Datenschutzkonzept für das Hinweisgebersystem

Inhaltsübersicht

1. Gegenstand und Vorbehalt

Das vorliegende Datenschutzkonzept betrifft das Hinweisgebersystem und wurde von einer KI erstellt. Es fasst den wesentlichen Sachverhalt der Datenverarbeitung zusammen (Ziffer 2), wie er in einem strukturierten Dialog zwischen KI und Nutzer ermittelt wurde. Daneben gibt das Datenschutzkonzept Ergebnisse einer datenschutzrechtlichen KI-Prüfung wieder (Ziffer 3) und empfiehlt nächste Schritte (Ziffer 4).

Eine KI erstellt Texte auf der Grundlage statistischer Wahrscheinlichkeiten. Die Ergebnisse können unvollständig oder falsch sein. Dieses Dokument stellt keine Rechtsberatung dar und kann diese nicht ersetzen. Sie müssen es von einer fachkundigen Person prüfen und anpassen lassen, z.B. von einem Rechtsanwalt oder Datenschutzbeauftragten. Sie können hierzu den Autor des Tools, IT-Fachanwalt Dr. Thomas Helbing, unter helbing@thomashelbing.com kontaktieren.

2. Sachverhalt

Die Verarbeitungstätigkeit umfasst den Betrieb und die Nutzung eines digitalen Hinweisgebersystems. Dieses System dient der Entgegennahme und Bearbeitung von Meldungen über potenzielle oder tatsächliche Verstöße gegen Gesetze oder unternehmensinterne Richtlinien. Es ermöglicht eine vertrauliche und auf Wunsch anonyme Kommunikation.

2.1 Gegenstand

Gegenstand der Datenverarbeitung ist die Bereitstellung und der Betrieb einer Plattform zur Abgabe von Hinweisen (Hinweisgebersystem) sowie die anschließende Bearbeitung, Untersuchung und Dokumentation der eingegangenen Meldungen. Ziel ist die Erfüllung der gesetzlichen Pflichten aus dem Hinweisgeberschutzgesetz (HinSchG) und die Aufdeckung sowie Prävention von Missständen im Unternehmen.

2.2 Beteiligte Akteure

An der Datenverarbeitung sind zwei Akteure beteiligt: die **deutsche Tochtergesellschaft** (für die dieses Konzept erstellt wird) und ihre **französische Muttergesellschaft**.

Die französische Muttergesellschaft hat die konkrete Hinweisgeber-Plattform (Software) ausgewählt und ist für deren technischen Betrieb verantwortlich. Sie konzipiert den grundlegenden Prozess von der Entgegennahme einer Meldung bis zur Erstprüfung.

Die deutsche Tochtergesellschaft hat entschieden, dieses von der Muttergesellschaft bereitgestellte System zu nutzen, um ihre lokalen gesetzlichen Pflichten nach dem HinSchG zu erfüllen. Sie hat den von der Muttergesellschaft konzipierten Prozess akzeptiert. Meldungen, die die deutsche Gesellschaft betreffen, werden nach einer Erstprüfung durch die Muttergesellschaft an die deutsche Gesellschaft zur weiteren Untersuchung und für Folgemaßnahmen übergeben.

2.3 Verarbeitungsphasen

Der Datenlebenszyklus gliedert sich in folgende Phasen:

- **Erhebung:** Hinweisgeber (z.B. Mitarbeiter, Lieferanten) geben über die von der Muttergesellschaft betriebene Plattform eine Meldung ab. Dies kann unter Angabe von Kontaktdaten oder anonym geschehen.
- **Bearbeitung (Phase 1 - Muttergesellschaft):** Die zentrale Meldestelle bei der Muttergesellschaft in Frankreich nimmt die Meldung entgegen, bestätigt den Eingang und führt eine erste Plausibilitätsprüfung durch.
- **Übermittlung:** Stellt die Muttergesellschaft fest, dass die Meldung die deutsche Tochtergesellschaft betrifft, übermittelt sie die relevanten Informationen an die zuständigen Stellen (z.B. Compliance, HR) in Deutschland.
- **Bearbeitung (Phase 2 - Tochtergesellschaft):** Die deutsche Tochtergesellschaft übernimmt den Fall, führt interne Untersuchungen durch, ergreift Folgemaßnahmen (z.B. Befragungen, Einleitung disziplinarischer Schritte) und kommuniziert mit dem Hinweisgeber.
- **Speicherung und Löschung:** Alle im Zusammenhang mit einer Meldung stehenden Daten und Dokumentationen werden für die Dauer des Verfahrens und darüber hinaus gemäß den gesetzlichen Vorgaben aufbewahrt und anschließend gelöscht.

