Datenschutzkonzept für Interne Ermittlungen bei Compliance-Verstößen

Inhaltsübersicht

1. Gegenstand und Vorbehalt

Das vorliegende Datenschutzkonzept betrifft die Durchführung von internen Ermittlungen bei Compliance-Verstößen und wurde von einer KI erstellt. Es fasst den wesentlichen Sachverhalt der Datenverabeitung 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

Dieses Dokument beschreibt die Verarbeitung personenbezogener Daten im Rahmen der Durchführung von internen Ermittlungen bei Verdachtsfällen auf Compliance-Verstöße. Ziel des Prozesses ist die Aufklärung von möglichem Fehlverhalten, die Sicherung von Beweisen und die Vorbereitung eventueller arbeitsrechtlicher oder zivilrechtlicher Maßnahmen.

2.1 Gegenstand

Gegenstand der Datenverarbeitung ist der Prozess "Interne Ermittlungen bei Compliance-Verstößen". Dies umfasst alle Schritte von der Entgegennahme eines Hinweises über die Untersuchung des Sachverhalts bis hin zum Abschluss des Verfahrens. Die Ermittlungen werden nur bei einem konkreten, auf Tatsachen beruhenden Anfangsverdacht eines schwerwiegenden Compliance-Verstoßes (z.B. Straftat, erhebliche Pflichtverletzung) eingeleitet.

2.2 Beteiligte Akteure

An der Datenverarbeitung sind mehrere Akteure beteiligt. Dieses Datenschutzkonzept wird aus der Sicht Ihres Unternehmens erstellt, das die Ermittlungen initiiert und steuert.

- **Ihr Unternehmen:** Es trifft die grundlegende Entscheidung, *ob* eine interne Ermittlung eingeleitet wird, *was* deren Ziel ist und *welche wesentlichen Schritte* unternommen werden. Es behält die Gesamtsteuerung über den Prozess.
- **Anwaltskanzlei:** Eine Kanzlei kann zur rechtlichen Beratung hinzugezogen werden. Sie agiert dabei im Rahmen ihres Mandats eigenständig und ist nicht an Weisungen gebunden, wie sie die Daten zur Erfüllung ihrer anwaltlichen Tätigkeit verarbeitet.
- **IT-Forensik-Spezialist:** Ein externer Spezialist kann für die technische Analyse von Daten beauftragt werden. Ihr Unternehmen gibt ihm genau vor, welche Systeme er nach welchen Kriterien zu durchsuchen hat. Der Spezialist verfolgt keine eigenen Zwecke mit den Daten.

2.3 Verarbeitungsphasen

Der Prozess der Datenverarbeitung lässt sich in mehrere Phasen gliedern:

- **Kollektion / Sammeln:** Die Verarbeitung beginnt mit dem Eingang eines Hinweises auf einen möglichen Compliance-Verstoß. Daten werden aus verschiedenen Quellen gesammelt, darunter Hinweise von internen oder externen Hinweisgebern, Analysen von IT-Systemen des Unternehmens (z.B. E-Mail-Postfächer, Dateiserver), Befragungen von Zeugen und Beschuldigten sowie öffentlich zugängliche Quellen.
- **Bereithaltung und Nutzung:** Die gesammelten Informationen werden ausgewertet, um den Sachverhalt aufzuklären. Die Ergebnisse werden in einer Ermittlungsakte dokumentiert.
- **Beseitigung / Löschen:** Nach Abschluss des Verfahrens und Ablauf relevanter Fristen werden die Daten gelöscht.

2.4 Datenarten und Herkunft

Es werden folgende Datenarten verarbeitet:

1. Identifikations- und Stammdaten
2. Daten zum Tatvorwurf/Sachverhalt
3. Kommunikations- und IT-Nutzungsdaten
4. Sonstige Ermittlungsdaten

Die Daten beziehen sich auf folgende Betroffenengruppen:

- Beschuldigte
- Hinweisgeber
- Zeugen
- Sonstige Betroffene

Die Daten stammen aus diesen Quellen:

- Personaldatensysteme des Unternehmens
- Hinweisgeber, Zeugen, interne Meldungen
- IT-Systeme des Unternehmens (z.B. E-Mail-Server, Dateiserver, Firewalls)
- Interne Befragungen, unternehmensinterne Systeme, öffentlich zugängliche Quellen

