Datenschutz-Folgeabschätzung

Verantwortlicher: FortSchritt Würzburg gemeinnützige GmbH
Friedrich-Bergius-Ring 44
97076 Würzburg
E-Mail: info@fortschritt-wuerzburg.net

und

Leu Rechtsanwaltsgesellschaft mbH
Heinrich-Hoffmann-Straße 3
60528 Frankfurt am Main
E-Mail: datenschutz@kanzlei-leu.de

Stand: 29. Dezember 2023

Bearbeiter: Franz Philippe Bachmann (Kanzlei Leu)

Inhaltsverzeichnis

Änderungen dieses Dokuments

Revision	Datum	Änderung	Geändert durch
1	29.12.2023	Erstellung	F. Ph. Bachmann

I. Erforderlichkeit der Datenschutz-Folgeabschätzung

Gemäß der „Orientierungshilfe der Datenschutzaufsichtsbehörden zu Whistleblowing-Hotlines: Firmeninterne Warnsysteme und Beschäftigtendatenschutz“ vom 14. November 2018 erfordert ein Hinweisgeberkanal eine Datenschutz-Folgeabschätzung: „Ein Verfahren zur Meldung von

Missständen unterliegt wegen des besonders hohen Risikos für die Rechte und Freiheiten natürlicher Personen einer Datenschutz-Folgenabschätzung.“ (a.a.O., Abschnitt E9).

Diese Sichtweise wird durch die Praxis beispielsweise der italienischen Aufsichtsbehörde *Garante per la protezione dei dati personali (GPDP)* bestätigt: *Ordinanza ingiunzione nei confronti di Aeroporto Guglielmo Marconi di Bologna S.p.a. - 10 giugno 2021 [9685922]*. Sie stellte fest, dass das besagte Unternehmen eine Erhebung und Verarbeitung personenbezogener Daten für einen Hinweisgeberkanal durchgeführt hat, ohne entsprechend Art. 32 DSGVO eine Datenschutz-Folgeabschätzung durchgeführt zu haben und somit einen Verstoß begangen hat.

Sachlich besteht ein hohes Risiko für die Rechte und Freiheiten derjenigen natürlichen Personen, die in einer Meldung als eine Person bezeichnet werden, die einen im Sinne der Richtlinie (EU) 2019/1937 („Whistleblower-Richtlinie“, in Folge: „WBRL“) relevanten Verstoß begangen hat oder mit einer solchen Person verbunden ist. Analog verweisen wir hierzu auf § 1 Abs. 1 Hinweisgeberschutzgesetz (in Folge: „HinSchG). Dazu sind auch solche natürlichen Personen zu rechnen, die durch ihre Tätigkeit zum Beispiel in einer Organfunktion den Verstoß einer juristischen Person ermöglicht haben. Eine Meldung wird in der Regel ohne Kenntnis einer insofern betroffenen Person abgegeben, und sie kann ihre berufliche Stellung und persönliche Lebenssituation erheblich beeinträchtigen, zum Beispiel durch Haftung für tatsächlich von ihr begangene oder ermöglichte Verstöße. Es ist auch möglich, dass eine solche Person irrtümlich oder absichtlich unbegründet beschuldigt wird und damit ihrem Ansehen geschadet wird. Für die Dauer, in der sie von der Meldung keine Kenntnis hat, kann sie ihre Rechte nicht verteidigen.

II. Beschreibung der Datenverarbeitung

1. Zweck der Datenverarbeitung

Der Hinweisgeberkanal ermöglicht einem Hinweisgeber, der Organisation auf einem der dafür eingerichteten Meldekanäle Informationen über mögliche Verstöße gegen Unionsrecht hinsichtlich einem der in Art. 2 Abs. 1 WBRL genannten Bereiche zukommen zu lassen. Das sind unter anderem: Öffentliches Auftragswesen; Finanzdienstleistungen, Finanzprodukte und Finanzmärkte sowie Verhinderung von Geldwäsche und Terrorismusfinanzierung; Produktsicherheit und -konformität; Verkehrssicherheit; Umweltschutz; Strahlenschutz und kerntechnische Sicherheit; Lebensmittel- und Futtermittelsicherheit, Tiergesundheit und Tierschutz; öffentliche Gesundheit; Verbraucherschutz; Schutz der Privatsphäre und personenbezogener Daten sowie Sicherheit von Netz- und Informationssystemen; Wettbewerb und staatliche Beihilfen. Der deutsche Gesetzgeber hat diesen Katalog im Rahmen seiner Befugnis aus Art. 2 Abs. 2 WBRL auch auf nationale Rechtsverstöße ausgeweitet. Diese Ausweitung umfasst gemäß § 2 Abs. 1 HinSchG strafbewehrte Verstöße, bußgeldbewehrte Verstöße (soweit die verletzte Vorschrift dem Schutz von Leben, Leib oder Gesundheit oder dem Schutz der Rechte von Beschäftigten oder Ihrer Vertretungsorgane dient) und sonstige Verstöße gegen Rechtsvorschriften des Bundes und der Länder sowie unmittelbar geltende Rechtsakte der Europäischen Union.

