Vorwort

Die Evermood GmbH hat die Anwendung Evermood entwickelt. Die Anwendung ist eine browserbasierte Softwarelösung, welche von Organisationen zur Beratung und Unterstützung ihrer Beschäftigten (Endnutzer) bei arbeitsrelevanten, privaten, gesundheitlichen oder compliancebezogenen Anliegen eingesetzt wird. Das System ermöglicht Organisationen insbesondere:

- ihre Pflichten gem. §12 AGG zu wahren;
- ihre Arbeits- und betrieblichen Umweltschutzpflichten gem. § 89 BetrVG zu wahren;
- die EU-Hinweisgeberrichtlinie (EU) 2019/1937 umzusetzen.

Da es sich bei den Daten, die in der Anwendung verarbeitet werden, um sensible Inhalte zu Anliegen von Endnutzern handeln kann, hat die Evermood GmbH unabhängig von einer Schwellwertanalyse entschieden, eine Datenschutzfolgenabschätzung (DSFA) durchzuführen, um zu ermitteln, ob die bereits getroffenen Maßnahmen zur Datensicherheit den vorherrschenden Risiken für Betroffene entsprechen. Hierbei wurden Beteiligte aus verschiedenen Verantwortungsbereichen der Evermood GmbH sowie der externe Datenschutzbeauftragte eingebunden. Der Datenschutzbeauftragte Simon Lenz, Mitarbeiter der ProSec GmbH, ein Unternehmen spezialisiert auf Penetrationstests, Sicherheitsaudits und Beratung zu Fragen des Datenschutzes und der Informationssicherheit, hatte dabei die Aufgabe, die Risikomodellierung zu moderieren und zu bewerten.

1. Verantwortlicher und Beteiligte der DSFA

1.1. Verantwortlicher für die DSFA

Evermood GmbH
c/o betahaus
Rudi-Dutschke-Str. 23
10969 Berlin

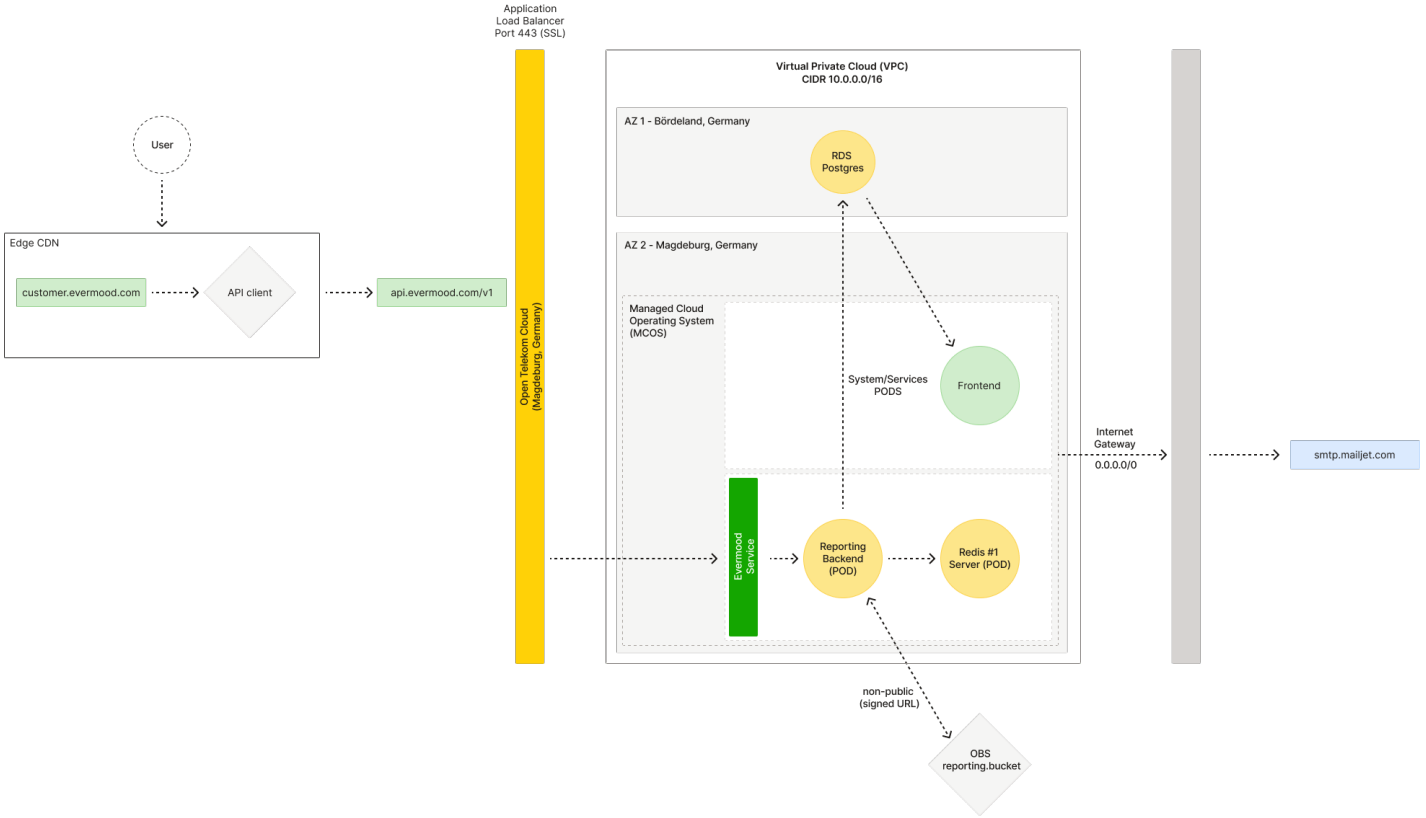
1.2. Beteiligte der DSFA

Name	Funktion
Marie Nitze	Geschäftsführerin, Evermood GmbH
Tobias Rohloff	CTO und Sicherheitsbeauftragter, Evermood GmbH
Henning Bittscheidt	Sachbearbeiter Datenschutz, Evermood GmbH
Simon Lenz	Mitarbeiter ProSec GmbH, Datenschutzbeauftragter Evermood GmbH

2. Verarbeitungsvorgang

2.1. Systemarchitektur

Die technische Umsetzung der Systemarchitektur wurde mit dem Ziel einer möglichst hohen Flexibilität und Robustheit konzipiert, insbesondere um die Anforderungen von Datenschutz und Datensicherheit zu erfüllen. Die Verarbeitung und Speicherung von personenbezogenen Daten erfolgt ausschließlich in der dargestellten Virtual Private Cloud der Open Telekom Cloud in Deutschland.



22. Allgemeine Darstellung des Verarbeitungsvorganges

Endnutzer erreichen die Anwendung Evermood über eine individuelle URL des Kunden (z.B. customer.evermood.com). Endnutzer können hier (1) Beiträge zu verschiedenen Themen lesen und/oder (2) ein Anliegen an eine von ihnen ausgewählte Ansprechperson senden.

1. Das Abrufen von Beiträgen erfolgt ohne die Erfassung von personenbezogenen Daten.
2. Sofern ein Anliegen an eine ausgewählte Ansprechperson gesendet wird, werden die übermittelten Daten verschlüsselt an eine Datenbank übertragen. Personenbezogene Daten, die in diesem Anliegen enthalten sind, können ausschließlich von der ausgewählten Ansprechperson eingesehen werden. Darüber hinaus können Endnutzer im Rahmen eines Anliegens ebenfalls über einen verschlüsselten Chat mit ihrer ausgewählten Ansprechperson kommunizieren. Das Chat-Protokoll ist Teil des Anliegens und unterliegt den gleichen Zugriffsberechtigungen.

Endnutzer können ihre Anliegen stets über einen sichtbaren Button anonymisieren. Anonymisiert ein Endnutzer ihr/sein Anliegen, werden alle personenbezogenen Daten im Zusammenhang mit dem Anliegen innerhalb von 30 Tagen unwiderruflich gelöscht.

Alle Eingabefelder, die von Endnutzern im Zusammenhang mit der Abgabe eines Anliegens genutzt werden, sind als "enthält personenbezogene Daten" oder "enthält keine personenbezogene Daten" deklariert. Anonymisieren Endnutzer ihre Anliegen, werden alle Daten im Zusammenhang mit Eingabefeldern, die als "enthält personenbezogene Daten" deklariert sind, systemseitig anonymisiert. Folgende Eingaben werden entsprechend anonymisiert:

- Freitextfelder;
- Multiple-Choice Felder, die als "enthält personenbezogene Daten" deklariert sind;
- Chatprotokolle.