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. Aufklärung von Compliance-Verstößen
- B. Geltendmachung und Abwehr von Rechtsansprüchen
- C. Erfüllung rechtlicher Pflichten
- D. Dokumentation und Nachweisbarkeit

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 werden an diese Empfänger weitergegeben:

- Anwaltskanzlei (Deutschland)
- IT-Forensik-Spezialist (USA)
- Behörden und Gerichte (Deutschland)

Für die Bewertung der Datenübermittlung in die USA wird davon ausgegangen, dass der IT-Forensik-Spezialist nicht nach dem "EU-U.S. Data Privacy Framework" (DPF) zertifiziert ist.

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

3. Bewertung

3.1 Datenschutzechtliche Rollen

Die datenschutzrechtlichen Rollen der beteiligten Akteure werden wie folgt bewertet:

- **Ihr Unternehmen** ist **Verantwortlicher** gemäß Art. 4 Nr. 7 DSGVO.
- Die **Anwaltskanzlei** ist **eigenständige Verantwortliche**.
- Der **IT-Forensik-Spezialist** ist **Auftragsverarbeiter** für Ihr Unternehmen gemäß Art. 4 Nr. 8, Art. 28 DSGVO.

Begründung: Ihr Unternehmen ist als Verantwortlicher einzustufen, da es allein über die Zwecke (Warum wird ermittelt?) und die wesentlichen Mittel (Welche Schritte werden unternommen?) der Datenverarbeitung entscheidet. Es initiiert und steuert den gesamten Ermittlungsprozess.

Die Anwaltskanzlei ist als Berufsgeheimnisträgerin bei der Erbringung ihrer Rechtsberatung nicht an die Weisungen Ihres Unternehmens gebunden, wie sie die Daten zur Erfüllung ihres Mandats verarbeitet. Sie legt die Zwecke und Mittel ihrer eigenen Tätigkeit selbst fest und ist daher als eigenständige Verantwortliche anzusehen.

Der IT-Forensik-Spezialist hingegen handelt ausschließlich im Auftrag und nach den dokumentierten Weisungen Ihres Unternehmens. Er hat keinen eigenen Ermessensspielraum bezüglich der Zwecke der Verarbeitung und verfolgt keine eigenen Interessen an den Daten. Seine Tätigkeit beschränkt sich auf die technische Umsetzung der vorgegebenen Analyse, was ihn klar als Auftragsverarbeiter qualifiziert.

3.2 Rechtsgrundlagen

Die Verarbeitung der personenbezogenen Daten stützt sich auf verschiedene Rechtsgrundlagen, je nach Zweck der Verarbeitung.

Für den Zweck der **Aufklärung von Compliance-Verstößen (A)** kommen mehrere Rechtsgrundlagen in Betracht. Primär ist dies **§ 26 Abs. 1 S. 2 BDSG**, wenn es um die Aufdeckung von Straftaten durch Beschäftigte geht und ein auf Tatsachen beruhender Verdacht vorliegt. Ergänzend kann die Verarbeitung auf das **berechtigte Interesse** Ihres Unternehmens gemäß **Art. 6 Abs. 1 lit. f DSGVO** gestützt werden. Dieses Interesse besteht in der Aufklärung von schwerwiegenden Pflichtverletzungen (auch unterhalb der Schwelle einer Straftat) und der Abwehr von Schäden. Diese Rechtsgrundlage ist insbesondere dann relevant, wenn Nicht-Beschäftigte betroffen sind. Sofern ein Gesetz die Untersuchung eines Vorfalls vorschreibt (z.B. nach dem Geldwäschegesetz), kann die Verarbeitung auch zur Erfüllung einer **rechtlichen Verpflichtung** nach **Art. 6 Abs. 1 lit. c DSGVO** erforderlich sein.

Die Verarbeitung zum Zweck der **Geltendmachung und Abwehr von Rechtsansprüchen (B)** sowie zur **Dokumentation und Nachweisbarkeit (D)** ist zur Wahrung der **berechtigten Interessen** Ihres Unternehmens gemäß **Art. 6 Abs. 1 lit. f DSGVO** erforderlich. Das Interesse an der Durchsetzung von Ansprüchen (z.B. Kündigung, Schadensersatz) und an einer lückenlosen Dokumentation für spätere Verfahren überwiegt in der Regel die Interessen der Betroffenen, sofern die Ermittlung anlassbezogen und verhältnismäßig erfolgt.