2.4 Datenarten und Herkunft

Es werden folgende Datenarten verarbeitet:

1. Identifikations- und Kontaktdaten
2. Inhaltsdaten der Meldung
3. Daten zur Fallbearbeitung und Untersuchung
4. Nutzungsdaten des Systems

Die Daten beziehen sich auf folgende Betroffenengruppen:

- Hinweisgeber
- Beschuldigte Personen
- Sonstige im Sachverhalt genannte Personen (z.B. Zeugen)
- Bearbeitende Personen (Mitarbeiter in Compliance/HR)

Die Daten stammen aus diesen Quellen:

- Hinweisgeber
- Interne Systeme (z.B. HR-Verzeichnis zur Identifizierung von Beteiligten)
- Werden im Rahmen der internen Untersuchung erzeugt und erhoben
- Hinweisgebersystem

Eine **Zuordnung**, welche Daten sich auf welche Betroffenen beziehen, woher die Daten stammen und welche konkreten Datenfelder umfasst sind, findet sich in der Datentabelle im Anhang A.

2.5 Nutzungszwecke

Die Daten können für folgende Zwecke genutzt werden:

- A. **Betrieb des Hinweisgebersystems und Entgegennahme von Meldungen**: Dies umfasst die Bereitstellung der Plattform durch die Muttergesellschaft und die Entgegennahme der Meldungen.
- B. **Prüfung von Meldungen und Durchführung von Folgemaßnahmen**: Dies beinhaltet die Untersuchung des gemeldeten Sachverhalts und die Umsetzung daraus resultierender Maßnahmen.
- C. **Gewährleistung der IT-Sicherheit und Integrität des Systems**: Dies betrifft die Sicherstellung, dass die Plattform sicher und funktionsfähig ist.

Die Zuordnung, welche Datenarten für die einzelnen Nutzungszwecke verwendet werden, ergibt sich aus der Daten-Zweck-Matrix im Anhang B.

2.6 Empfänger

Die Daten können an diese Empfänger weitergegeben werden:

- Französische Muttergesellschaft (Frankreich)
- Externe Berater (z.B. Rechtsanwälte, Wirtschaftsprüfer) (Deutschland / EU)
- Behörden (z.B. Strafverfolgungsbehörden, Aufsichtsbehörden) (Deutschland)

Die externen Berater werden zur unabhängigen rechtlichen Beratung oder Untersuchung hinzugezogen und handeln dabei nicht als weisungsgebundene Dienstleister. Eine Datenweitergabe an Behörden erfolgt nur, wenn eine gesetzliche Verpflichtung hierzu besteht oder ein zwingendes Interesse an der Verfolgung einer Straftat vorliegt.

Welche Datenarten an welche Empfänger zu welchen Zwecken übermittelt werden, ist in Anhang C dargestellt.

3. Bewertung

3.1 Datenschutzrechtliche Rollen

Die **deutsche Tochtergesellschaft** und die **französische Muttergesellschaft** sind **gemeinsam Verantwortliche** (Joint Controller) im Sinne des Art. 26 DSGVO.

Gemäß Art. 4 Nr. 7 DSGVO ist "Verantwortlicher", wer allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. Eine gemeinsame Verantwortlichkeit nach Art. 26 DSGVO liegt vor, wenn zwei oder mehr Verantwortliche die Zwecke und Mittel der Verarbeitung gemeinsam festlegen. Dies erfordert eine gemeinsame oder sich ergänzende (konvergierende) Entscheidungsfindung, sodass die Verarbeitung ohne den Beitrag jedes Beteiligten nicht in der beabsichtigten Form stattfinden könnte.