Nicht-personenbezogene Daten (z.B. aufgerufene Beiträge, Themen und Themengruppen von Anliegen) werden wöchentlich aggregiert und ausgewählten Ansprechpersonen in Form von Statistiken angezeigt. Die

wöchentliche Aggregierung ist ausgewählt worden, um das Verhalten von Endnutzern nicht in Echtzeit oder täglich zurückverfolgen zu können.

2.3. Zwecke der Verarbeitung

Die Evermood GmbH fungiert bei der Verarbeitung personenbezogener Daten als Auftragsverarbeiter. Daher obliegt ihr nicht die Definition von Zwecken, aufgrund derer Organisationen die Verarbeitungen beauftragen. Nachfolgend sind daher Zwecke genannt, die vermutlich von den Verantwortlichen verfolgt werden, wenn sie die Anwendung Evermood nutzen und ihren Beschäftigten zur Verfügung stellen.

- Unterstützung ihrer Beschäftigten bei arbeitsrelevanten, privaten, gesundheitlichen oder compliancebezogenen Anliegen;
- Wahrung der Arbeitgeberpflichten gem. §12 AGG;
- Wahrung der Arbeits- und betrieblichen Umweltschutzpflichten gem. § 89 BetrVG;
- Umsetzung der EU-Hinweisgeberrichtlinie (EU) 2019/1937.

2.3.1. Verarbeitete Daten und Betroffene

Art der Daten	**Art und Zweck der Verwendung**	**Betroffene Personen**
Vorname Nachname E-Mail-Adresse Passwort	Erstellung eines Nutzerprofils zur Einsicht und Verwaltung des Systems	Ausgewählte Ansprechpersonen des Auftraggebers
Telefonnummer (freiwillig)	Telefonische Kontaktaufnahme für ratsuchende Beschäftigte	Ausgewählte Ansprechpersonen des Auftraggebers
Profilfoto (freiwillig)	Darstellung eines Benutzerprofils im System	Ausgewählte Ansprechpersonen des Auftraggebers
Freitextangaben (freiwillig) Multiple-Choice Angaben (freiwillig)	Nutzung der Suchfunktion im System; Spezifizierung des Anliegens; Kommunikation mit Ansprechpersonen über anonymen Chat	Beschäftigte des Auftraggebers
E-Mail-Adresse (freiwillig)	Bestätigung einer Terminvereinbarung	Beschäftigte des Auftraggebers
Telefonnummer (freiwillig)	Vereinbarung eines telefonischen Beratungsgespräches	Beschäftigte des Auftraggebers

* Freiwillige Angabe

Notwendige Daten für die Verarbeitung und Übertragung werden verarbeitet, jedoch unmittelbar gelöscht. Eine Protokollierung von personenbezogenen Daten findet nicht statt.

Für Nutzer des Beratungsangebots gibt es immer die Möglichkeit, sich anonym mit einem Anliegen über die Anwendung Evermood an die verantwortliche Ansprechperson zu wenden. In diesen Fällen werden sämtliche gemachten Angaben nicht personenbeziehbar gespeichert. Sämtliche Angaben von Nutzern sind aus Sicht der Evermood GmbH freiwillig.

2.3.2. Speicherdauer

Die erhobenen Daten werden nach folgenden Kriterien bis zur Löschfrist aufbewahrt.

Datenart	**Fristbeginn**	**Frist**
Ressourcen	Löschantrag eines Administrators	Unmittelbar
	Vertragsende	1 Jahr
Organisationsdaten	Ende des Kalenderjahres, in dem der entsprechende Beleg entstanden ist.	10 Jahre
Ansprechpersonen und Admins (Vollständige Profile)	Löschantrag eines Administrators oder Vertragsende	1 Jahr
Optionale Einzeldaten von Ansprechpersonen und Admins	Löschantrag der Ansprechperson/des Admins (bspw. die Löschung einer Telefonnummer)	Unmittelbar
Notwendige Einzeldaten von Profilen von Ansprechpersonen und Admins	Löschantrag der Ansprechperson/ des Admins	1 Jahr

Anliegen (inkl. Kommentare), Status "nicht bearbeitet" oder "In Bearbeitung"	Löschantrag der meldenden Person	30 Tage
Anliegen (inkl. Kommentare), Status "Geschlossen"	Löschantrag der meldenden Person	30 Tage
	Letzter Statuswechsel zu "Geschlossen"	2 Jahre
Kommentare zu Anliegen	Löschantrag der Verfasser*in	Unmittelbar

2.3.3. Rechtsgrundlage

Da es sich bei der Verarbeitung von personenbezogenen Daten in der Anwendung Evermood um eine Auftragsverarbeitung handelt, ist die Rechtsgrundlage der Verarbeitung durch die Evermood GmbH Art. 28 DSGVO.

Bei den Rechtsgrundlagen der Verantwortlichen wird es sich in der Regel um folgende Rechtsgrundlagen handeln:

- Einwilligung Art. 6 Abs. 1 lit a) DSGVO;
- §26 BDSG;
- Ausdrückliche Einwilligung gem. Art 9 Abs. 2 lit a).

2.3.4. Datenschutzanforderungen

Bei den durch die Anwendung verarbeiteten personenbezogenen Daten handelt es sich zum Teil regelmäßig um Anliegen der Endnutzer. Bei diesen Anliegen ist regelmäßig davon auszugehen, dass es sich um private oder sensible Angaben des Endnutzers handelt. Somit sind diese personenbezogenen Daten als sensibel einzustufen. Im Rahmen der Angaben durch Endnutzer zu diesen Anliegen besteht auch die Möglichkeit, dass besondere Kategorien personenbezogener Daten im Sinne des Art 9 der DSGVO verarbeitet werden. Dies hat zur Folge, dass für die Verarbeitung dieser Kategorien von Daten besondere über den Standard hinausgehende Maßnahmen zur Datensicherheit getroffen werden müssen. Weil sich diese Kategorien von Daten aufgrund der Eingabe über Freitextfelder nicht von anderen Datenkategorien trennen lassen, gilt der erhöhte Schutzbedarf für sämtliche verarbeiteten Datenkategorien und wird auch entsprechend in der Risikobeurteilung der DSFA bedacht.

In Konsequenz müssen auch sämtliche Maßnahmen zur Datensicherheit gem. Art. 32 DSGVO dem erhöhten Schutzbedarf entsprechen. Entsprechend den Anforderungen der DSGVO sieht die Evermood GmbH sich dazu verpflichtet:

- die Anforderungen an Pseudonymisierung und Verschlüsselung der personenbezogenen Daten zu erfüllen;
- die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der für die Verarbeitung verwendeten Systeme auf Dauer zu gewährleisten;
- die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem Zwischenfall rasch wiederherzustellen;
- Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der definierten und eingesetzten technischen und organisatorischen Maßnahmen zur Gewährleistung der Datensicherheit einzusetzen und die Maßnahmen bei Bedarf entsprechend anzupassen.

Diese Datenschutzanforderungen finden entsprechend Anklang bei der Beurteilung der Risiken für Betroffene der Verarbeitung.

