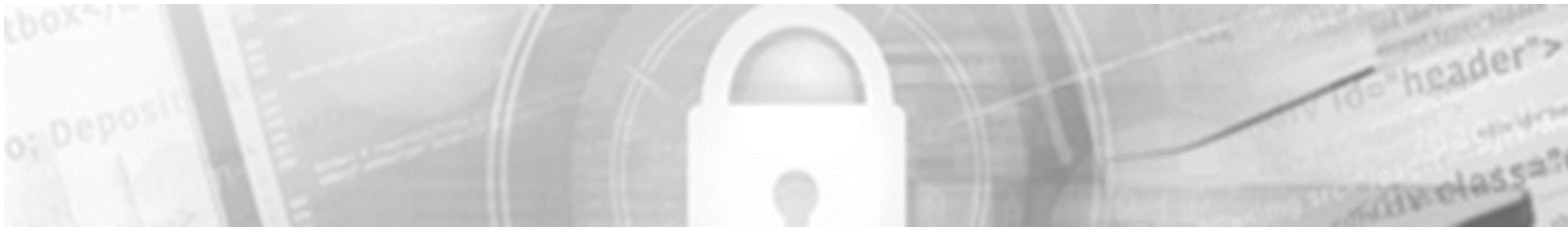


AdOrga Solutions

Gesetz für einen besseren Schutz hinweisgebender Personen sowie zur Umsetzung der Richtlinie zum Schutz von Personen, die Verstöße gegen Unionsrecht melden

Hinweisgeberschutzgesetz (HinSchG-E)

Autorin: Regina Mühlich

Stand: September 2021

Inhaltsverzeichnis

1 Einleitung

Die Richtlinie (EU) 2019/1937 des Europäischen Parlaments und Rates vom 23. Oktober 2019 zum „**Schutz von Personen, die Verstößen gegen das Unionrecht melden**“, sog. Whistleblower-Richtlinie, ist am 16. Dezember 2019 in Kraft getreten. Die Erwägungsgründe für den EU-Gesetzgeber waren u.a.:[1]

1. *Der bestehende Hinweisgeberschutz in der Union ist in den Mitgliedstaaten unterschiedlich und in den verschiedenen Politikbereichen uneinheitlich gestaltet. Die Folgen der von Hinweisgebern gemeldeten Verstöße gegen das Unionsrecht, die eine grenzüberschreitende Dimension aufweisen, zeigen deutlich, dass ein unzureichender Schutz in einem Mitgliedstaat die Funktionsweise der Unionsvorschriften nicht nur in diesem Mitgliedstaat, sondern auch in anderen Mitgliedstaaten und in der Union als Ganzem beeinträchtigt.*
2. *Es sollten gemeinsame Mindeststandards zur Gewährleistung eines wirksamen Hinweisgeberschutzes in Rechtsakten und Politikbereichen gelten, in denen die Notwendigkeit besteht, die Rechtsdurchsetzung zu verbessern, […]*
3. *Der Schutz von Hinweisgebern ist notwendig, um die Durchsetzung des Unionsrechts im Bereich der öffentlichen Auftragsvergabe zu verbessern. Es ist erforderlich, nicht nur Betrug und Korruption bei der Auftragsvergabe im Zusammenhang mit der Ausführung des Unionshaushalts aufzudecken und zu verhindern, sondern auch die unzureichende Durchsetzung der Vorschriften bei der Vergabe öffentlicher Aufträge durch nationale öffentliche Auftraggeber und Auftraggeber bei der Ausführung von Bauleistungen, der Lieferung von Waren oder der Erbringung von Dienstleistungen anzugehen.*
4. *Die Meldung von Verstößen durch Hinweisgeber kann entscheidend dazu beitragen, Risiken für die öffentliche Gesundheit und den Verbraucherschutz, die aus andernfalls womöglich unbemerkten Verstößen gegen Unionsvorschriften erwachsen, aufzudecken, zu verhindern, einzudämmen oder zu beseitigen. Vor allem im Bereich Verbraucherschutz besteht eine starke Verbindung zu Fällen, in denen Verbraucher durch unsichere Produkte erheblich geschädigt werden können. […]*
5. *Die Achtung der Privatsphäre und der Schutz personenbezogener Daten, welche als Grundrechte in den Artikeln 7 und 8 der Charta der Grundrechte der Europäischen Union (im Folgenden „Charta“) verankert sind, sind weitere Bereiche, in denen Hinweisgeber dazu beitragen können, Verstöße gegen das Unionsrecht, die das öffentliche Interesse schädigen können, aufzudecken. […]*

[1] https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32019L1937&from=DE

Die **Ziele** der EU-Whistleblowing-Richtlinie sind folglich:

- Verstöße aufdecken
- Prävention (!)
- Rechtsdurchsetzung verbessern
    - effektive, vertrauliche und sichere Meldekanäle
    - wirksamer Schutz von Hinweisgebern vor Repressalien
    - Hinweisgeber können weder zivil-, straf- oder verwaltungsrechtlich in Bezug auf ihre Beschäftigung haftbar gemacht werden.

Daraus ergibt sich:

- Anonymität ist das A und O
- Wer sollte Hinweise entgegennehmen?
  Z.B. Datenschutzbeauftragter, Leiter Compliance
- Interne oder externe Meldekanäle
  Laut EU-Richtlinie haben Hinweisgeber auch die Möglichkeit, Meldungen extern an die zuständigen Behörden weiterzugeben.
  → Nicht kalkulierbare Risiken für das betroffene Unternehmen.
- Was passiert mit Hinweisen?
  Meldungen von Verstößen müssen dokumentiert werden, Maßnahmen müssen ergriffen werden.
  →Dokumentations- und Nachweispflicht („Rechenschaftspflicht“)

Ein Referentenentwurf des Bundesministeriums der Justiz und für Verbraucherschutz liegt vor: „Gesetz für einen besseren Schutz hinweisgebender Personen sowie zur Umsetzung der Richtlinie zum Schutz von Personen, die Verstöße gegen Unionsrecht melden“, sprich das **Hinweisgeberschutzgesetz** (HinSchG), umgangssprachlich Whistleblower-Gesetz.