Im vorliegenden Fall legt die französische Muttergesellschaft wesentliche *Mittel* der Verarbeitung fest, indem sie die technische Plattform auswählt, betreibt und den grundlegenden Prozessablauf gestaltet. Die deutsche Tochtergesellschaft entscheidet über die Nutzung dieser Plattform und ist für die wesentlichen Folgemaßnahmen und Untersuchungen bei Deutschland-Bezug verantwortlich. Beide Akteure verfolgen zudem *gemeinsame und sich ergänzende Zwecke*: Die Muttergesellschaft hat ein Interesse an einer konzernweit einheitlichen Compliance, während die Tochtergesellschaft ihre spezifischen gesetzlichen Pflichten nach dem HinSchG erfüllt. Da die Entscheidungen beider Gesellschaften untrennbar miteinander verknüpft sind und die Verarbeitung ohne das Zusammenwirken beider nicht möglich wäre, liegt eine gemeinsame Verantwortlichkeit vor.

3.2 Rechtsgrundlagen

Die Verarbeitung der Daten stützt sich auf verschiedene Rechtsgrundlagen gemäß Art. 6 Abs. 1 DSGVO.

Für den **Betrieb des Hinweisgebersystems und die Entgegennahme von Meldungen (Zweck A)** sowie für die **Prüfung von Meldungen und Durchführung von Folgemaßnahmen (Zweck B)** ist die primäre Rechtsgrundlage die Erfüllung einer **rechtlichen Verpflichtung** gemäß **Art. 6 Abs. 1 lit. c DSGVO**. Diese Verpflichtung ergibt sich für die deutsche Tochtergesellschaft aus dem deutschen Hinweisgeberschutzgesetz (HinSchG), welches Unternehmen ab 50 Mitarbeitern zur Einrichtung und zum Betrieb eines internen Meldekanals verpflichtet.

Ergänzend stützt sich die Verarbeitung für die **Prüfung von Meldungen und Folgemaßnahmen (Zweck B)** sowie für die **Gewährleistung der IT-Sicherheit (Zweck C)** auf das **berechtigte Interesse** des Unternehmens gemäß **Art. 6 Abs. 1 lit. f DSGVO**. Das berechtigte Interesse besteht darin, Compliance-Verstöße und strafrechtlich relevantes Verhalten aufzudecken, Schäden vom Unternehmen abzuwenden, interne Prozesse zu verbessern und die Integrität und Sicherheit des IT-Systems zu gewährleisten. Diese Interessen überwiegen in der Regel die Interessen der betroffenen Personen (insbesondere der beschuldigten Person), da das HinSchG selbst einen Rahmen schafft, der die Vertraulichkeit und die Rechte aller Beteiligten schützt.

Die für die jeweiligen Datenarten und Nutzungszwecke geltenden Rechtsgrundlagen sind im Anhang D (Übersicht Rechtsgrundlagen) dargestellt.

3.3 Besondere Kategorien personenbezogener Daten

Die **Inhaltsdaten der Meldung (Datenart 2)** sowie die daraus resultierenden **Daten zur Fallbearbeitung und Untersuchung (Datenart 3)** können besondere Kategorien personenbezogener Daten im Sinne des Art. 9 Abs. 1 DSGVO enthalten. Dies ist der Fall, wenn eine Meldung beispielsweise Angaben zur ethnischen Herkunft, zu politischen Meinungen, zur Gewerkschaftszugehörigkeit oder zu Gesundheitsdaten einer Person enthält (z.B. bei Meldungen über Diskriminierung oder Mobbing).

Die Verarbeitung solcher Daten ist grundsätzlich untersagt. Hier greift jedoch die Ausnahme des **Art. 9 Abs. 2 lit. b DSGVO**. Demnach ist die Verarbeitung zulässig, wenn sie zur Ausübung von Rechten und zur Erfüllung von Pflichten aus dem Arbeitsrecht und dem Recht der sozialen Sicherheit und des Sozialschutzes erforderlich ist. Das deutsche Hinweisgeberschutzgesetz ist dem Arbeits- und Sozialschutzrecht zuzuordnen. Die Verarbeitung potenziell enthaltener besonderer Datenkategorien ist zur Erfüllung der gesetzlichen Pflichten aus dem HinSchG (Prüfung der Meldung, Ergreifen von Folgemaßnahmen) erforderlich und somit zulässig.