3. Risikoanalyse vor Umsetzung von Abhilfemaßnahmen

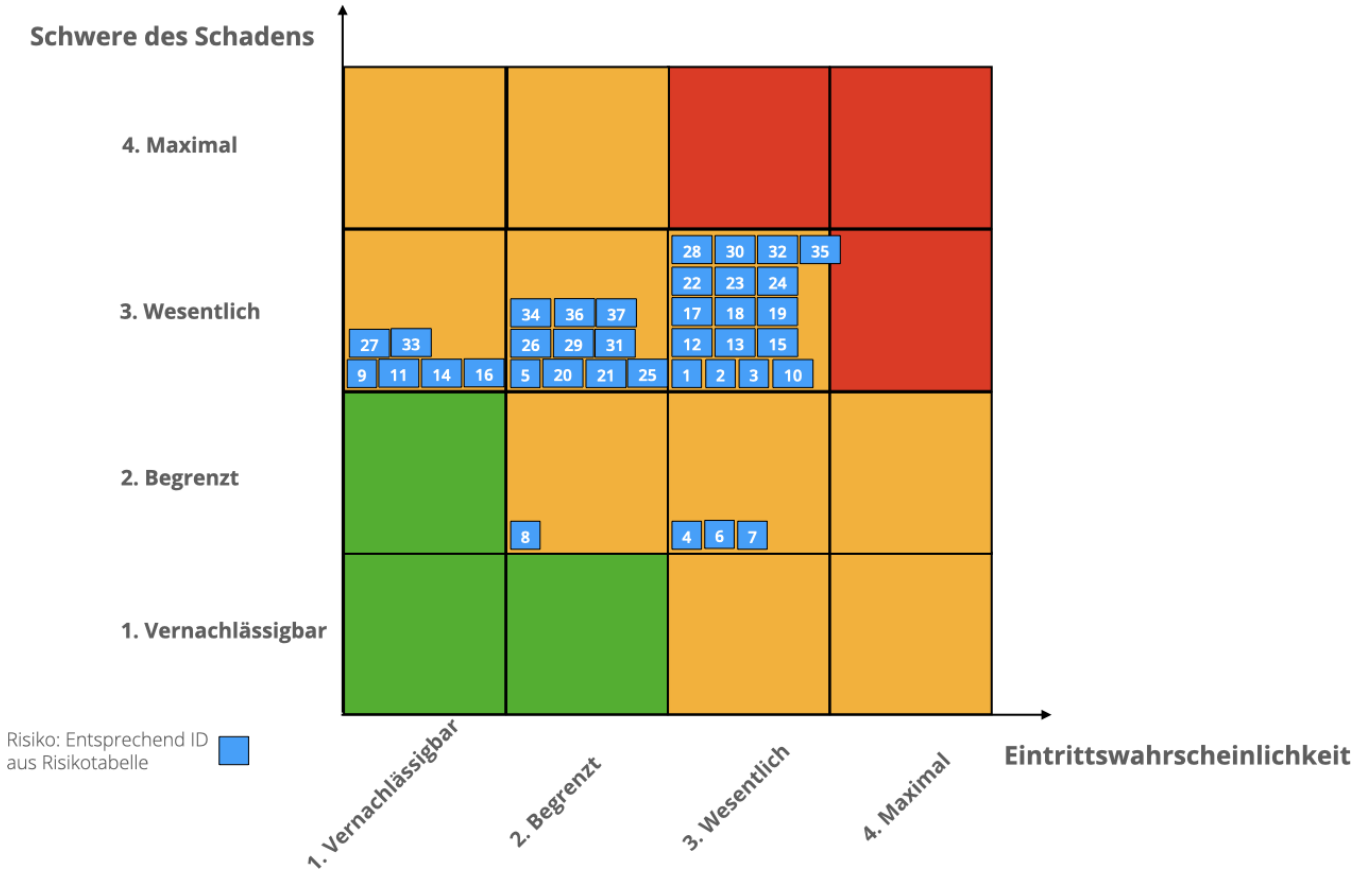
3.1. Risikoeinstufung aus Sicht des Betroffenen

Es ist zu bewerten, welche Risiken für Rechte und Freiheiten des Betroffenen der beschriebenen Verarbeitungsvorgänge bestehen. Hierzu wird die Risikoeinschätzung der Bitkom zugrunde gelegt. Diese ist in dem folgenden Diagramm in den relevanten Auszügen dargestellt:

Risiko-Niveau	1. Vernachlässigbar	2. Eingeschränkt	3. Signifikant	4. Maximal
Allgemeine Kategorisierung	Betroffene erleiden eventuell Unannehmlichkeiten, welche sie aber mit einigen Problemen überwinden können.	Betroffene erleiden eventuell signifikante Unannehmlichkeiten, welche Sie aber mit einigen Schwierigkeiten überwinden können.	Betroffene erleiden eventuell signifikante Konsequenzen, die sie nur mit ernsthaften Schwierigkeiten überwinden können.	Betroffene erleiden eventuell signifikante oder sogar unumkehrbare Konsequenzen, die sie nicht überwinden können.
Beispiele für materielle Auswirkungen	Zeitverlust bei Wiederholung von Formalitäten oder Warten, bis sie erfüllt werden	Unrichtiges oder unangebrachtes Profiling	Verlust des Arbeitsplatzes	Erhebliche Schulden; Unfähigkeit zu arbeiten
Beispiele für moralische Auswirkungen	Angst, die Kontrolle über die eigenen Daten zu verlieren; Gefühl der Verletzung der Privatsphäre ohne wirklichen oder objektiven Schaden (z.B. kommerzielle Eingriffe)	Probleme im Umgang mit privaten oder beruflichen Kontakten (z.B. Rufschädigung, keine Wiedererkennung);Verletzung der Privatsphäre ohne bleibende Schäden	Gefühl der Verletzung der Privatsphäre mit irreversiblen Schaden; Gefühl der Verwundbarkeit nach einer Vorladung vor Gericht	Langfristige oder dauerhafte psychische Beschwerden; strafrechtliche Verurteilung

3.2. Risikobewertung vor Umsetzung von Abhilfemaßnahmen

In der Risikobewertung wurden 37 Risiken für Betroffene identifiziert. Entsprechend der Dimensionen Eintrittswahrscheinlichkeit (1-Vernachlässigbar, 2-Begrenzt, 3-Wesentlich, 4-Maximal) und der erwarteten Schwere des Schadens für den Betroffenen (1-Vernachlässigbar, 2-Begrenzt, 3-Wesentlich, 4-Maximal) wurden diese Risiken zunächst unter der Annahme betrachtet, dass keinerlei Maßnahmen zur Sicherheit der Verarbeitungen getroffen werden. Dies geschah unabhängig davon, ob solche Maßnahmen bereits standardmäßig vorgesehen waren. Aus dieser Risikobewertung ergab sich folgende Klassifizierung der identifizierten Risiken.



Eine detaillierte Dokumentation der Risiken findet sich in Anhang 1 - Risikotabelle vor Maßnahmen.

4. Umzusetzende Abhilfemaßnahmen

Folgende Abhilfemaßnahmen waren bereits im Einsatz oder geplant, bzw. wurden nach Betrachtung der Risiken getroffen.

4.1. Maßnahmengruppe 1 - Maßnahmen zur Vertraulichkeit und Integrität der Daten

Die Anwendungsdaten werden in von einem Unterauftragnehmer zur Verfügung gestellten Rechenzentren verarbeitet.

Evermood nutzt für den Serverbetrieb im Rechenzentrum einen Unterauftragnehmer, die Open Telekom Cloud der Telekom Deutschland GmbH. Der Unterauftragnehmer wird entsprechend der Vereinbarung zur Auftragsvereinbarung durch Evermood geprüft. Das Rechenzentrum des von Evermood beauftragten Unterauftragnehmers erfüllt mindestens folgende Anforderungen:

4.1.1. Zutrittskontrollen

- Alarmüberwachung
- Personenüberprüfung und -identifikation bei Zutritt
- Zutrittsprotokollierung
- Kameraüberwachung sowie Bewegungs- und Einbruchmelder
- Personenkontrolle und -überwachung durch Vor-Ort-Personal

Diese Sicherheitsmaßnahmen werden durch die Unterauftragnehmer rund um die Uhr an sieben Tagen pro Woche sichergestellt.

Der Unterauftragnehmer führt regelmäßige Audits der Sicherheitsmaßnahmen durch. Diese werden durch Evermood angefordert und geprüft.

4.1.2. Zugangskontrollen

Für die Rechner der Beschäftigten, für eigene Server als auch für externe Dienste (z.B. zur Administration von gemieteten Servern) unternimmt Evermood umfangreiche Maßnahmen, um die Nutzung durch Unbefugte zu verhindern:

- Alle nicht-öffentlichen Dienste sind grundsätzlich durch individuelle Benutzername/ Passwort-Kombinationen geschützt.
- Die Anmeldung bei kritischen Diensten ist nur mit Zwei-Faktor-Authentifizierung möglich, d.h. mit Benutzername, Passwort und einem zusätzlichen, getrennt generierten Einmaltoken.
- Ein externer Zugang zum Büronetzwerk ist nur über eine verschlüsselte VPN-Verbindung möglich.
- Sofern die Beschäftigten firmeneigene Smartphones nutzen, sind diese durch Vollverschlüsselung geschützt und können bei Diebstahl oder Verlust durch eine zentrale Administrationsplattform gelöscht werden.
- Die Daten auf den Rechnern der Beschäftigten sind vollständig verschlüsselt und nur nach Anmeldung durch den Nutzer entschlüsselbar, um einen Zugriff auf die Daten bei Verlust oder Diebstahl des Rechners zu verhindern.
- Durch den ausschließlichen Einsatz von Linux- und Apple-Computern reduzieren sich die Angriffsmöglichkeiten auf die Systeme deutlich.

4.1.3. Zugriffskontrolle

Evermood stellt durch verschiedene Maßnahmen sicher, dass Personen nur entsprechend der ihnen eingeräumten Zugriffsberechtigung auf IT-Systeme und die darauf gespeicherten Daten zugreifen können. Dies wird durch folgende Maßnahmen erreicht:

- Benutzer und ihre Zugriffsrechte werden zentral verwaltet, aktiviert und gesperrt.
- Die Verwaltung der Nutzer für sicherheits- und datenschutzrelevante Systeme ist nur durch den Geschäftsführer und einen leitenden Angestellten möglich.
- Für den Zugriff auf die verwendeten Systeme werden, sofern technisch möglich, Passwortrichtlinien inkl. Passwortlänge und Änderungsintervallen vorgegeben.
- Für die ordnungsgemäße Vernichtung von Dokumenten und optischen Datenträgern wird ein Aktenvernichter der Sicherheitsstufe 3 gemäß DIN 32757 genutzt.