Dieser Referentenentwurf befand sich seit Dezember 2020 in der Ressortabstimmung der beteiligten Bundesministerien. Im April 2021 kommt das Gesetzesverfahren ins Stocken. Die CDU stimmt dem Entwurf nicht zu und kritisiert vor allem, dass der Entwurf „ohne Notwendigkeit“ über die Richtlinie hinausgeht. Die SPD besteht weiterhin auf dem bisherigen Entwurf.

Die Richtlinie sieht vor, dass sich der Hinweisgeberschutz ausschließlich auf Unionsrecht bezieht und nicht auf nationale Rechte. Der Gesetzesentwurf des HinSchG geht aber darüber hinaus und regelt auch den Hinweisgeberschutz für nationale Rechtsvorschriften.

Das Datenschutzrecht, die Datenschutz-Grundverordnung (DSGVO), gilt direkt und unmittelbar für alle EU-Mitgliedsstaaten und den EWR. Für die DSGVO spielt diese nationale „Ausklammerung“ formaljuristisch keine Rolle.

Der aktuelle Status der Umsetzung der 27 EU-Mitgliedstaaten (Auszug):[2]

Austria	not started
Belgium	in progress
Bulgaria	in progress
Croatia	in progress
Cyprus	not started
Denmark	in progress
France	in progress
Germany	in progress
Italy	in progress
Spain	in progress
Schweden	in progress
The Netherlands	in progress

Insgesamt haben bis heute 23 von 27 Länder mit der Umsetzung begonnen, 4 Länder haben noch nicht begonnen.

Gemäß Art. 26 der EU-Richtlinie haben die Mitgliedsstaaten bis zum 17. Dezember 2021 Zeit, entsprechende Rechts- und Verwaltungsvorschriften in Kraft zu setzen.

2 Hinweisgeberschutz-Gesetz (HinSchG-E)

2.1 Begriffsbestimmung

Whistleblower (zu deutsch zunehmend Hinweisgeber, Enthüller oder Aufdecker) ist der Anglizismus für eine Person, die für die Öffentlichkeit wichtige Informationen aus einem geheimen oder geschützten Zusammenhang veröffentlicht.[3]

[2] Vgl. EU Whistleblowing Monitor (August 2021)

[3] vgl. https://de.wikipedia.org/wiki/Whistleblower (zuletzt abgerufen 14.09.2021)

Einer der bekanntesten (ersten) Whistleblower: Daniel Ellsberg: 1971 veröffentlichte er geheime Pentagon-Papiere, die die Täuschung der Öffentlichkeit durch mehrere US-Regierungen enthüllten. In Deutschland ist aktuell der Diesel-Gate und der Wirecard-Skandal zu nennen.

Bereits in der Gesetzesbegründung des Gesetzes zum Schutz von Geschäftsgeheimnissen (GeschGehG) wurde der Schutz der so genannten Whistleblower (§ 5 Nr. GeschGehG) berücksichtigt. Das GeschGehG beruht auf der am 08. Juni 2016 verabschiedeten Richtlinie (EU) 2016/943 des Europäischen Parlaments und des Rates vom 08. Juni 2016 über den Schutz vertraulichen Know-hows und vertraulicher Geschäftsinformationen (Geschäftsgeheimnisse) vor rechtswidrigem Erwerb sowie rechtswidriger Nutzung und Offenlegung (ABl. L 157 vom 15.06.2016).

2.2 Geschäftsgeheimnisgesetz

Der HinSchG-Entwurf regelt auch das Verhältnis der Whistleblower-Meldung zu möglicherweise entgegenstehenden Verschwiegenheits- und Geheimhaltungspflichten des Hinweisgebers (§§ 5, 6 HinSchG-E). So fällt eine Meldung u.a. dann nicht in den Anwendungsbereich des Hinweisgeberschutzgesetzes, wenn der Meldende Berufsgeheimnisträger (z.B. Rechtsanwalt, Notar, Steuerberater, Arzt) ist. Im Falle einer Meldung durch einen (arbeits-)vertraglichen Geheimhaltungspflichten unterliegenden Beschäftigten verhält es sich anders, wenn dieser mit der Meldung eines Sachverhalts zugleich ein Geschäftsgeheimnis offenbart. Sofern der Hinweisgeber hinreichend Grund zu der Annahme hat, dass die Weitergabe bzw. Offenlegung erforderlich ist, um den Verstoß aufzudecken, ist dies erlaubt. Ggf. ist es empfehlenswert dies für den betroffenen Personenkreis bereits im Arbeitsvertrag zu regeln.

2.3 Deutschland

Bislang war der Hinweisgeberschutz in Deutschland vor allem durch die Rechtsprechung geprägt. Die Zivil- und Arbeitsgerichtsbarkeit orientieren sich an den Vorgaben des Europäischen Gerichtshofes für Menschenrechte (EGMR).[4]

2011 hat der EGMR eine Grundsatzentscheidung getroffen: Bestätigung der Pflicht des Arbeitnehmers zu Loyalität, Zurückhaltung und Vertraulichkeit gegenüber seinem Arbeitgeber und bezeichnete den Gang an die Öffentlichkeit als „letztes Mittel“.[5]

[4] Der Europäische Gerichtshof für Menschenrechte (EGMR) ist ein auf Grundlage der Europäischen Menschenrechtskonvention (EMRK) eingerichteter Gerichtshof mit Sitz in Straßburg.