Die personenbezogenen Daten der Hinweisgeber, von Beschäftigten und weiteren betroffenen Personen werden zur Ermittlung des Sachverhalts, der Klärung der Vorwürfe und der eventuell erforderlichen Abstellung von Fehlverhalten verarbeitet. Im Falle der Beschäftigten dient die Datenverarbeitung darüber hinaus der Aufdeckung von Straftaten, wenn eine Meldung tatsächliche Anhaltspunkte enthält, die den Verdacht begründen, dass eine Mitarbeiterin oder ein Mitarbeiter

eine Straftat begangen hat, die Verarbeitung zur Aufdeckung erforderlich ist und das schutzwürdige Interesse der Betroffenen nicht überwiegt (§ 26 Abs. 1 S. 2 BDSG).

2. Gemeinsame Verantwortlichkeit der Organisation und der Ombudsstelle

Datenschutzrechtlich sind die Organisation und die Ombudsstelle gemeinsam Verantwortliche (Art. 26 DSGVO). Daher wurden in der betreffenden Vereinbarung die jeweiligen Wirkbereiche festgelegt und die gemeinsamen und getrennten Verantwortlichkeiten geregelt. Darin ist auch die gegenseitige Unterstützung bei einer Datenschutz-Folgeabschätzung vereinbart.

3. Personenkreis, dessen Daten verarbeitet werden, und ihre Schutzbedürftigkeit

Es werden im Rahmen der betrachteten Prozesse die Daten von drei Personengruppen verarbeitet: (a) Hinweisgeberinnen und Hinweisgeber, das heißt die meldenden Personen; (b) Mitarbeiterinnen und Mitarbeiter in einer Organisation, die mit Ihren Verhalten möglicherweise gegen Regeln verstoßen haben; (c) weitere Personen im Zusammenhang mit dem gemeldeten Sachverhalt. Die Schutzbedürftigkeit der Personengruppen erklärt sich wie folgend:

(a) Die Hinweisgeber*innen unterstehen einem gesetzlichen Schutz, um Repressalien gegen sie zu verhindern. Darunter werden “direkte oder indirekte Handlungen oder Unterlassungen in einem beruflichen Kontext, die durch eine interne oder externe Meldung oder eine Offenlegung ausgelöst werden und durch die dem Hinweisgeber ein ungerechtfertigter Nachteil entsteht oder entstehen kann“ (Art. 5 Nr. 11 WBRL/ § 3 Abs. 6 HinSchG). Hinweisgeber setzen sich einem erheblichen persönlichen Risiko aus, wenn sie identifiziert oder identifizierbar sind, und zumindest das Letztere ist immer anzunehmen.

(b) Die in einer Meldung genannten Mitarbeiterinnen und Mitarbeiter können irrtümlich oder absichtlich mit einem möglichen Verstoß in Verbindung gebracht werden. Die Meldung des Verstoßes kann sogar selbst einen Verstoß zum Schaden der Mitarbeiterinnen und Mitarbeiter darstellen, der darüber hinaus strafrechtlich relevant sein kann, zum Beispiel als Beleidigung (§ 185 StGB), Üble Nachrede (§ 186 StGB) oder Verleumdung (§ 187 StGB). Dadurch besteht für sie ein bedeutendes persönliches Risiko (siehe Abschnitt I oben). Sie müssen daher vor den durch sie nicht zu verantwortenden Folgen der Meldung geschützt werden.

(c) Das für (b) Gesagte gilt auch für die weiteren Personen, deren Daten im Zusammenhang mit dem gemeldeten Sachverhalt verarbeitet werden, zum Beispiel weil sie als mögliche Zeugen durch den Hinweisgeber benannt werden. Darüber können sie durch den Verstoß auch geschädigt worden sein, beispielsweise als Opfer eines Übergriffs oder eines grenzverletzenden Verhaltens. Dadurch können sie auch zu einer besonders vulnerablen Personengruppe werden.