4.1.4. Trennungskontrolle

Mit den folgenden Maßnahmen realisiert Evermood die Trennung der Daten verschiedener Kunden bzw. Kundenprojekte:

- Beim Betrieb werden die Daten verschiedener Kunden auf jeweils eigenen, getrennten Datenbanken gespeichert.
- Produktiv- und Testsysteme werden getrennt betrieben.

4.1.5. Weitergabekontrolle

Daten zwischen Auftraggeber und Auftragnehmer werden ausschließlich elektronisch übertragen, ein Datentransport per Datenträger findet nicht statt. Dementsprechend werden folgende Maßnahmen zur Sicherung der personenbezogenen Daten bei der Übertragung vorgenommen:

- Daten werden ausschließlich verschlüsselt (per SSH-, TLS- oder VPN-Verbindung) übertragen.
- Falls Anwendungsdaten zur Demonstration von Funktionen der Anwendung benötigt werden (sogenannte Test-Daten), werden diese vor der Übertragung auf das Testsystem pseudonymisiert.
- Zugriffe auf Systeme mit personenbezogenen Daten werden protokolliert.

4.1.6. Eingabekontrolle

Folgende Maßnahmen gewährleisten die Überprüfung und Feststellung, ob und von wem personenbezogene Daten eingegeben, verändert oder entfernt worden sind:

- Im Rahmen der Anwendungsentwicklung und des Betriebs der Anwendung erfolgt keine Eingabe oder Änderung von Anwendungsdaten durch Evermood. Dies obliegt allein dem Auftraggeber.
- Maßnahmen innerhalb der Anwendung, die die Nachvollziehbarkeit von Datenänderungen sicherstellen und Lösch- und Sperrfristen umsetzen, sind durch den Auftraggeber im Rahmen der Zusammenarbeit zu beauftragen.

4.2. Maßnahmengruppe 2 - Maßnahmen zur Verfügbarkeit und Belastbarkeit

Die Verarbeitung personenbezogener Daten erfolgt im Rechenzentrum des Unterauftragnehmers.

Der Unterauftragnehmer für den Serverbetrieb im Rechenzentrum ist vertraglich verpflichtet, mindestens mit den folgenden Maßnahmen die Verfügbarkeit sicherzustellen:

- Betrieb einer unterbrechungsfreien Stromversorgung
- Temperatur-, Feuchtigkeits- und Klimaüberwachung
- Feuer- und Rauchmeldeanlagen
- Automatische Löschanlagen

4.2.1. Maßnahmen zur Wiederherstellbarkeit

Zum Schutz der personenbezogenen Daten vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung werden alle relevanten Daten täglich gesichert (Art. 32 DSGVO).

Die Datensicherung umfasst sowohl die Datenbank als auch alle hochgeladenen Dateien in Onlinespeichern. Hierdurch ist die Integrität aller erhobenen Daten gewährleistet.

Die Backups werden täglich durchgeführt und in einem vom normalen Betrieb getrennten Speicher gesichert. Die Aufbewahrungsfristen sind wie folgt:

- Tägliche Sicherung für einen Monat (30 Tage)
- Wöchentliche Sicherung für ein Jahr

Nach Ablauf der jeweiligen Fristen werden sämtliche Daten unwiederbringlich gelöscht. Es werden jeweils alle Dateien vollständig gesichert (nicht-inkrementell), sodass für das Wiederherstellen die Integrität von nur einem Backup gegeben sein muss.

Das Ergebnis der Datensicherung wird vor der Übertragung in den Sicherungsspeicher verschlüsselt. Hierbei wird die höchsten Sicherheitsstandards genügende AES-Verschlüsselung mit einer Schlüssellänge von 256 Bit verwendet. Der Schlüssel wird in einem Schlüsselbund gesichert, auf den lediglich Administratoren Zugriff haben. Der vom normalen Betrieb getrennte Speicher wird mit denselben Vorkehrungen gesichert wie die Infrastruktur des normalen Betriebs:

- Selektive Zugriffe nur für notwendige Personen (Administratoren) und zwei-Faktor-Authentifizierung.
- Erst bei einer Wiederherstellung der Daten wird die Sicherung außerhalb des Sicherungsspeichers wieder entschlüsselt.

So liegen niemals unverschlüsselte Daten im Speicher. Die Übertragung der Sicherung selbst erfolgt ebenfalls über eine verschlüsselte Verbindung. Somit sind Daten In-Transit als auch At-Rest immer verschlüsselt.

Um der Speicherbegrenzung gerecht zu werden, werden vor Inbetriebnahme einer wiederhergestellten Datensicherung die für personenbezogene Daten relevanten automatisierten Sperr- und Löschregeln auf die

Daten angewandt. Hierdurch wird sichergestellt, dass Daten, welche zwischenzeitlich gelöscht wurden, aber in der Sicherung noch vorhanden waren, erneut gelöscht werden (Art. 5 DSGVO).

Das Programm, welches die Daten sichert, wird ebenfalls zur Wiederherstellung der Daten genutzt. Sowohl Sicherung als auch Wiederherstellung werden dokumentiert und sind durch autorisierte Personen einfach umsetzbar.

Die tägliche Datensicherung wird überwacht. Bei einem Fehler werden qualifizierte Beschäftigte umgehend benachrichtigt. Erst bei Bestätigung der Beschäftigten wird die Eskalation gestoppt. Darüber hinaus wird bei einem Fehler automatisch mehrfach versucht, die Datensicherung neu zu starten.

4.3. Maßnahmengruppe 3 – Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Datensicherheitsmaßnahmen

4.3.1. Netzwerkschutz

Um einen umfangreichen Netzwerkschutz gewährleisten zu können, werden umfassende Sicherheitsdienste von der Open Telekom Cloud sowie eigene cloudflarebasierte Edge-Protection-Netzwerke verwendet.

Darüber hinaus werden regelmäßige Audits und Network-Intelligence-Technologien eingesetzt, die das Netzwerk kontinuierlich auf bekannte bösartige Verkehrsmuster und Netzwerkattacken überwachen und diese blockieren.

4.3.2. Architektur

Die Netzwerksicherheitsarchitektur besteht aus mehreren Sicherheitszonen. Sensiblere Systeme, wie Datenbankserver, befinden sich in der vertrauenswürdigsten Zone. Andere Systeme befinden sich je nach Funktion, Informationsklassifizierung und Risiko in Zonen, die ihrer Sensibilität entsprechen. Abhängig von der jeweiligen Zone kommen zusätzliche Sicherheitsüberwachungs- und Zugangskontrollen zum Einsatz.

4.3.3. Penetrationstests durch externe Experten

Die Produktions- und Unternehmensnetzwerke von Evermood werden einmal jährlich von externen Sicherheitsexperten mithilfe eines umfangreichen Penetrationstest überprüft. Werden hierbei Risiken für die Verarbeitungen erkannt, werden diese ihrer Prioritäten entsprechend behoben.

4.3.4. Datenschutz durch Technikgestaltung

Die auf Produkten von Evermood ausgeführten Interaktionen sind stets verschlüsselt. Ferner nutzt Evermood flexible Audit Trails, sodass die Datenminimierung gewährleistet ist.

Nutzer haben die Möglichkeit, unkompliziert Löschanträge für von ihnen eingetragene Daten zu stellen. Im Fall von Anliegen von Endnutzern werden diese nach spätestens 30 Tagen gelöscht.

Löschungen erfolgen durch vollständige Anonymisierung der Datensätze. Es werden auch Daten gelöscht, die identifizierbare Inhalte enthalten könnten (z.B. Kommentar oder Freitextfelder), um zu verhindern, dass personenbezogene Daten in diesen Inhalten verbleiben.

4.3.5. Datenschutzfreundliche Voreinstellungen

Die Zugriffsrechte sind automatisch an die verschiedenen Benutzerrollen angepasst bzw. beschränkt. Die Zugriffsrechte der Beschäftigten von Evermood auf Endgeräte, die an das Netzwerk von Evermood angeschlossen sind, sind automatisch beschränkt.

Alle nicht zwingend für die Funktion der Anwendung notwendigen Angaben sind freiwillig. Für Nutzer der Anwendung Evermood besteht stets die Möglichkeit, Anliegen anonym anzugeben.