Soweit Daten zur **Erfüllung rechtlicher Pflichten (C)** an Behörden übermittelt werden, ist die Rechtsgrundlage **Art. 6 Abs. 1 lit. c DSGVO**.

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

3.3 Datenübermittlungen

3.3.1 Anwaltskanzlei

Die Anwaltskanzlei agiert als **eigenständige Verantwortliche**. Da sie ihre Tätigkeit als Berufsgeheimnisträgerin eigenverantwortlich ausübt, ist kein Auftragsverarbeitungsvertrag oder Vertrag über eine gemeinsame Verantwortlichkeit erforderlich. Die Übermittlung der Daten an die Kanzlei stützt sich auf das **berechtigte Interesse** Ihres Unternehmens an der Einholung von Rechtsrat und der Vorbereitung von Rechtsansprüchen (Art. 6 Abs. 1 lit. f DSGVO). Da die Kanzlei ihren Sitz in Deutschland hat, unterliegt die Übermittlung **keinen besonderen Anforderungen** für einen Datenexport.

3.3.2 IT-Forensik-Spezialist

Der IT-Forensik-Spezialist ist als **Auftragsverarbeiter** tätig. Die Übermittlung an ihn wird durch den Abschluss eines **Auftragsverarbeitungsvertrags (AVV)** nach Art. 28 DSGVO legitimiert. Da der Dienstleister seinen Sitz in den USA hat, einem Drittland ohne allgemeinen Angemessenheitsbeschluss, unterliegt die Übermittlung besonderen Anforderungen. Es müssen die **EU-Standardvertragsklauseln (SCC)** abgeschlossen werden. Das Modul 2 der SCC (für die Übermittlung an einen Auftragsverarbeiter) erfüllt dabei bereits die Anforderungen eines

AVV. Zusätzlich muss ein **Transfer Impact Assessment (TIA)** durchgeführt und dokumentiert werden, um zu prüfen, ob die SCC im US-Rechtsumfeld wirksam eingehalten werden können.

3.3.3 Behörden und Gerichte

Behörden und Gerichte sind **eigenständige Verantwortliche**. Eine vertragliche Regelung ist nicht erforderlich. Die Übermittlung erfolgt entweder zur Erfüllung einer **rechtlichen Verpflichtung** (Art. 6 Abs. 1 lit. c DSGVO), z.B. bei einer Strafanzeige, oder zur Wahrung Ihres **berechtigten Interesses** an der Geltendmachung oder Verteidigung von Rechtsansprüchen (Art. 6 Abs. 1 lit. f DSGVO). Da die Empfänger ihren Sitz in Deutschland haben, gelten **keine besonderen Anforderungen** für einen Datenexport.

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

3.4 Löschregeln

Die im Rahmen der Ermittlungen verarbeiteten Daten sind zu löschen, sobald sie für die Zwecke, für die sie erhoben wurden, nicht mehr erforderlich sind (Art. 17 Abs. 1 lit. a DSGVO).

Dies führt zu einer differenzierten Löschfrist: Stellt sich im Laufe der Ermittlungen heraus, dass der Verdacht unbegründet war, sind die Daten unverzüglich nach Abschluss der Ermittlungen zu löschen.

Wird ein Compliance-Verstoß festgestellt, müssen die Daten aufbewahrt werden, solange sie für daraus resultierende Maßnahmen (z.B. arbeitsrechtliche Schritte, Geltendmachung von Schadensersatz) oder zur Verteidigung gegen Ansprüche (z.B. Kündigungsschutzklage) benötigt werden. Maßgeblich sind hier die jeweiligen Verjährungsfristen. In der Regel ist von der allgemeinen zivilrechtlichen Verjährungsfrist von drei Jahren nach § 195 BGB auszugehen. Die Frist beginnt mit dem Schluss des Jahres, in dem der Anspruch entstanden ist und der Gläubiger Kenntnis von den anspruchsbegründenden Umständen erlangt hat. Die Ermittlungsakte ist daher in diesen Fällen drei Jahre nach Abschluss des Verfahrens zu löschen.