Es werden keine Daten von Personen verarbeitet, die keinen Anlass für ihre Speicherung gegeben haben oder für deren Speicherung eine irgendwie geartete Negativprognose erforderlich ist.

4. Verarbeitete Datenarten der betroffenen Personen

Es können folgende Daten der betroffenen Personen erhoben und verarbeitet werden, die hier darüber hinaus grob hinsichtlich ihrer Sensibilität eingestuft werden.

Datenkategorie	Beispiele für Datenarten	Sensibilität
Identität (Hinweisgeber)	Vorname, Name, IP-Adresse	Hoch
Kontaktdaten (Hinweisgeber)	Wohnanschrift, Telefonnummer, E-Mail-Adresse	Hoch
Umstände der Meldung (Hinweisgeber)	Zeitpunkt	Normal
Identität (Beschäftigte, weitere Personen)	Vorname, Name	Hoch
Angaben zur Beschäftigung (Beschäftigte, weitere Personen)	Tätigkeitsbereich	Hoch
Mögliches Fehlverhalten (Beschäftigte)	Beschreibung des Verstoßes und weiterer beteiligter Personen	Hoch (ggf. auch Art. 10 DSGVO)
Inhalt der Meldung (alle Kategorien Betroffener)	ggf. Gesundheitsdaten und andere besondere Kategorien	Hoch (ggf. auch Art. 9 DSGVO)
Ermittelter Sachverhalt (alle Kategorien Betroffener)	ggf. Anhaltspunkte für Straftaten, ggf. besondere Kategorien	Hoch (ggf. auch Art. 9, 10 DSGVO)

Es werden nicht planmäßig besondere Kategorien personenbezogener Daten nach Art. 9 Abs. 1 DSGVO bzw. § 46 Nr. 14 BSDG verarbeitet, aber der Inhalt einer Meldung und der anschließend ermittelte Sachverhalt können solche Daten enthalten. Dasselbe gilt für personenbezogene Daten über strafrechtliche Verurteilungen und Straftaten (Art. 10 DSGVO).

Die personenbezogenen Daten der unter Punkt II.3. genannten betroffenen Personen, werden aufgrund einer rechtlichen Verpflichtung des Verantwortlichen verarbeitet. Diese rechtliche Verpflichtung ergibt sich aus Art. 6 Abs. 1 lit. c DSGVO i.V.m. § 10 HinSchG.

Die Daten werden zur Aufdeckung von Straftaten verarbeitet, wenn die Meldung tatsächliche Anhaltspunkte enthält, die den Verdacht begründen, dass eine Mitarbeiterin oder ein Mitarbeiter eine Straftat begangen hat, die Verarbeitung zur Aufdeckung erforderlich ist und das schutzwürdige Interesse der Betroffenen nicht überwiegt (§ 26 Abs. 1 S. 2 BDSG).

5. Abrufberechtigte Stellen und Übermittlungsempfänger

Die Daten der Betroffenen sind ausschließlich für die folgenden Personengruppen zugänglich:

(a) Geschäftsführung der Organisation und von ihr mit der Ermittlung des Sachverhalts beauftragte Personen;

(b) Beschäftigte der Leu Rechtsanwaltsgesellschaft mbH, die mit dem Betrieb der Meldekanäle, der Prüfung von Meldungen und rechtlichen Beratung der Geschäftsführung der Organisation betraut sind.

Es können fallweise Datenübermittlungen an andere Stellen stattfinden. Dabei kann es sich um externe Rechtsberater, Steuerberater, Wirtschaftsprüfer, Mediziner und andere Sachverständige handeln. Weiterhin können Strafverfolgungsbehörden wie Polizei, Staatsanwaltschaft, Zoll- und Finanzverwaltung involviert werden.

Darüber hinaus kann eine weitere Datenübermittlungen an Dritte durch Auftragsverarbeitung verfolgen (Art. 28 DSGVO). Der Verantwortliche wählt seine Auftragsverarbeiter jedoch sorgfältig aus. Sie müssen nachweislich hinreichend Garantien dafür bieten, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den datenschutzrechtlichen Anforderungen erfolgen und der Schutz der Rechte der betroffenen Personen gewährleistet ist.

6. Speicherdauer, Aussonderungsprüffristen und Löschmechanismen

Die Dokumentation wird drei Jahre nach Abschluss des Verfahrens gelöscht. Die Dokumentation kann länger aufbewahrt werden, um die Anforderungen nach diesem Gesetz oder nach anderen Rechtsvorschriften zu erfüllen, solange dies erforderlich und verhältnismäßig ist (§ 11 Abs. 5 HinSchG).