4.3.6. Auftragskontrolle

Um zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend der Weisungen des Auftraggebers verarbeitet werden, unternimmt Evermood u.a. die folgenden Maßnahmen:

- Überprüfung vorhandener Zertifizierungen von Unterauftragnehmern (speziell gem. ISO 9001, ISO 27001 und ISO 27018)
- Abschluss einer Vereinbarung zur Auftragsverarbeitung oder von EU-Standardvertragsklauseln
- Überprüfung sonstiger Dokumentationen und Rechercheergebnissen, die eine Beurteilung der Zuverlässigkeit eines Anbieters ermöglichen
- Kontrolle der Vertragsausführung
- Regelmäßige Prüfung von Auditberichten der Unterauftragnehmer

4.4. Maßnahmengruppe 4 - Incident Response

Firewalls werden gemäß den Best Practices der Branche konfiguriert.

Um umfassende Protokolle von wichtigen Netzwerkgeräten und Hostsystemen zu erfassen, wird ein Security-Incident-Event-Management-System (SIEM) verwendet. Bei einem Sicherheitsalarm werden Vorfälle an den Sicherheitsbeauftragten eskaliert. Der Sicherheitsbeauftragte ist mit den jeweiligen Kommunikationskanälen und Eskalationspfaden vertraut.

5. Risikoanalyse nach Umsetzung von Abhilfemaßnahmen

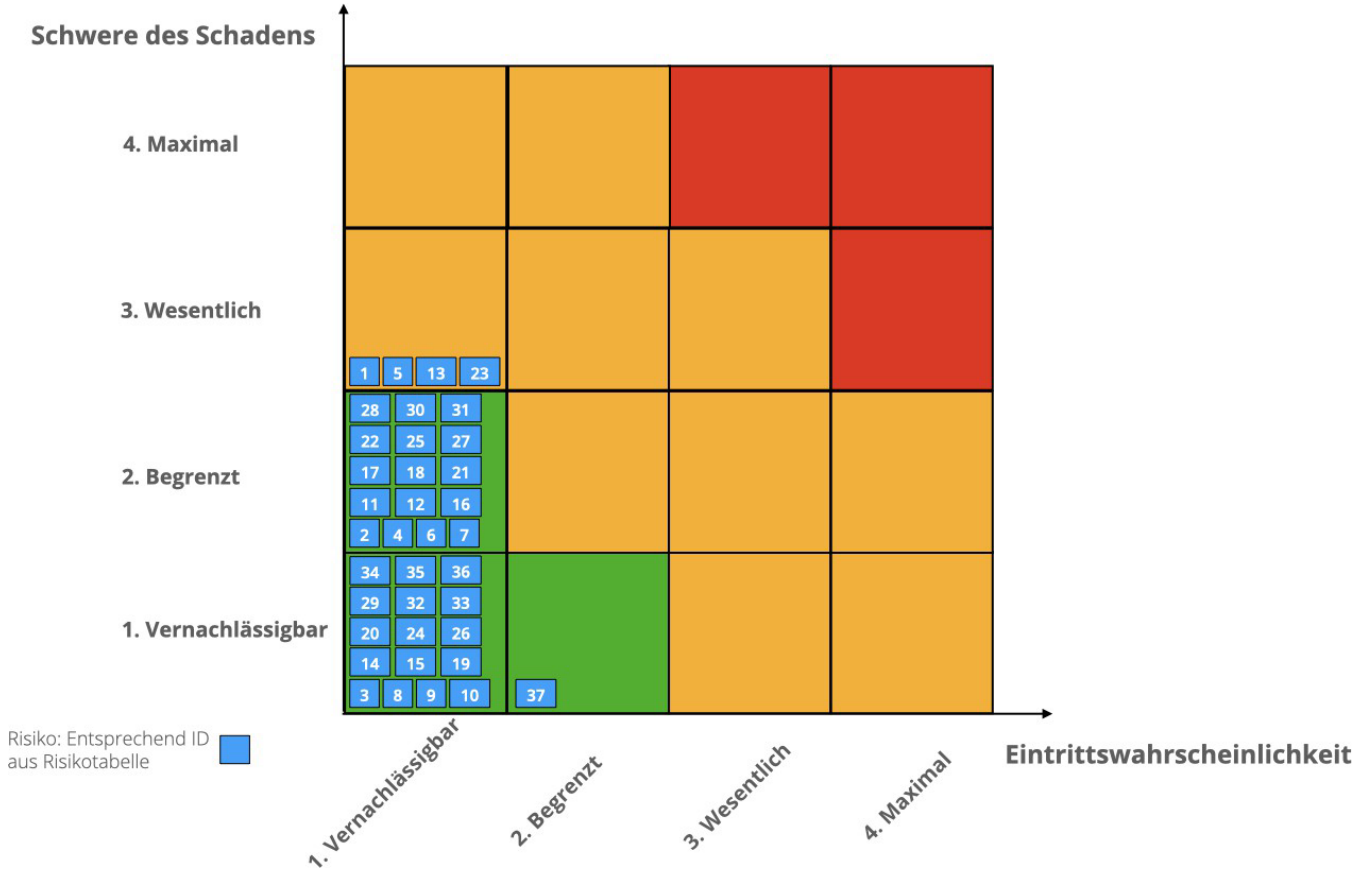
5.1. Risikoeinstufung aus Sicht des Betroffenen

Es ist zu bewerten, welche Risiken für Rechte und Freiheiten des Betroffenen der beschriebenen Verarbeitungsvorgänge bestehen. Hierzu wird die Risikoeinschätzung der Bitkom zu Grund gelegt. Diese ist in dem folgenden Diagramm in den relevanten Auszügen dargestellt:

Risiko-Niveau	1. Vernachlässigbar	2. Eingeschränkt	3. Signifikant	4. Maximal
Allgemeine Kategorisierung	Betroffene erleiden eventuell Unannehmlichkeiten, welche sie aber mit einigen Problemen überwinden können.	Betroffene erleiden eventuell signifikante Unannehmlichkeiten, welche Sie aber mit einigen Schwierigkeiten überwinden können.	Betroffene erleiden eventuell signifikante Konsequenzen, die sie nur mit ernsthaften Schwierigkeiten überwinden können.	Betroffene erleiden eventuell signifikante oder sogar unumkehrbare Konsequenzen, die sie nicht überwinden können.
Beispiele für materielle Auswirkungen	Zeitverlust bei Wiederholung von Formalitäten oder Warten, bis sie erfüllt werden	Unrichtiges oder unangebrachtes Profiling	Verlust des Arbeitsplatzes	Erhebliche Schulden; Unfähigkeit zu arbeiten
Beispiele für moralische Auswirkungen	Angst, die Kontrolle über die eigenen Daten zu verlieren; Gefühl der Verletzung der Privatsphäre ohne wirklichen oder objektiven Schaden (z. B. kommerzielle Eingriffe)	Probleme im Umgang mit privaten oder beruflichen Kontakten (z. B. Rufschädigung, keine Wiedererkennung);Verletzung der Privatsphäre ohne bleibende Schäden	Gefühl der Verletzung der Privatsphäre mit irreversiblen Schaden; Gefühl der Verwundbarkeit nach einer Vorladung vor Gericht	Langfristige oder dauerhafte psychische Beschwerden; strafrechtliche Verurteilung

5.2. Risikobewertung nach Umsetzung von Abhilfemaßnahmen

In der anfänglichen Risikobewertung wurden 37 Risiken für Betroffene identifiziert. Diese wurden entsprechend der Annahme klassifiziert, dass keinerlei Schutzmaßnahmen für diese Daten getroffen werden. Im zweiten Schritt der Risikobewertung wurden die entsprechenden Risiken unter Einbeziehung aller zuvor dargestellten Abhilfemaßnahmen erneut klassifiziert. Dabei entstand folgende Risikomatrix:



Durch die Maßnahmen zu Datensicherheit und Datenschutz werden die meisten Risiken mit einem Risikoscore von 2 bis 3 klassifiziert. Lediglich bei 4 Risiken wurde ein Risikoscore von 4 vergeben. Nach Analyse der Risiken wurden somit keine hohen Risiken identifiziert, die gegen eine Durchführung der Verarbeitungen in der Anwendung Evermood sprechen.

Eine detaillierte Dokumentation der Risiken findet sich in Anhang 2 - Risikotabelle nach Maßnahmen.

6. Bewertung der Notwendigkeit und Verhältnismäßigkeit

Da die Evermood GmbH bei der Verarbeitung als Auftragsverarbeiter für den jeweiligen Verantwortlichen tätig ist, kann eine Bewertung der Notwendigkeit und Verhältnismäßigkeit zur Erreichung der intendierten Zwecke für den Verantwortlichen nicht abschließend durch die Evermood GmbH durchgeführt werden. Diese Bewertung muss durch den jeweiligen Verantwortlichen erfolgen. Für eine solche Bewertung soll diese Datenschutzfolgenabschätzung als Grundlage für den Verantwortlichen dienen.