[5] Bericht über die Rechtsprechung des EGMR https://www.bmjv.de/SharedDocs/Downloads/DE/Themen/Menschenrechte/Bericht_ueber_die_Rechtsprechung_des_Europaeischen_Gerichtshofs_fuer_Menschenrechte_und_die_Umsetzung_seiner_Urteile_in_V

Seit 2003 gibt es in Niedersachsen ein anonymes Hinweisgebersystem. Das online Angebot wird vom LKA Niedersachsen betrieben, über das Hinweise zu Korruption und wirtschaftskriminellen Handlungen gegeben werden können und gleichzeitig mit dem polizeilichen Sachbearbeiter anonym kommuniziert werden kann.[6]

2.4 Zentrale Reglungselemente

§ 1 **Persönlicher Anwendungsbereich**: umfasst alle Personen, die in ihrem beruflichen Umfeld Informationen über Verstöße erlangt haben Hinweis: Gleichstellung von nicht-öffentlichen und öffentlichen Bereich § 1 Abs. 8: […] Beschäftigte sind Arbeitnehmerinnen und Arbeitnehmer, Beamtinnen und Beamte, Tarifbeschäftigte, Richterinnen und Richter, Berufssoldaten sowie auf Zeit (Organisation = Beschäftigungsgeber und Dienststellen).

§ 2 **Sachlicher Anwendungsbereich** greift Rechtsbereiche auf, einbezogen werden z.B. Strafrecht und das Recht der Ordnungswidrigkeiten.

§§ 7 - 30 Interne und externe **Meldekanäle** als gleichwertig nebeneinanderstehende Meldekanäle, zwischen denen die hinweisgebende Person frei wählen kann.

§§ 32 - 38 Bei Einhaltung der Anforderungen an eine Meldung oder Offenlegung, werden hinweisgebende Personen umfangreich vor Repressalien wie Kündigung oder sonstigen **Benachteiligungen geschützt.**

Das HinSchG macht keinen Unterschied hinsichtlich der Organisation (§ 1 HinSchG-E). Es soll für Unternehmen und Behörden gleichermaßen gelten und stellt somit die gleichen Anforderungen an nicht-öffentliche wie auch öffentliche Stellen.

Eines der Hauptziele, sowohl auf EU- als auch auf nationaler Ebene ist, Anonymität für den Hinweisgeber, dem Whistleblower, zu gewähren und sicherstellen zu können. Das Gesetz sieht keine Pflicht einer anonymen Meldung vor. Allerdings haben Untersuchungen gezeigt, dass sich viele Hinweisgeber für eine anonyme Meldung entscheiden, weil sie eine hohe Unsicherheit über den Prozess und seine Konsequenzen haben. 58 % der Hinweisgeber entscheiden sich für Anonymität, wenn diese Option verfügbar ist.[7]

erfahren_gegen_die_Bundesrepublik_Deutschland_im_Jahr_2011.pdf?__blob=publicationFile&v=3 (zuletzt abgerufen 21.09.2021)

[6] https://www.lka.polizei-nds.de/kriminalitaet/deliktsbereiche/korruption/korruption-1232.html

[7] Whistleblowing Report 2019 https://uploads-campax.s3.eu-central-1.amazonaws.com/whistleblowing_report_2019_de_-_sperrfrist_15_05.pdf (zuletzt abgerufen 14.09.2021)

2.5 Sorgfaltspflicht der hinweisgebenden Person

- Art. 6 Abs. 1 lit. a RL 2019/1937: **hinreichenden Grund zu der Annahme**, dass die gemeldeten Informationen über Verstöße zum Zeitpunkt der Meldung der Wahrheit entsprachen.
- § 32 Abs. 1 Nr. 2 HinSchG-E: zum Zeitpunkt der Meldung **hinreichenden Grund zu der Annahme**, dass die gemeldeten Informationen der Wahrheit entsprachen.
- ErwG 32 S. 3 RL 2019/1937 / HinSchG, S. 68: in **gutem Glauben** ungenaue oder unzutreffende Informationen gemeldet.
- **vorsätzliches und grob fahrlässiges Handeln ausgeschlossen** (vgl. § 932 Abs. 2 BGB)
- **Zeitpunkt** der Meldung maßgeblich
  (objektive Ex-ante-Sicht; siehe dazu auch BAG, Urteil vom 07.12.2006 – 2 AZR 400/05)
- So auch BVerfG, Beschluss vom 02.07.2021 – 1 BvR 2039/00: „nicht wissentlich unwahre oder leichtfertig falsche Angaben“ sowie BAG, Urteil vom 07.12.2006 – 2 AZR 400/05: „nicht mehr berechtigt […], wenn der Arbeitnehmer schon bei Erstattung der Anzeige weiß, dass der erhobene Vorwurf nicht zutrifft oder dies jedenfalls leicht erkennen kann“.

2.6 Whistleblowing im Konzern

Ein zentrales Meldesystem ist vielfach nicht mehr ausreichend, dazu hat sich die EU-Kommission geäußert. Die EU-Kommission hat in zwei Stellungnahmen (02. Juni und 29. Juni 2021) Auslegungshinweise zur Umsetzung der Hinweisgeberrichtlinie gegeben.

Hinweisgebersysteme sind in Großunternehmen bereits heute schon verbreitet. In der Regel sind zentrale oder mehrere regionale Meldestellen eingerichtet und vielfach werden die Meldungen durch eine zentrale Stelle bearbeitet und Aufklärungsmaßnahmen von dort koordiniert. Nach Auffassung der Kommission genügt ein zentral organisiertes, konzernweites Hinweisgebersystem nicht, denn jede Gesellschaft, die mehr als 50 Mitarbeiter beschäftigt ist nach Art. 8 Abs. 3 der Hinweisgeberrichtlinie verpflichtet, ein eigenes Hinweisgebersystem einzurichten.

Für den Fall, dass eine Meldung auf einen gesellschaftsübergreifenden Verstoß hinweist und Aufklärungsmaßnahmen auf Konzernebene erforderlich machen, ist eine Bearbeitung und Aufklärung des Hinweises durch eine andere Stelle im Konzern möglich, so die EU-Kommission. Allerdings nur, wenn der Hinweisgeber zuvor über die geplante Weiterleitung der Meldung informiert wurde und sein Einverständnis zur Übermittlung erteilt. Ist der

Hinweisgeber damit nicht einverstanden, soll er seine Meldung „zurücknehmen“ und eine externe Meldung bei der zuständigen Behörde abgeben können. Offen bleibt die Frage, wie Unternehmen mit einer zurückgenommenen Meldung umgehen sollen. Es stellen sich vor allem die Fragen, ob das Unternehmen, trotz der Rücknahme, intern ermitteln darf oder sogar muss.