III. Risiken, deren Bewertung und Schutzmaßnahmen

1. Gesetzliche Schutzziele zur Selektion relevanter Risiken

Relevante Risiken sind solche, die die Ziele des Datenschutzes gefährden, die in der Datenschutz-Grundverordnung (DSGVO) zum Ausdruck kommen: „Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten“ (Art. 1 Abs. 1 DSGVO) und Schutz der „Grundrechte und Grundfreiheiten natürlicher Personen und insbesondere deren Recht auf Schutz personenbezogener Daten“ (Art. 1 Abs. 2 DSGVO). Der Schutz des freien Verkehrs personenbezogener Daten in der Europäischen Union, ebenfalls ein ausdrückliches ein Ziel der DSGVO (Art. 1 Abs. 3 DSGVO), spielt für die hier betrachtete Datenverarbeitung keine Rolle.

2. Identifikation relevanter Risiken durch Experteneinschätzung

Die Risiken wurden vorläufig durch Experteneinschätzung identifiziert, weil zum Zeitpunkt der Erstellung dieser Datenschutz-Folgeabschätzung die Organisation noch keine Erfahrungen mit der Meldung von Verstößen auf den geplanten Meldekanälen hat. Dabei sind auch die Erfahrungen der Ombudsstelle sowie des Datenschutz-Beauftragten der Organisation miteingeflossen und insoweit die gesetzliche Anforderung mit erfüllt: „Der Verantwortliche holt bei der Durchführung einer Datenschutz-Folgenabschätzung den Rat des Datenschutzbeauftragten, sofern ein solcher benannt wurde, ein“ (Art. 35 Abs. 2 DSGVO).

Bei einer Aktualisierung dieser Datenschutz-Folgeabschätzung kann ggf. der Standpunkt der betroffenen Personen oder ihrer Vertreter zu der Verarbeitung personenbezogener Daten (Art. 35 Abs. 9 DSGVO), eingeholt werden. Ein solcher Vertreter ist u.a. ein Betriebsrat, welcher beim Verantwortlichen jedoch nicht installiert ist.

3. Bewertung der Risiken anhand Eintrittswahrscheinlichkeit und Schadensausmaß

Die identifizierten Risiken werden anhand folgender Fragen bewertet:

(a) Eintrittswahrscheinlichkeit (EW): Wie wird die Wahrscheinlichkeit für das Eintreten des möglichen Ereignisses geschätzt? Um eine Pseudogenauigkeit zu vermeiden, wird die Wahrscheinlichkeit qualitativ angegeben: Niedrig ($0\% < EW \leq 25\%$), Mittel ($25\% < EW \leq 75\%$), Hoch ($75\% < EW < 100\%$).

(b) Schadensausmaß (SA): Wie sehr verletzt das Ereignis die Rechte und Freiheiten der von der Datenverarbeitung und dem Ereignis betroffenen Personen? Der Wert hat dieselbe Skala wie die EW: Niedrig, Mittel, Hoch. Da ein Ereignis in der Regel eine Verletzung des Schutzes personenbezogener Daten (Art. 33 DSGVO) sein wird, wird das Schadensausmaß entsprechend der Behandlung einer Datenpanne eingeschätzt. Niedrig: Dokumentationspflichtig (Art. 33 Abs. 5 DSGVO), aber nicht meldepflichtig (Art. 33 Abs. 1 DSGVO); Mittel: Meldepflichtig, aber nicht informationspflichtig (Art. 34 Abs. 1 DSGVO); Hoch: Melde- und informationspflichtig („voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen“, Art. 34 Abs. 1 DSGVO).

(c) Gegenmaßnahmen (GM): Welche technischen und organisatorischen Maßnahmen zur Reduzierung der Eintrittswahrscheinlichkeit und zur Begrenzung des Schadensausmaßes wurden getroffen und wie wird deren Wirksamkeit „Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung“ (Art. 32 Abs. 1 DSGVO) qualitativ eingeschätzt? Die Wirkung ebenfalls anhand der Skala angegeben: Niedrig, Mittel, Hoch.

(d) Restrisiko (RR): Welches Risiko für die Rechte und Freiheiten der von der Datenverarbeitung betroffenen Personen verbleibt? Dazu wird der Schadenserwartungswert durch gedankliche Multiplikation der EW und des SA gebildet und die GM davon abgezogen.