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

3.5 Transparenz

Grundsätzlich sind die betroffenen Personen (insbesondere Beschuldigte) über die Verarbeitung ihrer Daten zu informieren (Art. 13, 14 DSGVO). Bei internen Ermittlungen kann die Informationspflicht jedoch aufgeschoben werden, solange die Gefahr besteht, dass eine vorzeitige Information den Untersuchungszweck gefährden würde (Art. 14 Abs. 5 lit. b DSGVO, § 33 Abs. 1 Nr. 2 BDSG).

Sobald diese Gefahr nicht mehr besteht, spätestens jedoch bei Abschluss der Ermittlungen, muss die Information nachgeholt werden. Die Information muss den gesamten Umfang der Datenverarbeitung umfassen, einschließlich der Rechtsgrundlagen, Empfänger und der Rechte der betroffenen Person.

4. Empfehlungen und nächste Schritte

Auf Basis der Analyse ergeben sich folgende Handlungsempfehlungen:

- **Vertragsmanagement:** Schließen Sie mit dem IT-Forensik-Spezialisten in den USA die EU-Standardvertragsklauseln (Modul 2) ab.
- **Datenexport in die USA:** Führen Sie für die Übermittlung an den IT-Forensik-Spezialisten ein Transfer Impact Assessment (TIA) durch und dokumentieren Sie dieses sorgfältig.

Prüfen Sie, ob der Anbieter alternativ nach dem EU-U.S. Data Privacy Framework zertifiziert ist, was die Übermittlung erleichtern würde.

- **Prozessdokumentation:** Stellen Sie sicher, dass der Anlass und die wesentlichen Schritte jeder internen Ermittlung sorgfältig dokumentiert werden, um den Anfangsverdacht und die Verhältnismäßigkeit der Maßnahmen nachweisen zu können.
- **Erstellung von Datenschutzhinweisen:** Entwerfen Sie Datenschutzhinweise gemäß Art. 14 DSGVO, die den Betroffenen (insbesondere Beschuldigten) nach Abschluss der Ermittlungen oder Wegfall der Gefährdung des Untersuchungszwecks zur Verfügung gestellt werden.
- **Einzelfallprüfung:** Jede interne Ermittlung erfordert eine sorgfältige Prüfung der Verhältnismäßigkeit im Einzelfall. Insbesondere die Analyse von Kommunikationsdaten (z.B. E-Mails) stellt einen erheblichen Eingriff dar und muss gut begründet sein.

5. Anhänge

5.1 Anhang A: Datentabelle

Lfd. Nr.	Datenart	Dateninhalte (Beispiele)	Betroffenengruppen	Datenquelle
1	**Identifikations- und Stammdaten**	Name, Personalnummer, Abteilung, Position/Funktion, dienstliche Kontaktdaten (E-Mail, Telefon)	Beschuldigte, Hinweisgeber, Zeugen, Sonstige Betroffene	Personaldatensysteme des Unternehmens
2	**Daten zum Tatvorwurf/Sachverhalt**	Schilderungen des Sachverhalts, Zeitpunkt und Ort des Vorfalls, beteiligte Personen, eingereichte Unterlagen/Beweismittel	Beschuldigte, Hinweisgeber, Zeugen	Hinweisgeber, Zeugen, interne Meldungen
3	**Kommunikations- und IT-Nutzungsdaten**	Inhalte und Metadaten von dienstlichen E-Mails und Chats, Protokolldaten von IT-Systemen (Logfiles), Browserverläufe, Zugriffsdaten auf Dateien/Server	Beschuldigte, Sonstige Betroffene (als Kommunikationspartner)	IT-Systeme des Unternehmens (z.B. E-Mail-Server, Dateiserver, Firewalls)
4	**Sonstige Ermittlungsdaten**	Ergebnisse aus Befragungen/Interviews, Notizen der Ermittler, ggf. Daten aus anderen Systemen (z.B. Zeiterfassung, Zutrittskontrolle,	Beschuldigte, Zeugen, Sonstige Betroffene	Interne Befragungen, unternehmensinterne Systeme, öffentlich zugängliche Quellen