Unternehmensgruppen und Konzerne, die ein Hinweisgebersystem mit den Vorzügen einer zentralen oder regionalen Lösung kombiniert haben, werden ihr bestehendes System daher ergänzen und die verschiedenen Gestaltungsmöglichkeiten miteinander kombinieren müssen.

2.7 Whistleblowing im öffentlichen Dienst

Beamte und Beschäftigte im öffentlichen Dienst unterliegen der Verschwiegenheitspflicht. Sie müssen aber auch bei Rechtsverstößen und Missständen tätig werden. Mit der nationalen Gesetzgebung sollen Behörden und Kommunen mit mehr als 10.000 Einwohnern verpflichtet werden, Kanäle einzurichten, über die Verstöße gegen EU- wie auch nationales Recht gemeldet werden können. Es entsteht dabei ein Spannungsverhältnis zwischen Geheimhaltungsinteresse und Transparenz für die Beamten und Beschäftigten. Zum einen gilt es das öffentlich-rechtliche Dienst- und Treuverhältnis gegenüber dem Dienstherrn und der Verschwiegenheitspflicht, zum anderen die unbedingte Verfassungs- und Gesetzestreue. Aus diesem Grundkonflikt der Normen hat sich eine „Stufentheorie“ etabliert, nach der zunächst der interne Dienstweg einzuhalten ist (Remonstrationspflicht [8]). Die EU-Richtlinie selbst sieht ein Wahlrecht des Hinweisgebenden vor.

3 Praktische Umsetzung

Die Implementierung des HinSchG sollte wie auch die Einführung eines jeden anderen Managementsystems z. B. Datenschutz oder Qualitätsmanagement, angegangen werden. Auf jeden Fall ist ein strukturiertes Vorgehen erforderlich.

Praxistipp

Was ist ein Managementsystem?

Ein Managementsystem beschreibt Maßnahmen, die dazu beitragen, den Hauptzweck sowie die Rahmenbedingungen des Unternehmens sicher und effizient umzusetzen. Dazu erfasst das Managementsystem interne wie externe Anforderungen und setzt diese anschließend in Aufgaben um. Die Durchführung dieser Aufgaben wird organisiert und

[8] Pflicht des Beamten, Bedenken gegen die Rechtmäßigkeit dienstlicher Anordnungen unverzüglich bei dem unmittelbaren Vorgesetzten geltend zu machen (§ 63 BGB).

regelmäßig überprüft (PDCA-Zyklus). Entspricht sie nicht den festgelegten Kriterien, erfolgt eine Korrektur, die das System insgesamt verbessert und anpasst.

Der „Problemlösezyklus“ (Projektmanagement):

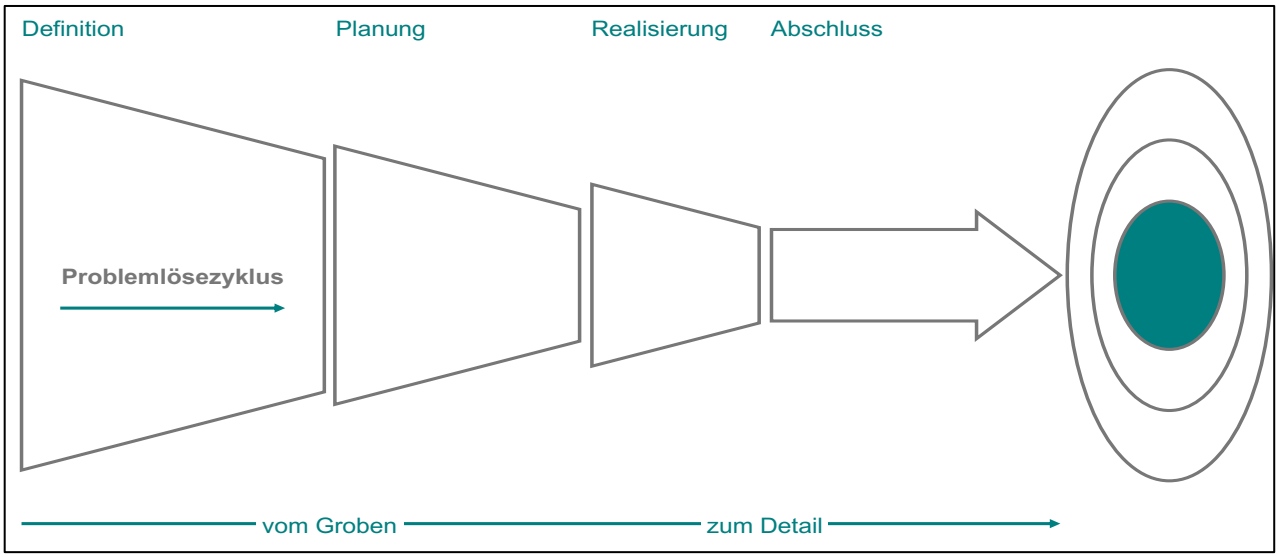


Abb. 1: Problemlösungszyklus (Quelle: Regina Mühlich)

Es gilt die Beweisumkehr. Für den Arbeitgeber bzw. den Dienstherren bedeutet dies, dass sie zum Beispiel nachweisen müssen, dass die Beendigung des Arbeitsvertrages bzw. Dienstvertrages nichts mit der Aufdeckung der Missstände zu tun hat. Die neuen Regeln sollen für Angestellte wie auch für Beamte gleichermaßen gelten (§ 35 HinSchG-E).

