Anlage Verarbeitung „Hinweismelder-System“, Stand 19.06.2023, in Verbindung mit der Rahmenvereinbarung zur Auftragsverarbeitung nach Art. 28 DSGVO

1. Gegenstand, Art und Zweck der Verarbeitung

Der Auftragnehmer stellt – je nach kaufmännisch beauftragter Leistung – ein
- Online-Meldesystem auf Basis von globaleaks (Open Source) zur Verfügung
- Telefon-Meldesystem zur Verfügung (Eingaben im Online-Meldesystem)

2. Beginn und Dauer des Auftrages

Die Rahmen-Vereinbarung zur Auftragsverarbeitung, in Verbindung mit den relevanten Anlagen, kommt zur Anwendung, sobald und solange der Auftragnehmer personenbezogene Daten des Auftraggebers im Auftrag verarbeitet und keine individuelle Vereinbarung zur Auftragsverarbeitung zwischen Auftraggeber und Auftragnehmer abgeschlossen wurde.

3. Kategorie betroffener Personen und Kategorie der jew. Art der Daten

Kategorie betroffener Personen	**Kategorie der jeweiligen Art der Daten***
Meldende Person(en)	Datum und Uhrzeit der Meldung und/oder Ergänzung der Meldung (Kommentarfunktion) Name und Kontaktdaten (sofern keine anonyme Meldung abgeben wurde oder aufgrund der Vorgaben des Kunden möglich ist) Inhalt der Meldung, zzgl. möglicher bereitgestellter Dateien und Dokumente Melde-ID und Nummer der Meldung (für Zugriff auf die Meldung zur Einsicht des Bearbeitungsstatus und hinterlegte Rückmeldungen bzw. Kommentare)
Beschäftigte oder beauftragte Personen welche als interne Meldestelle fungieren und Zugriff auf Meldungen haben, sowie evtl. Personen die Benachrichtigungen erhalten und keinen Zugriff auf Meldungen erhalten (z. B. zur Überwachung von Fristen)	- Zugangsdaten (Benutzername und Passwort) - Name (Vor- und Nachname) - Öffentlicher Name (optional Auswahl Meldung) - Beschreibung - E-Mail-Adresse - Auswahlfeld „Aktiviert“ (Benutzerkonto) - Auswahlfeld „Passwortänderung erzwingen“ - Auswahlfeld Sprache (ausgewählte Sprache) - Auswahlfeld E-Mail-Benachrichtigung aktivieren - Auswahlfeld „Zwingend ausgewählt“ - Auswahlfeld „Empfängern das Löschen von Hinweisen erlauben“ - Auswahlfeld „Empfängern das Hinausschieben des Berichtablaufdatums erlauben“ - Auswahlfeld „Geben Sie diesem Empfänger die Möglichkeit, Benutzern Zugriff auf Berichte zu gewähren“ - Auswahlfeld „Geben Sie dem Benutzer administrativen Zugriff auf die folgenden Funktionen“ (aktuell Auswahlfeld Einstellungen)

	- Hinterlegung im Kanal / in Kanälen als Empfänger
Externe Ansprechpartner des Auftraggebers	Der Auftraggeber kann dem Auftragnehmer Organisationen und Ansprechpartner nennen, welche eine tiefergehende Prüfung von Vorfällen vornehmen. Dies sind voraussichtlich vom Auftraggeber beauftragte Rechtsanwälte, Steuerberater, Wirtschaftsprüfer, Unternehmensberater, Sachverständige oder Gutachter. Name der Organisation, sowie die i. V. stehenden Ansprechpartner mit beruflichen Kontaktdaten (i. d. R. Anschrift, E-Mail-Adresse, Telefon/Mobiltelefon/Telefax), sowie Angaben in der Signatur (i. d. R. zusätzlich Funktion/Beruf)
Dritte	Im Rahmen einer Meldung oder deren Bearbeitung können personenbezogene Daten von Dritten verarbeitet werden, z. B. als Bestandteil der Meldung, direkt in beigefügten Dateien oder Dokumenten, oder als Meta-Daten von Dokumenten oder Korrespondenz.

* Unterstrichene Angaben = sensible Daten, unterstrichene + fett dargestellte Angaben = besondere Kategorien von Daten nach Art. 9 DSGVO

4. Angaben des Auftragnehmers zur Risikoeinschätzung durch den Auftraggeber

Nachfolgend erhalten Sie Informationen und Einschätzungen des Auftragnehmers zum Risiko der Verarbeitung. Das Risiko, also die Wahrscheinlichkeit des Eintritts und der mögliche Schaden für die Betroffenen kann im individuellen Einzelfall abweichen. Beispielsweise da aufgrund der Tätigkeit des Auftraggebers die personenbezogenen Daten von einer besonderen Gruppe von Personen verarbeitet werden. Ein abweichendes Risiko kann vorhanden sein wenn der Auftraggeber vorsieht in Freifeldern, Zusatzfeldern etc. besondere Kategorien von personenbezogenen Daten gemäß Art. 9 DSGVO zu verarbeiten. Sofern Sie als Auftraggeber zum Ergebnis kommen, dass Sie abweichende oder zusätzliche technische und organisatorische Maßnahmen zum Schutz der personenbezogenen benötigen, können Sie uns gerne ansprechen.