Aus Perspektive der Evermood GmbH werden durch den Auftragsverarbeiter ausreichende Maßnahmen zur Sicherung der verarbeiteten Daten getroffen, sodass keine hohen oder erheblichen Risiken bestehen, die gegen die Verhältnismäßigkeit der Verarbeitung sprechen würden. Das Angebot der Evermood Anwendung dient dem Verantwortlichen zur Beratung und Unterstützung seiner Beschäftigten bei arbeitsrelevanten, privaten, gesundheitlichen oder compliancebezogenen Anliegen. Das System ermöglicht Organisationen insbesondere:

- ihre Pflichten gem. §12 AGG zu wahren;
- ihre Arbeits- und betrieblichen Umweltschutzpflichten gem. § 89 BetrVG zu wahren;
- die EU-Hinweisgeberrichtlinie (EU) 2019/1937 umzusetzen.

7. Fazit - Abschließende Bewertung

Die Durchführung der Datenschutzfolgenabschätzung ergab bei der Betrachtung der Risiken für die Betroffenen der Verarbeitung, dass durch die Umsetzung von technischen und organisatorischen Maßnahmen durch den Auftragsverarbeiter Evermood GmbH keine Risiken bestehen, die als „Hoch" einzustufen sind. Nach dieser Bewertung existieren also keine bekannten Risiken, die gegen eine Durchführung der Verarbeitung sprechen. Bei der Betrachtung der Risiken wurde deutlich, dass die Risiken durch die Umsetzung der Maßnahmen zur Datensicherheit erheblich verringert werden konnten. Aufgrund dieser Maßnahmen ist davon auszugehen, dass gemäß der Risikoanalyse keine erhöhte Gefährdung für die Rechte und Freiheiten der Beschäftigten von der Verarbeitung ausgeht.

Dies führt die Beteiligten der Datenschutzfolgenabschätzung einhellig zu dem Ergebnis, dass die Datenschutzfolgenabschätzung keine Erkenntnisse geliefert hat, die gegen eine Durchführung der geplanten Verarbeitung spricht. Auf dieser Grundlage wird ebenfalls festgestellt, dass eine Konsultation der Aufsichtsbehörde nach Artikel 36 DSGVO nicht erforderlich ist.

Anhänge

- Anhang 1 - Risikotabelle vor Maßnahmen
- Anhang 2 - Risikotabelle nach Maßnahmen
- Anhang 3 - Löschkonzept

Anhang 1 - Risikotabelle vor Maßnahmen

ID	Risikoquelle	Risiko-beschreibung	Verarbeitungs-grundsatz	Möglicher Schaden	Schadenskategorie	Eintritts-wahrscheinlichkeit	Schwere des Schadens	Risikobewertung	Status / Kommentar
1	Hacker	Zugriff auf Daten im Rechenzentrum	Integrität und Vertraulichkeit	Offenlegung und Veröffentlichung von personenbezogenen Daten mit tlw. sensiblem Inhalt	Diskriminierung, Rufschädigung	3 - Wesentlich	3 - Wesentlich	4-6 - Risiko	
2	Hacker	Löschung oder Verschlüsselung der Daten im Rechenzentrum	Verfügbarkeit	Nutzung Evermood nicht möglich, Einschränkungen bei der Erteilung von Auskünften	Hinderung der Kontrolle der Betroffenen über eigene Daten	3 - Wesentlich	3 - Wesentlich	4-6 - Risiko	
3	Hacker	Abfangen der Kommunikation zwischen Nutzer und Webanwendung	Integrität und Vertraulichkeit	Offenlegung und Veröffentlichung von personenbezogenen Daten mit tlw. sensiblem Inhalt	Diskriminierung, Rufschädigung	3 - Wesentlich	3 - Wesentlich	4-6 - Risiko	
4	Hacker	Denial of Service-Angriff auf die Webanwendung	Verfügbarkeit	Nutzung Evermood nicht möglich, Einschränkungen bei der Erteilung von Auskünften	Hinderung der Kontrolle der Betroffenen über eigene Daten	3 - Wesentlich	2 - Begrenzt	4-6 - Risiko	
5	Hacker	Manipulation der Anwendung	Integrität und Vertraulichkeit	Offenlegung und Veröffentlichung von personenbezogenen Daten mit tlw. sensiblem Inhalt	Diskriminierung, Rufschädigung	2 - Begrenzt	3 - Wesentlich	4-6 - Risiko	
6	Hacker	Zugang zu interner IT-Infrastruktur Evermood - Zugriff auf Daten	Integrität und Vertraulichkeit	Offenlegung und Veröffentlichung von personenbezogenen Daten mit tlw. sensiblem Inhalt	Diskriminierung, Rufschädigung	3 - Wesentlich	2 - Begrenzt	4-6 - Risiko	
7	Hacker	Zugang zu interner IT-Infrastruktur Evermood - Verschlüsselung von Daten	Verfügbarkeit	Nutzung Evermood nicht möglich, Einschränkungen bei der Erteilung von Auskünften	Hinderung der Kontrolle der Betroffenen über eigene Daten	3 - Wesentlich	2 - Begrenzt	4-6 - Risiko	
8	Hacker	Einbruch Büroräume	Integrität und Vertraulichkeit	Offenlegung und Veröffentlichung von personenbezogenen Daten mit tlw. sensiblem Inhalt	Diskriminierung, Rufschädigung	2 - Begrenzt	2 - Begrenzt	4-6 - Risiko	
9	Mitarbeiter Evermood	Vorsätzliche Löschung der Daten in der Anwendung	Verfügbarkeit	Nutzung Evermood nicht möglich, Einschränkungen bei der Erteilung von Auskünften	Hinderung der Kontrolle der Betroffenen über eigene Daten	1 - Vernachlässigbar	3 - Wesentlich	4-6 - Risiko	
10	Mitarbeiter Evermood	Unbeabsichtigte Löschung der Daten in der Anwendung	Verfügbarkeit	Nutzung Evermood nicht möglich, Einschränkungen bei der Erteilung von Auskünften	Hinderung der Kontrolle der Betroffenen über eigene Daten	3 - Wesentlich	3 - Wesentlich	4-6 - Risiko	
11	Mitarbeiter Evermood	Vorsätzliche Löschung der Daten in der Datensicherung	Verfügbarkeit	Nutzung Evermood nicht möglich, Einschränkungen bei der Erteilung von Auskünften	Hinderung der Kontrolle der Betroffenen über eigene Daten	1 - Vernachlässigbar	3 - Wesentlich	4-6 - Risiko	
12	Mitarbeiter Evermood	Unbeabsichtigte Löschung der Daten in der Datensicherung	Verfügbarkeit	Nutzung Evermood nicht möglich, Einschränkungen bei der Erteilung von Auskünften	Hinderung der Kontrolle der Betroffenen über eigene Daten	3 - Wesentlich	3 - Wesentlich	4-6 - Risiko	
13	Mitarbeiter Evermood	Nicht autorisierter Zugriff auf personenbezogene Daten	Integrität und Vertraulichkeit	Offenlegung von personenbezogenen Daten mit tlw. Sensiblem Inhalt	Diskriminierung, Rufschädigung	3 - Wesentlich	3 - Wesentlich	4-6 - Risiko	
14	CTO Evermood	Vorsätzliche Löschung der Daten in der Anwendung	Verfügbarkeit	Nutzung Evermood nicht möglich, Einschränkungen bei der Erteilung von Auskünften	Hinderung der Kontrolle der Betroffenen über eigene Daten	1 - Vernachlässigbar	3 - Wesentlich	4-6 - Risiko	