3.1 Pflicht zur Implementierung eines Hinweisgebersystems

(1) *Eine **interne Meldestelle** kann eingerichtet werden, indem eine beim Beschäftigungsgeber oder bei der Dienstelle beschäftigte Person, eine interne Organisationseinheit oder ein Dritter mit den Aufgaben einer internen Meldestelle betraut wird.*

*(2) Mehrere Beschäftigungsgeber mit in der Regel 50 bis 249 Beschäftigten können für die Entgegennahme von Meldungen und für die weiteren nach diesem Gesetz vorgesehenen Maßnahmen eine **gemeinsame Stelle** betreiben oder einen **Dritten** beauftragen, eine gemeinsame Stelle für sie zu betreiben.*

Es bleibt den öffentlichen und nicht-öffentlichen Stellen überlassen, „wie“ sie die Meldestellen organisieren. Eine Organisation ist ab mehr als 50 Beschäftigten zwingend erforderlich.

Welche Personen als Beschäftigte zu zählen sind, definiert das HinSchG-E in § 3 Abs. 3:

Beschäftigte sind

1. *Arbeitnehmerinnen und Arbeitnehmer,*
2. *die zu ihrer Berufsbildung Beschäftigten,*
3. *Beamtinnen und Beamte mit Ausnahme der Ehrenbeamtinnen und Ehrenbeamten,*
4. *Tarifbeschäftige,*
5. *Richterinnen und Richter mit Ausnahme der ehrenamtlichen Richterinnen und Richter,*
6. *Berufssoldatinnen und Berufssoldaten sowie Soldatinnen und Soldaten auf Zeit,*
7. *Personen, die wegen ihrer wirtschaftlichen Unselbständigkeit als arbeitnehmerähnliche Personen anzusehen sind; zu diesen gehören auch die in Heimarbeit Beschäftigten und die ihnen Gleichgestellten.*

Also vergleichbar mit den Regelungen des ArbPlSchG: Beschäftigte sind Arbeitnehmer, die zu ihrer Berufsbildung Beschäftigten, arbeitnehmerähnliche Personen, Beamte, Richter, Soldaten sowie die in Werkstätten für Behinderte beschäftigten oder des § 26 Abs. 8 BDSG.

Wobei auch hier, eine „Kopfzählerei und -schieberei“ nicht zielführend ist. Das Fehlen einer Organisationsform und Strukturen potenziert vielmehr das Risiko.

3.2 Präventionsmaßnahmen

- Risikosensibilisierung und Verantwortlichkeiten abgrenzen
- Organisationsinterne Arbeitsgruppe bilden
  (Compliance, HR, Legal, CSR, Datenschutzbeauftragter)
- „Code of Conduct“
  Organisation und Kommunikationsregeln
- (Themenbezogene) Meldewege und Ansprechstellen im Unternehmen definieren
- Prüf- und Abhilfeprozess implementieren:
  Abgrenzung rechtliche Relevanz, „Opfer- und Beschuldigtenschutz“ sicherstellen, Vertraulichkeitszusicherungen, Anonymitätsschutz, Datenschutz.
- Schulungen der Mitarbeiter und der Arbeitsgruppe in diskriminierungsrechtlicher Hinsicht sowie Schulung des Gesamtprozesses

3.3 Maßnahmen zum Schutz des Hinweisgebers

Gemäß §§ 32 ff. HinSchG-E hat die Organisation Maßnahmen zu treffen, die die hinweisgebende Person insbesondere vor Repressalien und Benachteiligungen oder Offenlegung des Sachverhalts schützt.

Der „Nichtschutz“, d.h. ein Verstoß gegen dieses Verbot, begründet Schadensersatzpflichten des Verursachers (z.B. unbefugte Offenlegung) gegenüber dem Hinweisgeber (§ 32 HinSchG-E) und ist gemäß § 39 Abs. 1 Nr. 3 HinSchG-E auch bußgeldbewährt.

Der Hinweisgeber soll außerdem für die Meldung oder Offenlegung der Informationen oder für daraus evtl. entstehenden Schäden auf Seiten des Betroffenen nicht verantwortlich gemacht werden können. Dies setzt aber voraus, dass der Hinweisgeber rechtmäßig Zugriff auf die Informationen nehmen konnte und Grund zu der Annahme hat, dass die Informationsweitergabe erforderlich war, um den Vorstoß aufzudecken (§ 34 HinSchG-E).

Diese gesetzlichen Anforderungen machen auch die Erforderlichkeit der Möglichkeit eines absolut vertrauenswürdigen Meldekanals ersichtlich. Eine weitestgehende Anonymität kann auch durch einen „neutralen“ und außerhalb der Organisation befindlichen Ansprechpartner (Ombudsperson, z.B. externer Datenschutzbeauftragter) gewährleistet werden.

Eine „anonyme Meldung“ führt evtl. zu Schwierigkeiten und Verzögerungen bei der Nachverfolgung und Klärung des Hinweises. Ein fachkundiger direkter Ansprechpartner kann außerdem gewisse Eckpunkte, wie z.B. Details zum Sachverhalt, Vorgehenswünsche des Hinweisgebers bezüglich der Anonymität, in einem Telefonat abklären.

3.4 Meldekanäle

Kommunikationswege „bei Anhaltspunkten für Verstöße gegen Gesetze oder Regelungen der Organisation“:

- **Telefonisch**
  Einrichtung einer telefonischen, für den Anrufer kostenlosen Hotline: Da die Meldung zu jeder Zeit möglich sein muss, muss bei einer persönlichen Hotline sichergestellt werden, dass diese permanent besetzt ist und sich keine sprachlichen Barrieren ergeben.
  Die Ombudsperson, die den Anruf in diesem Fall entgegennimmt, ist zur Wahrheit verpflichtet, muss laut Bundesverfassungsgericht (Beschluss vom 27.06.2018, 2

BvR 1405/17)[9] jedoch kein Anwalt sein. Diese Funktion kann somit auch der (vorrangig der externe) Datenschutzbeauftragte übernehmen. Dies bietet sich insofern an, da dieser in seiner Funktion eine Vertrauensperson innerhalb der Organisation sowie weisungsfrei ist, per se die Rechte der betroffenen Person, den Beschäftigten, vertritt und qua seiner Funktion auch zur Vertraulichkeit und Verschwiegenheit verpflichtet ist. Hinzu kommt, dass der DSB sehr gut mit den Prozessen und Verfahren im Unternehmen vertraut ist.