4.1 Werden besondere Kategorien von personenbezogenen Daten gemäß Art. 9 DSGVO verarbeitet?

Es kann nicht ausgeschlossen werden, dass im Rahmen einer Meldung, inkl. beigefügter Dokumente oder Dateien, besondere Kategorien von personenbezogenen Daten verarbeitet werden. Es sind jedoch keine entsprechenden konkreten Felder zur Abfrage vorgesehen.

4.2 Werden die personenbezogenen Daten von Kindern verarbeitet?

Es kann nicht ausgeschlossen werden, dass im Rahmen einer Meldung, inkl. beigefügter Dokumente oder Dateien, personenbezogene Daten von Kindern verarbeitet werden. Dies gilt insb. für Organisationen, die beruflich Daten von Kindern (als Kunde oder Leistungsempfänger) verarbeiten.

4.3 Sind durch die Art oder den Zweck der Verarbeitung besondere Risiken für die Betroffenen erkennbar?

Die Leistungen der Verarbeitungen sind zur Erfüllung von gesetzlichen Vorgaben vorgesehen. Das Ziel dieser gesetzlichen Vorgaben ist es Betroffene vor Risiken zu schützen.

4.4 Einschätzung der Schutzstufe nach dem Schutzstufenmodell der Aufsichtsbehörde Niedersachsen

Eine pauschale Einschätzung kann hier nicht erfolgen, da durch die offene Aufnahme von Meldungen

(Textfelder, Upload oder Übermittlung von Daten) nicht einschränkbar ist, welche Daten in welchem Umfang übermittelt werden. Im Rahmen der allgemeinen Konzeption der Verarbeitung wird eine große Schwere eines möglichen Schadens nicht ausgeschlossen und die Verarbeitung der Schutzstufe „E“ zugeordnet.

4.5 Gibt es Informationen oder Indizien für eine Datenschutz-Folgenabschätzung gemäß Art. 35 DSGVO?

Ja, aufgrund der Angaben unter Punkt 4.4 sollte der Verantwortliche eine Datenschutz-Folgenabschätzung unter Berücksichtigung der individuellen Gegebenheiten (Unternehmensgröße, Anzahl von Hierarchie-Ebenen, Branche/Tätigkeit) durchführen.

Da die Verarbeitung zur Erfüllung von gesetzlichen Vorgaben erfolgen muss, empfehlen wir zur Risikoreduktion für den Betroffenen (Meldung) die Möglichkeit einer anonymen Meldung anzubieten. Über die Kommentarfunktion ist ein anonymer Austausch zwischen Auftraggeber und Melder möglich.

4.6 Erfolgt die Verarbeitung personenbezogener Daten in einem Drittland und sonstige Anmerkungen des Auftragnehmers zur Risikoeinschätzung

Die Nutzung der bereitgestellten Systeme ist ohne eine Verarbeitung personenbezogener Daten in einem Drittland möglich. Es kann jedoch nicht ausgeschlossen werden, dass Meldende aus einem Drittland oder Nutzung entsprechender Dienste (z. B. E-Mail-Account) die Meldung durchführen. Auch ein entsprechendes Routing bei der Nutzung kann erfolgen, ohne dass der Auftragnehmer hier Einfluss hat.

5. Sub-Auftragsverarbeiter

Sub-Auftragsverarbeiter mit Anschrift	**Tätigkeit**	**AV und TOM**	**Anmerkungen**
IONOS SE, Elgendorfer Straße 57, 56410 Montabaur, Deutschland	Hosting Online-Meldekanal	Abschluss am 22.12.2022, seit 19.07.2022 sind die AV Bestandteil der AGB. https://www.ionos.de/terms-gtc/avv	Standard, sofern nicht im Rahmen der individuellen Erbringung ein anderes Hosting beauftragt wurde.
BSAG Bueroservice 24 AG Pappelallee 78/79 10437 Berlin, Deutschland	Annahme und Erfassung telefonischer Meldungen und ergänzender Kommentare, sowie Mitteilung des Status und evtl. hinterlegter Kommentare.	Stand: 12.11.2021	Nur relevant, wenn ein Telefon-Meldekanal mit Annahme beauftragt wurde
weclapp GmbH, Friedrich-Ebert-Straße 28, 97318 Kitzingen, Deutschland	Ticketsystem zur Überwachung der Meldungen, Austausch mit Auftraggeber oder ihm benannten Dritten Das Ticket-System wird auch zur Auftragserfüllung und Dokumentation von in Verbindung stehenden	Zuletzt Stand: Mai 2023	Kann bei Beauftragung von individuellen Paketen zum Sub-Unternehmer werden, sofern über die Tickets eine Überwachung der Meldung oder ein Austausch vorliegt und wir NICHT als

	Tätigkeiten genutzt, z. B. Dokumentation von Weisungsbefugnissen, Support etc. Diese Verarbeitungen stellen keine Auftragsverarbeitung dar.		interne Meldestelle fungieren.