15	CTO Evermood	Unbeabsichtigte Löschung der Daten in der Anwendung	Verfügbarkeit	Nutzung Evermood nicht möglich, Einschränkungen bei der Erteilung von Auskünften	Hinderung der Kontrolle der Betroffenen über eigene Daten	3 - Wesentlich	3 - Wesentlich	4-6 - Risiko	
16	CTO Evermood	Vorsätzliche Löschung der Daten in der Datensicherung	Verfügbarkeit	Nutzung Evermood nicht möglich, Einschränkungen bei der Erteilung von Auskünften	Hinderung der Kontrolle der Betroffenen über eigene Daten	1 - Vernachlässigbar	3 - Wesentlich	4-6 - Risiko	
17	CTO Evermood	Unbeabsichtigte Löschung der Daten in der Datensicherung	Verfügbarkeit	Nutzung Evermood nicht möglich, Einschränkungen bei der Erteilung von Auskünften	Hinderung der Kontrolle der Betroffenen über eigene Daten	3 - Wesentlich	3 - Wesentlich	4-6 - Risiko	
18	CTO Evermood	Nicht autorisierter Zugriff auf personenbezogene Daten	Integrität und Vertraulichkeit	Offenlegung von personenbezogenen Daten mit tlw. Sensiblem Inhalt	Diskriminierung, Rufschädigung	3 - Wesentlich	3 - Wesentlich	4-6 - Risiko	
19	Mitarbeiter Hostingdienstleister	Unbeabsichtigte Löschung der Daten in der Anwendung	Verfügbarkeit	Nutzung Evermood nicht möglich, Einschränkungen bei der Erteilung von Auskünften	Hinderung der Kontrolle der Betroffenen über eigene Daten	3 - Wesentlich	3 - Wesentlich	4-6 - Risiko	
20	Mitarbeiter Hostingdienstleister	Vorsätzliche Löschung der Daten in der Anwendung	Verfügbarkeit	Nutzung Evermood nicht möglich, Einschränkungen bei der Erteilung von Auskünften	Hinderung der Kontrolle der Betroffenen über eigene Daten	2 - Begrenzt	3 - Wesentlich	4-6 - Risiko	
21	Mitarbeiter Hostingdienstleister	Vorsätzliche Löschung der Daten in der Datensicherung	Verfügbarkeit	Nutzung Evermood nicht möglich, Einschränkungen bei der Erteilung von Auskünften	Hinderung der Kontrolle der Betroffenen über eigene Daten	2 - Begrenzt	3 - Wesentlich	4-6 - Risiko	
22	Mitarbeiter Hostingdienstleister	Unbeabsichtigte Löschung der Daten in der Datensicherung	Verfügbarkeit	Nutzung Evermood nicht möglich, Einschränkungen bei der Erteilung von Auskünften	Hinderung der Kontrolle der Betroffenen über eigene Daten	3 - Wesentlich	3 - Wesentlich	4-6 - Risiko	
23	Mitarbeiter Hostingdienstleister	Nicht autorisierter Zugriff auf personenbezogene Daten	Integrität und Vertraulichkeit	Offenlegung und Veröffentlichung von personenbezogenen Daten mit tlw. sensiblem Inhalt	Diskriminierung, Rufschädigung,	3 - Wesentlich	3 - Wesentlich	4-6 - Risiko	
24	IT-Infrastruktur (Evermood)	Ausfall der internen IT-Infrastruktur	Verfügbarkeit	Nutzung Evermood nicht möglich, Einschränkungen bei der Erteilung von Auskünften	Hinderung der Kontrolle der Betroffenen über eigene Daten	3 - Wesentlich	3 - Wesentlich	4-6 - Risiko	
25	IT-Infrastruktur (Evermood)	Ausfall der Kommunikationstechnologie	Verfügbarkeit	Einschränkung bei der Erteilung von Auskünften	Hinderung der Kontrolle der Betroffenen über eigene Daten	3 - Wesentlich	2 - Begrenzt	4-6 - Risiko	
26	IT-Infrastruktur (Evermood)	Diebstahl von IT-Systemen	Integrität und Vertraulichkeit	Offenlegung und Veröffentlichung von personenbezogenen Daten mit tlw. sensiblem Inhalt	Diskriminierung, Rufschädigung	2 - Begrenzt	3 - Wesentlich	4-6 - Risiko	
27	IT-Infrastruktur (Rechenzentrum Hostingdienstleister)	Ausfall eines Rechenzentrum aufgrund einer Katastrophe	Verfügbarkeit	Nutzung Evermood nicht möglich, Einschränkungen bei der Erteilung von Auskünften	Hinderung der Kontrolle der Betroffenen über eigene Daten	1 - Vernachlässigbar	3 - Wesentlich	4-6 - Risiko	
28	IT-Infrastruktur (Rechenzentrum Hostingdienstleister)	Ausfall eines Anwendungsservers	Verfügbarkeit	Nutzung Evermood nicht möglich, Einschränkungen bei der Erteilung von Auskünften	Hinderung der Kontrolle der Betroffenen über eigene Daten	3 - Wesentlich	3 - Wesentlich	4-6 - Risiko	
29	IT-Infrastruktur (Rechenzentrum Hostingdienstleister)	Diebstahl von IT-Systemen	Integrität und Vertraulichkeit	Offenlegung und Veröffentlichung von personenbezogenen Daten mit tlw. sensiblem Inhalt	Diskriminierung, Rufschädigung	2 - Begrenzt	3 - Wesentlich	4-6 - Risiko	
30	IT-Infrastruktur (Rechenzentrum Hostingdienstleister)	Defekt von IT-Systemen	Verfügbarkeit	Nutzung Evermood nicht möglich, Einschränkungen bei der Erteilung von Auskünften	Hinderung der Kontrolle der Betroffenen über eigene Daten	3 - Wesentlich	3 - Wesentlich	4-6 - Risiko	

31	IT-Infrastruktur (Rechenzentrum Hostingdienstleister)	Korruption der Daten in der Anwendung durch Software- oder Hardwarefehler	Verfügbarkeit	Nutzung Evermood nicht möglich, Einschränkungen bei der Erteilung von Auskünften	Hinderung der Kontrolle der Betroffenen über eigene Daten	2 - Begrenzt	3 - Wesentlich	4-6 - Risiko	
32	IT-Infrastruktur (Rechenzentrum Hostingdienstleister)	Unautorisierter physischer Zugang zu IT-Systemen	Integrität und Vertraulichkeit	Offenlegung und Veröffentlichung von personenbezogenen Daten mit tlw. sensiblem Inhalt	Diskriminierung, Rufschädigung	3 - Wesentlich	3 - Wesentlich	4-6 - Risiko	
33	IT-Infrastruktur (Rechenzentrum Hostingdienstleister)	Ausfall von IT-Systemen aufgrund von Schäden am Gebäude des Rechenzentrums	Verfügbarkeit	Nutzung Evermood nicht möglich, Einschränkungen bei der Erteilung von Auskünften	Hinderung der Kontrolle der Betroffenen über eigene Daten	1 - Vernachlässigbar	3 - Wesentlich	4-6 - Risiko	
34	IT-Infrastruktur (Rechenzentrum Hostingdienstleister)	Ausfall von IT-Systemen aufgrund von Feuer	Verfügbarkeit	Nutzung Evermood nicht möglich, Einschränkungen bei der Erteilung von Auskünften	Hinderung der Kontrolle der Betroffenen über eigene Daten	2 - Begrenzt	3 - Wesentlich	4-6 - Risiko	
35	IT-Infrastruktur (Rechenzentrum Hostingdienstleister)	Ausfall der Internetverbindung zum Rechenzentrum	Verfügbarkeit	Nutzung Evermood nicht möglich, Einschränkungen bei der Erteilung von Auskünften	Hinderung der Kontrolle der Betroffenen über eigene Daten	3 - Wesentlich	3 - Wesentlich	4-6 - Risiko	
36	IT-Infrastruktur (Rechenzentrum Hostingdienstleister)	Stromausfall im Rechenzentrum	Verfügbarkeit	Nutzung Evermood nicht möglich, Einschränkungen bei der Erteilung von Auskünften	Hinderung der Kontrolle der Betroffenen über eigene Daten	2 - Begrenzt	3 - Wesentlich	4-6 - Risiko	
37	IT-Infrastruktur (Evermood)	Verlust von IT-Systemen	Integrität und Vertraulichkeit	Offenlegung und Veröffentlichung von personenbezogenen Daten mit tlw. sensiblem Inhalt	Diskriminierung, Rufschädigung	2 - Begrenzt	3 - Wesentlich	4-6 - Risiko	

