. Die Unternehmen sind insoweit nachweisspflichtig.

Dritte, wie Softwareanbieter für interne Meldesysteme werden in der Regel als „Auftragsverarbeitende“ tätig. Hier bedarf es zwischen den Unternehmen und dem Auftragsverarbeiter den Abschluss eines Auftragsverarbeitungsvertrages gem. Art. 28 DSGVO. Sofern Rechtsanwälte oder Wirtschaftsprüfer weisungsunabhängig tätig werden, sind diese Verantwortliche. Hier kommt grundsätzlich eine Vereinbarung über eine gemeinsame Verantwortlichkeit in Betracht, vgl. § Art. 26 Abs. 2 DSGVO. Im konkreten Fall bedarf es jedoch für die Frage, ob zwischen den Beteiligten ein Auftragsverhältnis oder eine gemeinsame Verantwortlichkeit vorliegt, eine jeweils gesonderte Prüfung.

## Verantwortlichkeit und Nachweispflicht der Unternehmen

Eine Datenverarbeitung kann nach der DSGVO nur erfolgen, sofern und soweit eine Rechtsgrundlage vorliegt. Als Rechtsgrundlage kommt hier die Umsetzungsnorm des Art. 8 der WBRL in Betracht. Dabei gilt zu beachten, dass die Rechtsgrundlage nur für die von der WBRL bzw. vom HinwGebSchGE erfassten Verstöße, d. h. den sachlichen Anwendungsbereich des Gesetzes, gilt. Möchten Unternehmen die internen Meldesysteme auch für Verstöße anderer Art, wie beispielhaft gegen unternehmensinterne Ethikrichtlinien, öffnen, bedarf es gesonderter Rechtsgrundlagen (wie etwa Art. 6 Abs. 1 lit. f DSGVO). Auch aus diesem Grund und um ganz allgemein den Zugang von Meldungen zu strukturieren und kanalisieren, sollten Unternehmen festlegen, welche Verstöße Gegenstand von Hinweisen sein können. Für Meldungen etwa von sozial unerwünschtem aber ansonsten nicht rechtswidrigem Verhalten wird es grundsätzlich an Rechtsgrundlagen fehlen (siehe hierzu die Orientierungshilfe der Datenschutzaufsichtsbehörden zu Whistleblowing-Hotlines)<sup>4</sup>.

<sup>4</sup> [www.datenschutzkonferenz-online.de/media/oh/20181114\\_oh\\_whistleblowing\\_hotlines.pdf](http://www.datenschutzkonferenz-online.de/media/oh/20181114_oh_whistleblowing_hotlines.pdf)

Die gemeldeten Daten dürfen nach dem Grundsatz der Zweckbindung ausschließlich zu dem vorab festgelegten und durch die Rechtsgrundlage erfassten Zweck verarbeitet werden: Konkret bedeutet dies beispielhaft, dass eine über das Hinweisgebersystem erfasste Meldung über kundenunfreundliches Verhalten nicht für eine negative Leistungsbewertung des Arbeitnehmers genutzt werden darf. Ebenfalls dürfen Daten nur in dem für den Zweck erforderlichen Maß gespeichert werden. D. h. Daten, die für die Verfolgung der Vorwürfe unerheblich sind, dürfen bereits nicht mit aufgenommen bzw. gespeichert werden. Zudem haben die Unternehmen Löschkonzepte vorzusehen. Nach Auffassung der nationalen Datenschutzbehörden und des Europäischen Datenschutzbeauftragten sind die Daten im Regelfall zwei Monate nach Abschluss eines Verfahrens zu löschen.

## Informations-, Unterrichts- und Auskunftspflichten der Unternehmen

Zudem treffen die Unternehmen als Verantwortliche umfassende Informations-, Unterrichts- und Auskunftspflichten gegenüber den beteiligten Personen. So sind sowohl der Hinweisgebende als auch Beschuldigte und Zeugen im Verhältnis zum Unternehmen betroffene Personen im Sinne der DSGVO. Die datenschutzrechtlichen Verpflichtungen werden dabei ergänzt und überlagert durch die Vorgaben der WBRL zur Information der Hinweisperson zum Eingang ihrer Meldung und zum weiteren Fortgang des Verfahrens. Das künftige HinwGebSchG wird diese Vorgaben übernehmen.

## DSGVO-Checkliste

- Frühzeitige und ordnungsgemäße Einbindung der/s Datenschutzbeauftragten
- Erstellen eines Verarbeitungsverzeichnisses
- Ergreifen von technischen und organisatorischen Maßnahmen (ToMs)
- Erstellen einer Datenschutz-Folgeabschätzung (DSFA)<sup>5</sup>
- ggf. Abschluss eines Auftragsverarbeitungsvertrags (AVV) oder eine Vereinbarung über eine gemeinsame Verantwortlichkeit gem. § Art. 26 Abs. 2 DSGVO
- ggf. Erstellen einer unternehmensinternen Hinweisgeberrichtlinie bzw. Policy

## Fazit | Handlungsempfehlung

Bei der Einrichtung des Hinweisgebersystems sollten nicht lediglich die gesetzlichen Bestimmungen befolgt werden. Holen Sie alle relevanten Stakeholder (Betriebsrat, Datenschutzbeauftragte, HR etc.) rechtzeitig mit ins Boot und achten Sie auf eine passende Begleitkommunikation bei der Einführung des Hinweisgebersystems oder dem Relaunch. Nicht selten gibt es bei den Mitarbeitenden Vorurteile in Bezug auf Meldesysteme oder Meldungen selbst. Es soll keine Misstrauenskultur etabliert werden. Vielmehr geht es darum, dass das Unternehmen mit der zunehmenden Regulierungsdichte und den erhöhten Anforderungen an die Einhaltung von gesetzlichen Vorschriften zurechtkommt, eine angemessene Fehler(beseitigungs)kultur etabliert und bei alledem die Mitarbeitenden nicht überfordert.

Dieses Merkblatt beinhaltet lediglich eine Auswahl denkbarer Aspekte, die im Zusammenhang mit der Einführung oder der Anpassung eines Hinweisgebersystems bedacht werden sollten. Es ersetzt keine rechtliche Beratung.

Für Rückfragen stehen wir Ihnen jederzeit gerne zur Verfügung.

<sup>5</sup> Die Datenschutzbehörden halten eine solche zumindest noch für erforderlich.

## Ihre Ansprechpartner



### **Prof. Dr. Jörg Rodewald**

Rechtsanwalt, Dipl.-Kaufmann,  
Partner  
Berlin  
T +49 30 52133 21189  
[joerg.rodewald@luther-lawfirm.com](mailto:joerg.rodewald@luther-lawfirm.com)



### **Dr. Lajana von zur Gathen**

Rechtsanwältin, Associate  
Berlin  
T +49 30 52133 16764  
[lajana.von.zur.gathen@luther-lawfirm.com](mailto:lajana.von.zur.gathen@luther-lawfirm.com)



### **Caroline Risse**

Rechtsanwältin, Associate  
Berlin  
T +49 30 52133 21142  
[caroline.risse@luther-lawfirm.com](mailto:caroline.risse@luther-lawfirm.com)



### **Dr. Louisa Kimmig**

Rechtsanwältin, Associate  
Berlin  
T +49 30 52133 24845  
[louisa.kimmig@luther-lawfirm.com](mailto:louisa.kimmig@luther-lawfirm.com)