Alternativ besteht die Möglichkeit einer automatischen Voicebox, auf der die Meldung aufgenommen und für eine angemessene Dauer aufbewahrt werden kann (z.B. Hinweise zur Erreichbarkeit (09:00 – 17:00 h), ggf. Hinweise für andere Sprachen).

- **Persönlich / physisch**
  Auch hier bietet sich als direkter Ansprechpartner der Datenschutzbeauftragte an sowie der Compliance Officer oder die Revision.
- **E-Mail**
  Zugriff durch einen kleinen und definierten Kreis; vor allem ist aber zu gewährleisten, dass Abwesenheiten von Ansprechpartnern nicht zu Bearbeitungsverzögerungen führen.
- **Per Post**
  Die Post sollte möglichst durch die hinweisgebende Person entsprechend adressiert werden (z.B. Angaben im Intranet, Unternehmens-Wiki). Ungeachtet dessen muss bei der Bearbeitung des Posteingangs absolute Vertraulichkeit und Stillschweigen gewährleistet sein.
- (Elektronisches Hinweisgebersystem

  Ein IT-gestütztes Hinweisgebersystem ist gesetzlich nicht verpflichtend, aber möglich. Hier entstehen laufende Kosten, sowohl für die Zurverfügungstellung als auch für den technischen Support. Diese Möglichkeit ist vor allem für große Unternehmen(sgruppen) und Konzerne geeignet. (Hinweis: Die Identifizierung des Meldenden u.a. über die IP-Adresse muss ausgeschlossen sein.)

3.5 Datenschutzrechtliche Anforderungen

Die datenschutzrechtlichen Vorgaben bleiben von der Whistleblower-Gesetzgebung unberührt, d. h. die DSGVO, das BDSG und andere spezialgesetzliche Normen sind auch hier im Umgang mit den personenbezogenen Daten einzuhalten.

[9] https://www.bundesverfassungsgericht.de/e/rk20180627_2bvr140517.html

Als **Erlaubnistatbestände** kommen hier, neben einer Einwilligung, die Aufdeckung von Straftaten Art. 6 Abs. 1 Satz 1 lit. f DSGVO bzw. § 26 Abs. 1 Satz 2 BDSG als Rechtfertigungsgrundlage zum Ansatz.

Spezialgesetzlich werden die Datenverarbeitungsbefugnisse in § 10 HinSchG-E normiert. Meldungen, die personenbezogene Daten enthalten und durch Meldestellen im Rahmen ihrer Aufgaben (§§ 13, 23 HinSchG-E) entgegengenommen werden, dürfen hiernach entgegengenommen, ausgewertet, bearbeitet und weitergegeben werden. Dies gilt auch für Folgemaßnahmen.

Gemäß **Art. 15 DSGVO** besteht ein Auskunftsrecht des Betroffenen. Gemäß **Art. 14 DSGVO** (Informationspflicht) sind Unternehmen verpflichtet, Betroffene über die Datenverarbeitung, Eingang einer ihre Person betreffende Whistleblowing-Meldung, zu informieren.

Es sind geeignete **technisch-organisatorische Maßnahmen** (Artt. 32, 25 DSGVO) zu treffen. Ein Zugriff von Unbefugten ist auszuschließen und die Identität jeder von einer Meldung betroffenen Person muss geschützt sein. Berechtigungskonzept, Protokollierung von Dateiengaben sowie dauerhafte und abrufbare Dokumentation ist sicherzustellen (siehe Pkt. 4.6) wie auch Löschkonzepte.

Selbstverständlich sind die Verarbeitung im Rahmen des Hinweisgeberschutzsystems im **Verzeichnis der Verarbeitungstätigkeiten** (Art. 30 DSGVO) zu dokumentieren sowie gemäß Art. 28 DSGVO ggf. Vereinbarungen zur Auftragsverarbeitung mit Dienstleistern abzuschließen.

Des Weiteren ist, aufgrund des hohen Risikos für die Rechte und Freiheiten natürlicher Personen, welches sich bei einer Meldung von Missständen ergibt, eine **Datenschutz-Folgenabschätzung** (Art. 35 Abs. 1 DSGVO) erforderlich.

Selbstverständlich sind auch hier die **Grundsätze der Verarbeitung** personenbezogener Daten (Art. 5 Abs. 1 DSGVO) wie u.a. Zweckbindung, Datenminimierung und Transparenz sowie die **Rechenschaftspflicht** (Abs.2) zu gewährleisten.

Infolgedessen sollte der Datenschutzbeauftragte frühzeitig in die Planung und für die Bewertung der datenschutzrelevanten Anforderungen eingebunden werden.

3.6 Nachweis- und Dokumentationspflicht

Analog der Rechenschaftspflicht des Artikel 5 Abs. 2 der Datenschutz-Grundverordnung gilt auch beim HinSchG, dass die Organisation die Einhaltung nachweisen können muss. Vor allem ist es empfehlenswert - und eigentlich zwingend erforderlich - die Prozesse für die hinweisgebende Person transparent darzulegen.

Des Weiteren sollten klare Verfahren und Verhaltensweisen vorgegeben und beschrieben werden, wie das allgemeine Vorgehen ist sowie welche internen (z.B. Gleichbehandlungsbeauftragte, Datenschutzbeauftragte) und externe Stellen (z.B. Rechtsanwälte) wann und wie zu informieren sind.

„Wirksamkeitskontrolle“:

- Dokumentation
- Risikoanalysen
- Berichtswesen
- Richtlinien
- Reaktion(spläne) auf Vorfälle

Der **PDCA-Zyklus**, auch Deming-Zyklus genannt, beschreibt den vierstufigen Regelkreis des Kontinuierlichen Verbesserungsprozesses (KVP). Die Phasen sind: Plan, Do, Check, Act. Die Anwendung des Zyklus sorgt für einen kontinuierlichen und fortlaufenden (Verbesserungsprozess).