4. Identifizierte Risiken und deren Bewertung (Risikoportfolio)

Nr.	Beschreibung	EW	SA	GM	RR
1	Erfolgreiche Cyberattacke auf gespeicherte Meldungen	Niedrig	Hoch	IT-Grundschutz gemäß BSI-Standard	Mittel
2	Vollständiger oder teilweise Datenverlust auf Meldeplattform	Niedrig	Niedrig	IT-Grundschutz gemäß BSI-Standard; hier: Datensicherung	Niedrig
3	Ausfall der zentralen Datenbank bzw. deren eingeschränkte Verfügbarkeit	Niedrig	Niedrig	Betrieb in einem professionellen, betreuten Rechenzentrum mit redundanten Komponenten	Niedrig
4	Organisatorischer Ausfall der Ombudsstelle und verzögerte Bearbeitung von Meldungen	Niedrig	Mittel	Betriebliches Kontinuitätsmanagement	Niedrig
5	Angriff durch unzuverlässige Beschäftigte, welche bei einem IT-Dienstleister tätig sind	Niedrig	Hoch	Sorgfältige Auswahl der Dienstleister und Verpflichtung; ggf. Vereinbarung zur Auftragsverarbeitung mit entsprechenden Pflichten; Strafbewehrung eines solchen Angriffs	Mittel
6	Angriff durch unzuverlässige Beschäftigte in der Ombudsstelle	Niedrig	Hoch	Sorgfältige Auswahl der Beschäftigten und Verpflichtung	Mittel
7	Offensichtlich grundlos abgegebenen Meldung, insbesondere Umgehung von Anti-Spam-Maßnahmen	Hoch	Niedrig	Umgehende Prüfung und Löschung offensichtlich grundlos abgegebener Meldungen durch Ombudsstelle	Niedrig
8	Begründete aber irrtümlich oder vorsätzlich falsche Meldung eines Verstoßes	Mittel	Hoch	Umgehende Prüfung durch Ombudsstelle und Organisation auf Plausibilität	Mittel
9	Meldung eines Verstoßes in anderer Organisation	Niedrig	Niedrig	Umgehende Prüfung durch Ombudsstelle und Organisation auf Zuständigkeit	Niedrig

Von den neun identifizierten Risiken haben fünf ein niedriges und vier ein mittleres Restrisiko (RR). Angesichts dieses Risikoprofils ist eine Konsultation gemäß Art. 36 Abs. 1 DSGVO ist nicht erforderlich. Es wurde zwar ein hohes Risiko festgestellt, aber die Organisation ist als Verantwortlicher in der Lage, geeignete Maßnahmen zur Eindämmung des Risikos zu treffen.

5. Ergriffene Schutzmaßnahmen

Die wesentliche strukturelle Maßnahme zum Schutz der personenbezogenen Daten ist die Beauftragung der Leu Rechtsanwaltsgesellschaft mbH als externe, unabhängige Ombudsstelle. Dadurch ist stets eine zeitnahe, qualifizierte Prüfung von eingegangenen Meldungen sichergestellt.

Die technischen und organisatorischen Maßnahmen (TOM) zur Sicherstellung der Sicherheit der Verarbeitung (Art. 32 DSGVO) für die verwendeten IT-Systeme entsprechen dem Stand der Technik wie er im IT-Grundschutz-Kompendium des Bundesamts für Sicherheit in der Informationstechnik (BSI) in der jeweils aktuellen Fassung beschrieben ist.

Soweit Auftragsverarbeiter eingesetzt werden, haben sich diese vertraglich dazu verpflichtet, eigene TOM nachprüfbar umzusetzen.

IV. Standpunkt der betroffenen Personen oder ihrer Vertreter

Auf Einholung des Standpunkts der betroffenen Personen oder ihrer Vertreter (Art. 35 Abs. 9 DSGVO) wurde vorläufig verzichtet, weil die Organisation keinen Betriebsrat hat. Bei der turnusmäßigen nächsten Revision der Datenschutz-Folgeabschätzung wird geprüft werden, wie der Standpunkt der Beschäftigten als wesentliche Kategorie betroffener Personen berücksichtigt werden kann.

V. Zusammenfassung und abschließende Einschätzung

Der Verantwortliche verarbeitet sensible Daten betroffener Personen (Abschnitt II), deren Standpunkt für diese Betrachtung bei der nächsten Aktualisierung dieser Datenschutz-Folgeabschätzung berücksichtigt werden wird (Abschnitt IV). Die Risikoanalyse (Abschnitt III) ergibt ein niedriges bis leicht mittleres Profil der Restrisiken. Die ergriffenen Schutzmaßnahmen erfüllen also ihren Zweck, müssen jedoch regelmäßig überprüft und bei Bedarf angepasst werden.