3.4 Datenübermittlungen

3.4.1 Französische Muttergesellschaft

Die französische Muttergesellschaft ist, wie unter 3.1 dargelegt, **gemeinsam Verantwortliche**. Zwischen der deutschen Tochter- und der französischen Muttergesellschaft muss daher ein **Vertrag über die gemeinsame Verantwortlichkeit (Joint Controller Agreement, JCA)** gemäß Art. 26 DSGVO geschlossen werden. Dieser Vertrag muss transparent festlegen, wer welche datenschutzrechtlichen Pflichten erfüllt. Da Frankreich Mitglied der EU ist, handelt es sich **nicht um einen Datenexport** in ein Drittland; es sind keine besonderen Garantien nach Art. 44 ff. DSGVO erforderlich. Die Rechtsgrundlage für die Übermittlung ergibt sich aus der gemeinsamen Verarbeitungstätigkeit, die auf Art. 6 Abs. 1 lit. c und f DSGVO gestützt ist.

3.4.2 Externe Berater (z.B. Rechtsanwälte)

Externe Berufsgeheimnisträger wie Rechtsanwälte oder Wirtschaftsprüfer handeln bei der Inanspruchnahme ihrer Fachexpertise in der Regel als **eigenständige Verantwortliche**. Sie unterliegen eigenen berufsrechtlichen Pflichten und sind nicht weisungsgebunden. Ein Auftragsverarbeitungsvertrag ist daher nicht erforderlich. Da die Berater ihren Sitz in der EU haben, liegt **kein Datenexport** vor. Die Übermittlung an sie ist durch das **berechtigte Interesse** (Art. 6 Abs. 1 lit. f DSGVO) an der Einholung von Fachexpertise zur Aufklärung eines Sachverhalts oder zur Verteidigung von Rechtsansprüchen gerechtfertigt. Werden besondere Datenkategorien übermittelt, stützt sich dies auf die Notwendigkeit zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen (Art. 9 Abs. 2 lit. f DSGVO).

3.4.3 Behörden (z.B. Strafverfolgungsbehörden)

Behörden handeln bei der Erfüllung ihrer gesetzlichen Aufgaben ebenfalls als **eigenständige Verantwortliche**. Ein Vertrag ist nicht erforderlich. Da es sich um deutsche Behörden handelt, liegt **kein Datenexport** vor. Die Übermittlung an Behörden kann auf einer **rechtlichen Verpflichtung** (Art. 6 Abs. 1 lit. c DSGVO), z.B. einer gesetzlichen Meldepflicht, oder auf dem **berechtigten Interesse** (Art. 6 Abs. 1 lit. f DSGVO) an der Erstattung einer Strafanzeige beruhen. Bei der Übermittlung besonderer Datenkategorien greifen die Ausnahmen nach Art. 9 Abs. 2 lit. f (Rechtsansprüche) oder lit. g (erhebliches öffentliches Interesse) DSGVO.

Eine Zusammenfassung ist in Anhang E (Übersicht Bewertung Datenübermittlungen) enthalten.

3.5 Löschregeln

Die Aufbewahrung und Löschung der Daten richtet sich nach dem Zweck und den gesetzlichen Vorgaben.

Gemäß § 11 Abs. 5 HinSchG ist die Dokumentation zu einer Meldung **drei Jahre nach Abschluss des Verfahrens** zu löschen. Diese Regel gilt für alle fallbezogenen Daten, d.h. für die **Identifikations- und Kontaktdaten (Datenart 1)**, die **Inhaltsdaten der Meldung (Datenart 2)** und die **Daten zur Fallbearbeitung (Datenart 3)**.

Die **Nutzungsdaten des Systems (Datenart 4)**, die zur Gewährleistung der IT-Sicherheit verarbeitet werden (z.B. allgemeine Server-Logfiles), unterliegen nicht dieser spezifischen Frist. Sie sind zu löschen, wenn sie für den Sicherheitszweck nicht mehr erforderlich sind. Eine Regelfrist von **sechs Monaten** ist hierfür angemessen, sofern kein Sicherheitsvorfall eine längere Aufbewahrung zur Analyse erfordert.