Regelkreis des Managementsystems:

1. Planung
   Vorgaben: Gesetze (hier vorrangig das HinSchG)
2. Durchführung und Umsetzung
   Organisation, Prozessbeschreibungen, Anweisungen
3. Überprüfung
4. Anpassung

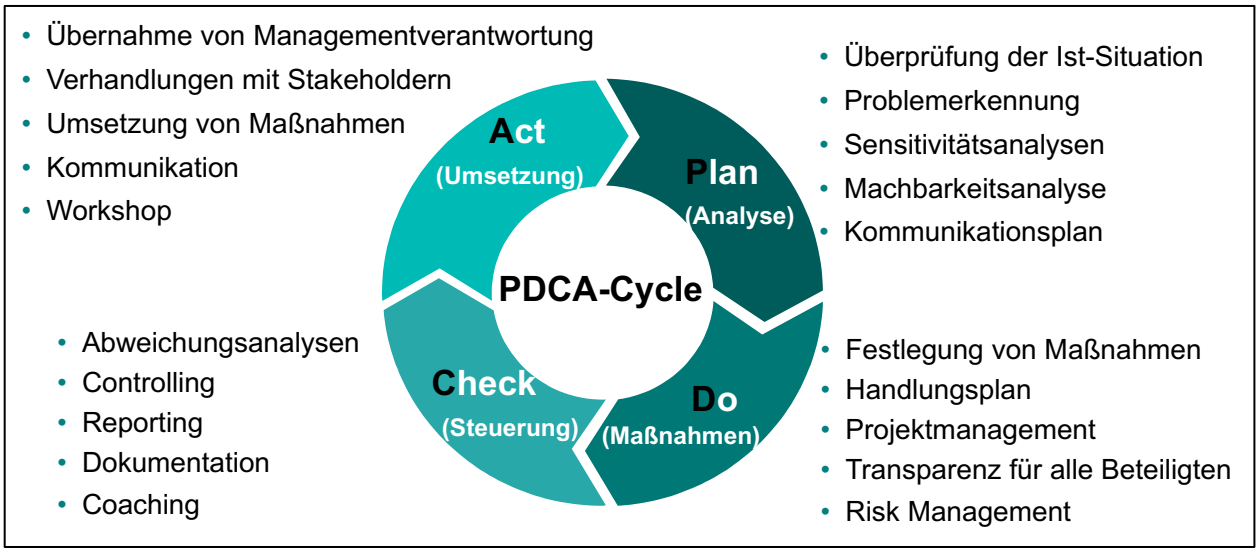


Abb. 2: PDCA-Methode (Quelle: Regina Mühlich)

4 Sanktionen

Eine Zuwiderhandlung gegen Verpflichtungen aus dem HinSchG stellt eine Ordnungswidrigkeit dar und es drohen Bußgelder bis zu 100.000 Euro. Das Fehlen einer internen Meldestelle ist sanktionslos. Es liegt jedoch im eigenen Interesse der Organisation, eine interne Aufklärung zu ermöglichen und zu vermeiden, dass Hinweisgeber sich an die Öffentlichkeit wenden.

- **Verstoß gegen Schutz des Hinweisgebers**
  - Verbot von Repressalien (§ 35 HinSchG-E) mit Beweislastumkehr
  - Schadensersatz nach Repressalien (§ 36 HinSchG-E)
  - Bußgeldsanktionen (§ 39 HinSchG-E)
- **Verstoß gegen Errichtung eines Hinweisgebersystems**
  - zivilrechtliche Haftung der Unternehmensleitung
  - Begründung der Haftung nach OWiG
  - Haftungszurechnung
- **Verstoß gegen insbesondere Datenschutzbestimmungen**
  - sowohl in Bezug auf Hinweisgebende als auch vom Hinweis Betroffene
  - Art. 82 DSGVO materielle und immaterieller Schaden
  - Art. 83 DSGVO Geldbußen
- **Verstoß gegen Schutz des Beschäftigungsgebers**
  - „beschäftigungsrechtliche Konsequenzen“
  - Schadensersatz
  - Strafbarkeit

5 Compliance

Die Gesetzgebung und Rechtsprechung treibt den Aufbau von Compliance Management-Systemen (CMS) voran. Mit „sanftem gesetzlichen Druck“ wird durch Anreize und Haftungserleichterungen (z.B. Verbandssanktionsgesetz) werden Organisationen dazu angehalten, Rechtsverstöße nicht mehr als Kavaliersdelikte zu betrachten oder sie gar zu ignorieren. In strafrechtlichen Ermittlungsverfahren stellt die Staatsanwaltschaft stets die Frage, nach der Verantwortung, d.h. wer hat diesen Compliance-Verstoß zu vertreten. Die Rechtsprechung agiert hier nach dem Schuldprinzip. Nach dem BGH-Urteil vom 09. Mai 2017 ist die Schuld bei der Strafe und Bemessung der Geldbuße gegen ein Unternehmen aller beteiligten Führungspersonen festzustellen.

Dabei ist es ein Irrtum zu denken, dass Stabsstellen, Datenschutzbeauftragte, Beauftragte für Geldwäsche, Compliance Officer und weitere Berater, aufgrund der Beratungsfunktion nicht haftbar gemacht werden können. Das BGH-Urteil vom 17. September 2009 stellt klar, dass es Aufgabe der Mitarbeiter im Unternehmen ist, Straftaten aktiv zu verhindern.

Ein Compliance Management System ist kein „nice-to-have“, sondern ein „must have“. Dies auch vor dem Hintergrund, dass sich ein gutes CMS strafmindernd auswirken kann. Ungeachtet dessen, dass Regelverstöße gemäß § 43 Abs. 2 GmbHG bzw. § 93 AktG von den zuständigen Organen – schon seit jeher - aufzuklären sind.

6 Fazit

Nach Auffassung der deutschen Datenschutzaufsichtsbehörden ist die Einrichtung und Nutzung firmeninterner Meldekanäle „unter besonderer Berücksichtigung des von dem Unternehmen verfolgten Zwecks und der Einrichtungsmodalitäten datenschutzgerecht“ möglich.