6. Ergänzende oder abweichende technische & organisatorische Maßnahmen (TOM)

Gemäß der Rahmen-Vereinbarung zur Auftragsverarbeitung gelten die allgemeinen technischen und organisatorischen Maßnahmen des Auftragnehmers, sowie beim Einsatz von Sub-Auftragsverarbeitern die TOM der jew. Sub-Auftragsverarbeiter (siehe Auflistung, Punkt 5). Nachfolgende ergänzende oder abweichende technische und organisatorische Maßnahmen sind für diese Verarbeitung(en) vorgesehen:

- Die Möglichkeit einer anonymen Meldung ist möglich (Auswahl bei der Bestellung bzw. Konfiguration der Meldeseite)
- Sicherheitsmaßnahmen des Entwicklers für GlobaLeaks (siehe unter https://docs.globaleaks.org/en/main/security/index.html)

6.1 Hinweise zu erforderlichen Tätigkeiten durch den Auftraggeber

Bei eigenenständigen Bearbeitung von Hinweisen durch den Auftraggeber (wir sind NICHT als interne Meldestelle aktiv):
- Der Auftraggeber muss sicherstellen, dass er dem Auftraggeber gegenüber mindestens eine funktionstüchtige und aktive E-Mail-Adresse von mindestens einem Benutzer zur Verfügung stellt, welche Meldungen empfängt und bearbeitet.

- Der Auftraggeber stellt sicher, dass nur befugte Personen Zugangsdaten für das Hinweismelder-System erhalten.

- Der Auftraggeber stellt sicher, dass nur befugte Personen Zugriff auf die Meldung erhalten (siehe insb. Vertraulichkeitsgebot § 9 HinSchG und Ausnahmen vom Vertraulichkeitsgebot § 10 HinSchG).

- Der Auftraggeber ist für die Rückmeldung an die hinweisgebende Person, Einhaltung der Fristen und gesetzlichen Vorgaben, insb. Einhaltung des Vertraulichkeitsgebotes, verantwortlich.

- Der Auftraggeber muss eine eigenständige Löschung der Meldung nach Erreichen der Aufbewahrungsfrist oder Zweckentfall durchführen.

- Der Auftraggeber muss die Betroffenen gemäß Art. 13 / 14 DSGVO über die Verarbeitung der personenbezogenen Daten informieren. Der Auftraggeber stellt dem Auftraggeber einen Mustertext zur Verfügung.

Sofern der Auftraggeber eine individuelle Lösung wünscht, sollte dieser mit dem Auftragnehmer die Themen Datensicherung und Wiederstellung, sowie Prüfung und Einspielung von Sicherheitsupdates (Server, erforderliche Komponenten und Anwendungen) abstimmen und die Zuständigkeit nachweislich festlegen.

Sofern der Auftraggeber eine individuelle Lösung beauftragt und diese selbst nutzt, um seinen Kunden ein Hinweisgeber-System anzubieten, muss dieser selbst prüfen, ob eine Vereinbarung zur Auftragsverarbeitung erforderlich ist und welche Datenschutzvorgaben zu berücksichtigen sind.

7. Ergänzende oder abweichende Regelungen zur Rahmenvereinbarung zur Auftragsverarbeitung

Wir gehen zum aktuellen Zeitpunkt davon aus, dass eine Auftragsverarbeitung nur erforderlich ist, wenn wir dem Auftraggeber Meldekanäle zur Verfügung stellen und wir NICHT als interne Meldestelle tätig sind. Sofern wir als interne Meldestelle aktiv werden stellt dies nach unserer Auffassung eine eigenverantwortliche Tätigkeit dar, da gemäß § 15 HinSchG die interne Meldestelle bei der Ausübung ihrer Tätigkeit unabhängig ist, gemäß § 14 HinSchG ein Dritter mit der Aufgabe betraut werden darf und Meldestellen gemäß § 10 HinSchG befugt sind personenbezogener Daten zur Erfüllung der Aufgaben zu verarbeiten.

8. Angaben zu Speicher- und Löschfristen bzw. -kriterien

Siehe Regelung § 11 Abs 5 HinSchG.

9. Angaben zum Datenschutz- und Sicherheitsmanagement

Keine weiteren Angaben.

10. Weitere Anmerkungen zu der Verarbeitung bzw. den Verarbeitungen

Keine weiteren Anmerkungen.

11. Stand des Dokumentes und Historie

Erstellung des Dokumentes am 19.06.2023, Sebastian Tausch