		Finanzbuchhaltung), Informationen aus öffentlichen Quellen		

5.2 Anhang B: Daten-Zweck-Matrix

Datenart	A. Aufklärung	B. Rechtsansprüche	C. Rechtl. Pflichten	D. Dokumentation
1. Identifikations- und Stammdaten	X	X	X	X
2. Daten zum Tatvorwurf/Sachverhalt	X	X	X	X
3. Kommunikations- und IT-Nutzungsdaten	X	X		X
4. Sonstige Ermittlungsdaten	X	X	X	X

5.3 Anhang C: Datenempfänger

Datenempfänger	Land	Zwecke/Beschreibung	Daten
1. Anwaltskanzlei	Deutschland	Rechtliche Beratung zum Sachverhalt, Bewertung der Rechtslage und Vorbereitung rechtlicher Schritte (z.B. Kündigung, Schadensersatz).	Alle Datenarten (1-4), soweit für das Mandat erforderlich.
2. IT-Forensik-Spezialist	USA	Technische Analyse von IT-Systemen, Sicherung und Auswertung von digitalen Spuren zur Aufklärung des Sachverhalts (im Auftrag).	Identifikationsdaten (1), Daten zum Sachverhalt (2), Kommunikations- und IT-Nutzungsdaten (3).
3. Behörden und Gerichte	Deutschland	Erfüllung rechtlicher Pflichten (z.B. Strafanzeige bei der Staatsanwaltschaft) oder zur Geltendmachung und Verteidigung von Rechtsansprüchen (z.B. bei einem Arbeitsgerichtsprozess).	Alle Datenarten (1-4), soweit für das jeweilige Verfahren relevant und erforderlich.

5.4 Anhang D: Übersicht Rechtsgrundlagen

Datenart	A. Aufklärung	B. Rechtsansprüche	C. Rechtl. Pflichten	D. Dokumentation

1. Identifikations- und Stammdaten	§ 26 (1) S. 2 BDSG / Art. 6 (1) f / c DSGVO	Art. 6 (1) f DSGVO	Art. 6 (1) c DSGVO	Art. 6 (1) f DSGVO
2. Daten zum Tatvorwurf/Sachverhalt	§ 26 (1) S. 2 BDSG / Art. 6 (1) f / c DSGVO	Art. 6 (1) f DSGVO	Art. 6 (1) c DSGVO	Art. 6 (1) f DSGVO
3. Kommunikations- und IT-Nutzungsdaten	§ 26 (1) S. 2 BDSG / Art. 6 (1) f / c DSGVO	Art. 6 (1) f DSGVO	n/a	Art. 6 (1) f DSGVO
4. Sonstige Ermittlungsdaten	§ 26 (1) S. 2 BDSG / Art. 6 (1) f / c DSGVO	Art. 6 (1) f DSGVO	Art. 6 (1) c DSGVO	Art. 6 (1) f DSGVO

5.5 Anhang E: Übersicht Bewertung Datenübermittlungen

Datenempfänger	**Land**	**Rolle**	**Verträge**	**Datenexport**	**Rechtsgrundlage (Übermittlung)**
1. Anwaltskanzlei	Deutschland	Eigenständige Verantwortliche	---	Keine	Art. 6 (1) f DSGVO
2. IT-Forensik-Spezialist	USA	Auftragsverarbeiter	AVV / SCC	SCC + TIA	Vertrag (AVV/SCC)
3. Behörden und Gerichte	Deutschland	Eigenständige Verantwortliche	---	Keine	Art. 6 (1) c oder f DSGVO

5.6 Anhang F: Übersicht Löschregeln

Datenart	**A. Aufklärung**	**B. Rechtsansprüche**	**C. Rechtl. Pflichten**	**D. Dokumentation**
1. Identifikations- und Stammdaten	3 Jahre nach Abschluss	3 Jahre nach Abschluss	3 Jahre nach Abschluss	3 Jahre nach Abschluss
2. Daten zum Tatvorwurf/Sachverhalt	3 Jahre nach Abschluss	3 Jahre nach Abschluss	3 Jahre nach Abschluss	3 Jahre nach Abschluss
3. Kommunikations- und IT-Nutzungsdaten	3 Jahre nach Abschluss	3 Jahre nach Abschluss	n/a	3 Jahre nach Abschluss
4. Sonstige Ermittlungsdaten	3 Jahre nach Abschluss	3 Jahre nach Abschluss	3 Jahre nach Abschluss	3 Jahre nach Abschluss