Eine Zusammenfassung ist in Anhang F (Übersicht Löschregeln) enthalten.

3.6 Transparenz

Alle von der Datenverarbeitung betroffenen Personengruppen – Hinweisgeber, beschuldigte Personen sowie im Sachverhalt genannte Dritte (z.B. Zeugen) – müssen über die Verarbeitung ihrer Daten informiert werden.

Die Information muss die Anforderungen der Art. 13 und 14 DSGVO erfüllen. Für **Hinweisgeber** sollten die Informationen nach Art. 13 DSGVO direkt auf der Meldeplattform vor Abgabe der Meldung zugänglich sein. **Beschuldigte Personen und sonstige Dritte**, deren Daten nicht direkt bei ihnen, sondern durch die Meldung erhoben werden, sind gemäß Art. 14 DSGVO zu informieren. Diese Information hat grundsätzlich innerhalb eines Monats zu erfolgen. Gemäß § 17 Abs. 2 HinSchG darf die Information an die beschuldigte Person jedoch so lange aufgeschoben werden, wie die Gefährdung der Untersuchung des gemeldeten Verstoßes zu befürchten ist.

4. Empfehlungen und nächste Schritte

Auf Basis der Analyse ergeben sich folgende Handlungsempfehlungen:

5. **Vertrag für gemeinsame Verantwortlichkeit (JCA) abschließen:** Mit der französischen Muttergesellschaft muss ein Vertrag nach Art. 26 DSGVO geschlossen werden. Dieser muss die Verantwortlichkeiten beider Parteien klar regeln, insbesondere wer die Informationspflichten gegenüber den Betroffenen erfüllt und wer als Anlaufstelle für Betroffenenrechte dient.
6. **Datenschutzhinweise erstellen und bereitstellen:** Es müssen umfassende Datenschutzhinweise gemäß Art. 13 und 14 DSGVO erstellt werden. Diese müssen alle Betroffenengruppen (Hinweisgeber, Beschuldigte, Dritte) adressieren und an den entsprechenden Stellen (z.B. auf der Meldeplattform, im Rahmen der internen Kommunikation) bereitgestellt werden.
7. **Löschkonzept implementieren:** Es muss ein technischer und organisatorischer Prozess sichergestellt werden, der die fristgerechte Löschung der Daten gemäß den in Ziffer 3.5 definierten Regeln gewährleistet. Insbesondere muss der "Abschluss des Verfahrens" klar definiert und dokumentiert werden, um den Beginn der dreijährigen Aufbewahrungsfrist auszulösen.

5. Anhänge

5.1 Anhang A: Datentabelle

Lfd. Nr.	Datenart	Dateninhalte (Beispiele)	Betroffenengruppen	Datenquelle
1	**Identifikations- und Kontaktdaten**	Name, Kontaktdaten (falls nicht anonym), Funktion/Position im Unternehmen	• Hinweisgeber • Beschuldigte Personen • Sonstige im	• Hinweisgeber • Interne Systeme (z.B. HR-Verzeichnis)

			Sachverhalt genannte Personen (z.B. Zeugen)	
2	**Inhaltsdaten der Meldung**	Inhalt der Meldung (Text, Dokumente), Beschreibung des Vorfalls. Dies kann auch *besondere Kategorien personenbezogener Daten* [^15] umfassen.	• Hinweisgeber • Beschuldigte Personen • Sonstige im Sachverhalt genannte Personen	Hinweisgeber
3	**Daten zur Fallbearbeitung und Untersuchung**	Untersuchungsprotokolle, Kommunikationsverläufe, Ergebnis der Untersuchung, ergriffene Folgemaßnahmen	• Beschuldigte Personen • Sonstige im Sachverhalt genannte Personen	Werden im Rahmen der internen Untersuchung erzeugt und erhoben
4	**Nutzungsdaten des Systems**	Log-Daten über den Zugriff auf Meldungen (wer, wann), IP-Adresse (falls technisch erfasst und nicht anonymisiert)	• Hinweisgeber • Bearbeitende Personen (Mitarbeiter in Compliance/HR)	Hinweisgebersystem

[^15]: Diese Daten werden nicht gezielt abgefragt, können aber Teil einer Meldung sein, z.B. Angaben zur Gesundheit, ethnischer Herkunft, politischer Meinung, Religion, sexueller Orientierung oder Gewerkschaftszugehörigkeit.