Das kommende Hinweisgeberschutzgesetz setzt die Regelungen der EU-Whistleblower-Richtlinie in deutsches Recht um. Der Gesetzesentwurf untersagt jedwede Vergeltungsmaßnahmen und Repressalien gegenüber dem Hinweisgebenden; es wird auch hier eine Beweislastumkehr bei Kündigungen eingeführt. Die Regelungen gelten sowohl für Unternehmen als auch Behörden. Die nationale Umsetzung muss bis spätestens 17. Dezember 2021 erfolgen.

Das Ziel eines Compliance-Management-Systems (CMS) sollte dabei nicht aus den Augen verloren gehen: Ziel eines wirksamen CMS ist der Schutz von Mitarbeitern, Führungskräften und Stakeholdern.

Für ein erfolgreiches Compliance-System ist die Unternehmensleitung daher sehr wichtig. Maßgeblich sind außerdem die Vorbildfunktion von Fach- und Führungskräften sowie den Leitungsorganen, die Kommunikation von Werten und das kompromisslose Sanktionieren von „Non-Compliance“.

Nicht-befolgen („Non-Compliance“) hat Konsequenzen. Für den Einzelnen, z.B. Abmahnung und Entlassung, aber auch für die ganze Organisation, z.B. Sanktionen, Bußgeld, Reputationsverlust.

Compliance ist eine zentrale Voraussetzung für langfristigen und nachhaltigen unternehmerischen Erfolg. Verlässlichkeit, Kontinuität und Vertrauen können in einem Unternehmen nur bestehen, wenn sich dieses deutlich, auch nach außen, zu Compliance bekennt.

Ob der Referentenentwurf des BMJV im Herbst 2021 das parlamentarische Verfahren durchläuft und die Frist bis zum 19. Dezember 2021 eingehalten werden kann, bleibt abzuwarten. Dies gilt auch für das Verbandssanktionengesetz. Festzuhalten bleibt:

Gelingt der Regierungskoalition die Verabschiedung nicht, droht Deutschland ein Vertragsverletzungsverfahren. Außerdem könnte sich eine hinweisgebende Person, sofern es die Verletzung von EU-Rechten betrifft, ggf. unmittelbar auf die EU-Whistleblower-Richtlinie berufen. Für die Organisationen bedeutet dies Rechtsunsicherheit und ggf. unterschiedliche staatsanwaltliche Ansätze.

Bis zum 17. Dezember 2021 bleibt nicht mehr viel Zeit – sowohl für den Gesetzgeber als auch für die Organisationen. Insbesondere für Unternehmen gilt: eine Übergangsfrist ist nicht geplant. Es sollte daher zeitnah mit der Prozessplanung begonnen werden – und der Datenschutzbeauftragte eingebunden werden.

7 Links

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

  Amtsblatt: https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32019L1937&from=DE

- Referentenentwurf des Bundesministeriums der Justiz und Verbraucherschutz „Gesetz zum Schutz hinweisgebender Personen https://www.whistleblower-net.de/wp-content/uploads/2021/02/2020_11_26-Referentenentwurf-Whistleblowing-BMJV-1.pdf

8 Abbildungsverzeichnis

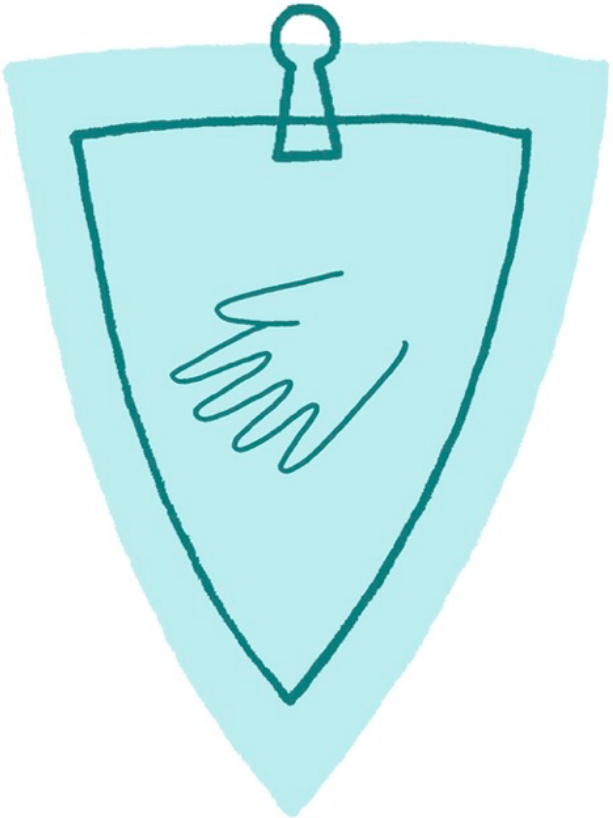
9 Autorin

Regina Mühlich ist Geschäftsführerin der Managementberatung AdOrga Solutions GmbH. Sie ist Expertin für Datenschutz, Sachverständige für EDV und Datenschutz, Informationssicherheits-beauftragte (ISO/IEC 27001 (ISMS), CSR-/Nachhaltigkeitsbeauftragte (zert.) sowie Auditorin für Datenschutz und Qualitätsmanagement (zert.) sowie Compliance Officer (zert.). Als Compliance Officer und Datenschutzbeauftragte berät und unterstützt sie und ihr Team nationale und internationale Unternehmen aus unterschiedlichsten Branchen. Sie ist gefragte Referentin für Seminare und Vorträge; Mitglied des Regionalausschusses der IHK München und Oberbayern sowie Vorstandsmitglied des Berufsverbands der Datenschutzbeauftragten Deutschlands (BvD) e. V.

Für weitere Informationen

Regina Mühlich
AdOrga Solutions GmbH
E-Mail: consulting@AdOrgaSolutions.de
www.AdOrgaSolutions.de

* Hinweis: Der Übersichtlichkeit wegen wurden nur männliche Formen verwendet.



(Bildquelle: © AdOrga Solutions GmbH)