5.2 Anhang B: Daten-Zweck-Matrix

Datenart	**A. Betrieb & Entgegennahme**	**B. Prüfung & Folgemaßnahmen**	**C. IT-Sicherheit**
1. Identifikations- und Kontaktdaten	X	X	
2. Inhaltsdaten der Meldung	X	X	
3. Daten zur Fallbearbeitung		X	
4. Nutzungsdaten des Systems	X		X

5.3 Anhang C: Datenempfänger

Lfd. Nr.	**Datenempfänger**	**Land**	**Zwecke/Beschreibung**	**Übermittelte Datenarten (Nr. aus Datentabelle)**
1	**Französische Muttergesellschaft**	Frankreich	Eure Muttergesellschaft ist als Mitverantwortliche die primäre Empfängerin der Meldung. Eine Rückübermittlung von	1, 2, 3, 4

			Daten von euch (z.B. Untersuchungsergebnisse) kann zur Koordination oder für das konzernweite Reporting erfolgen.	
2	**Externe Berater** (z.B. Rechtsanwälte, Wirtschaftsprüfer)	Deutschland / EU	Einholung von Rechtsrat, Unterstützung bei oder Durchführung von internen Untersuchungen, wenn dies zur Aufklärung des Sachverhalts erforderlich ist.	1, 2, 3
3	**Behörden** (z.B. Strafverfolgungsbehörden , Aufsichtsbehörden)	Deutschland	Erfüllung gesetzlicher Meldepflichten oder Erstattung einer Strafanzeige, wenn der gemeldete Vorfall dies erfordert.	1, 2, 3

5.4 Anhang D: Übersicht Rechtsgrundlagen

Datenart	**A. Betrieb & Entgegennahme**	**B. Prüfung & Folgemaßnahmen**	**C. IT-Sicherheit**
1. Identifikations- und Kontaktdaten	Rechtliche Pflicht	Rechtliche Pflicht, Berechtigtes Interesse	n/a
2. Inhaltsdaten der Meldung	Rechtliche Pflicht	Rechtliche Pflicht, Berechtigtes Interesse	n/a
3. Daten zur Fallbearbeitung	n/a	Rechtliche Pflicht, Berechtigtes Interesse	n/a
4. Nutzungsdaten des Systems	Rechtliche Pflicht	n/a	Berechtigtes Interesse

5.5 Anhang E: Übersicht Bewertung Datenübermittlungen

Lfd. Nr.	**Datenempfänger**	**Land**	**Rolle**	**Verträge**	**Datenexport**	**Rechtsgrundlage der Übermittlung**
1	**Französische Muttergesellschaft**	Frankreich	Gemeinsam Verantwortlicher	JCA	Nein	Rechtliche Pflicht / Berechtigtes Interesse
2	**Externe Berater** (z.B. Rechtsanwälte)	Deutschland / EU	Eigenständiger Verantwortlicher	---	Nein	Berechtigtes Interesse
3	**Behörden** (z.B. Strafverfolgungsbehörden)	Deutschland	Eigenständiger	---	Nein	Rechtliche Pflicht /

			Verantwortlicher			Berechtigtes Interesse

5.6 Anhang F: Übersicht Löschregeln

Datenart	**A. Betrieb & Entgegennahme**	**B. Prüfung & Folgemaßnahmen**	**C. IT-Sicherheit**
1. Identifikations- und Kontaktdaten	3 Jahre nach Abschluss	3 Jahre nach Abschluss	n/a
2. Inhaltsdaten der Meldung	3 Jahre nach Abschluss	3 Jahre nach Abschluss	n/a
3. Daten zur Fallbearbeitung	n/a	3 Jahre nach Abschluss	n/a
4. Nutzungsdaten des Systems	3 Jahre nach Abschluss	n/a	6 Monate nach Erhebung