Anhang 2 - Risikotabelle nach Maßnahmen

ID	Risikoquelle	Risiko-beschreibung	Verarbeitungs-grundsatz	Möglicher Schaden	Schadens-kategorie	Eintritts-wahrscheinlichkeit	Schwere des Schadens	Risiko-bewertung	Maßnahme
1	Hacker	Zugriff auf Daten im Rechenzentrum	Integrität und Vertraulichkeit	Offenlegung und Veröffentlichung von personenbezogenen Daten mit tlw. sensiblem Inhalt	Diskriminierung, Rufschädigung	1 - Vernachlässigbar	3 - Wesentlich	4-6 - Risiko	Abschluss Auftragsverarbeitungsvereinbarung mit Hosting-Dienstleister. Umsetzung der Technischen und Organisatorischen Maßnahmen des Hosters. Regelmäßige Prüfung der Auditberichte des Hosters. Technische und Organisatorische Maßnahmen zum Schutz der Zugänge zur Server-Infrastruktur (Vergabe von Rechten nach Need-to-Know-Prinzip) Verschlüsselung der Daten im Rechenzentrum
2	Hacker	Löschung oder Verschlüsselung der Daten im Rechenzentrum	Verfügbarkeit	Nutzung Evermood nicht möglich, Einschränkungen bei der Erteilung von Auskünften	Hinderung der Kontrolle der Betroffenen über eigene Daten	1 - Vernachlässigbar	2 - Begrenzt	2-3 - Geringes Risiko	Abschluss Auftragsverarbeitungsvereinbarung mit Hosting-Dienstleister. Umsetzung der Technischen und Organisatorischen Maßnahmen des Hosters. Regelmäßige Prüfung der Auditberichte des Hosters. Technische und Organisatorische Maßnahmen zum Schutz der Zugänge zur Server-Infrastruktur (Vergabe von Rechten nach Need-to-Know-Prinzip)
3	Hacker	Abfangen der Kommunikation zwischen Nutzer und Webanwendung	Integrität und Vertraulichkeit	Offenlegung und Veröffentlichung von personenbezogenen Daten mit tlw. sensiblem Inhalt	Diskriminierung, Rufschädigung	1 - Vernachlässigbar	1 - Vernachlässigbar	2-3 - Geringes Risiko	Abschluss Auftragsverarbeitungsvereinbarung mit Hosting-Dienstleister. Umsetzung der Technischen und Organisatorischen Maßnahmen des Hosters. Regelmäßige Prüfung der Auditberichte des Hosters. Technische und Organisatorische Maßnahmen zum Schutz der Zugänge zur Server-Infrastruktur (Vergabe von Rechten nach Need-to-Know-Prinzip)
4	Hacker	Denial of Service-Angriff auf die Webanwendung	Verfügbarkeit	Nutzung Evermood nicht möglich, Einschränkungen bei der Erteilung von Auskünften	Hinderung der Kontrolle der Betroffenen über eigene Daten	1 - Vernachlässigbar	2 - Begrenzt	2-3 - Geringes Risiko	Abschluss Auftragsverarbeitungsvereinbarung mit Hosting-Dienstleister. Umsetzung der Technischen und Organisatorischen Maßnahmen des Hosters. Regelmäßige Prüfung der Auditberichte des Hosters. Technische und Organisatorische Maßnahmen zum Schutz der Zugänge zur Server-Infrastruktur (Vergabe von Rechten nach Need-to-Know-Prinzip) Durchführung von Penetrationstests Softwareentwicklung nach Vorgaben zur sicheren Entwicklung
5	Hacker	Manipulation der Anwendung	Integrität und Vertraulichkeit	Offenlegung und Veröffentlichung von personenbezogenen Daten mit tlw. sensiblem Inhalt	Diskriminierung, Rufschädigung	1 - Vernachlässigbar	3 - Wesentlich	4-6 - Risiko	Abschluss Auftragsverarbeitungsvereinbarung mit Hosting-Dienstleister. Umsetzung der Technischen und Organisatorischen Maßnahmen des Hosters. Regelmäßige Prüfung der Auditberichte des Hosters. Technische und Organisatorische Maßnahmen zum Schutz der Zugänge zur Server-Infrastruktur (Vergabe von Rechten nach Need-to-Know-Prinzip) Durchführung von Penetrationstests Softwareentwicklung nach Vorgaben zur sicheren Entwicklung

6	Hacker	Zugang zu interner IT-Infrastruktur Evermood - Zugriff auf Daten	Integrität und Vertraulichkeit	Offenlegung und Veröffentlichung von personenbezogenen Daten mit tlw. sensiblem Inhalt	Diskriminierung, Rufschädigung	1 - Vernachlässigbar	2 - Begrenzt	2-3 - Geringes Risiko	Technische und Organisatorische Maßnahmen zum Schutz der Zugänge zur Server-Infrastruktur (Vergabe von Rechten nach Need-to-Know-Prinzip) Nutzung eines Passwortmanagers Es werden keine personenbezogenen Daten aus der Anwendung innerhalb der internen IT-infrastruktur gespeichert
7	Hacker	Zugang zu interner IT-Infrastruktur Evermood - Verschlüsselung von Daten	Verfügbarkeit	Nutzung Evermood nicht möglich, Einschränkungen bei der Erteilung von Auskünften	Hinderung der Kontrolle der Betroffenen über eigene Daten	1 - Vernachlässigbar	2 - Begrenzt	2-3 - Geringes Risiko	Anwendung wird autark von IT-Infrastruktur des Unternehmens in einem Rechenzentrum betrieben. Ausfall der Infrastruktur von Evermood hat keine Auswirkungen auf die Anwendung Es werden keine personenbezogenen Daten aus der Anwendung innerhalb der internen IT-infrastruktur gespeichert
8	Hacker	Einbruch Büroräume	Integrität und Vertraulichkeit	Offenlegung und Veröffentlichung von personenbezogenen Daten mit tlw. sensiblem Inhalt	Diskriminierung, Rufschädigung	1 - Vernachlässigbar	1 - Vernachlässigbar	2-3 - Geringes Risiko	Technische und Organisatorische Maßnahmen für Zutrittsschutz Es werden keine personenbezogenen Daten der Anwendung in den Büroräumen gespeichert.
9	Mitarbeiter Evermood	Vorsätzliche Löschung der Daten in der Anwendung	Verfügbarkeit	Nutzung Evermood nicht möglich, Einschränkungen bei der Erteilung von Auskünften	Hinderung der Kontrolle der Betroffenen über eigene Daten	1 - Vernachlässigbar	1 - Vernachlässigbar	2-3 - Geringes Risiko	Technische und Organisatorische Maßnahmen zum Schutz der Zugänge zur Server-Infrastruktur (Vergabe von Rechten nach Need-to-Know-Prinzip) Datenschutzvereinbarung und Belehrung für alle Mitarbeiter Datensicherung
10	Mitarbeiter Evermood	Unbeabsichtigte Löschung der Daten in der Anwendung	Verfügbarkeit	Nutzung Evermood nicht möglich, Einschränkungen bei der Erteilung von Auskünften	Hinderung der Kontrolle der Betroffenen über eigene Daten	1 - Vernachlässigbar	1 - Vernachlässigbar	2-3 - Geringes Risiko	Technische und Organisatorische Maßnahmen zum Schutz der Zugänge zur Server-Infrastruktur (Vergabe von Rechten nach Need-to-Know-Prinzip) Datenschutzvereinbarung und Belehrung für alle Mitarbeiter Datensicherung
11	Mitarbeiter Evermood	Vorsätzliche Löschung der Daten in der Datensicherung	Verfügbarkeit	Nutzung Evermood nicht möglich, Einschränkungen bei der Erteilung von Auskünften	Hinderung der Kontrolle der Betroffenen über eigene Daten	1 - Vernachlässigbar	2 - Begrenzt	2-3 - Geringes Risiko	Technische und Organisatorische Maßnahmen zum Schutz der Zugänge zur Server-Infrastruktur (Vergabe von Rechten nach Need-to-Know-Prinzip) Datenschutzvereinbarung und Belehrung für alle Mitarbeiter Redundanz der Datensicherung
12	Mitarbeiter Evermood	Unbeabsichtigte Löschung der Daten in der Datensicherung	Verfügbarkeit	Nutzung Evermood nicht möglich, Einschränkungen bei der Erteilung von Auskünften	Hinderung der Kontrolle der Betroffenen über eigene Daten	1 - Vernachlässigbar	2 - Begrenzt	2-3 - Geringes Risiko	Technische und Organisatorische Maßnahmen zum Schutz der Zugänge zur Server-Infrastruktur (Vergabe von Rechten nach Need-to-Know-Prinzip) Datenschutzvereinbarung und Belehrung für alle Mitarbeiter Redundanz der Datensicherung
13	Mitarbeiter Evermood	Nicht autorisierter Zugriff auf personenbezogene Daten	Integrität und Vertraulichkeit	Offenlegung von personenbezogenen Daten mit tlw. Sensiblem Inhalt	Diskriminierung, Rufschädigung	1 - Vernachlässigbar	3 - Wesentlich	4-6 - Risiko	Technische und Organisatorische Maßnahmen zum Schutz der Zugänge zur Server-Infrastruktur (Vergabe von Rechten nach Need-to-Know-Prinzip) Mitarbeiter haben keinen Zugriff auf die personenbezogenen Daten in der Datenbank der Anwendung Datenschutzvereinbarung und Belehrung für alle Mitarbeiter
14	CTO Evermood	Vorsätzliche Löschung der Daten in der Anwendung	Verfügbarkeit	Nutzung Evermood nicht möglich, Einschränkungen bei der Erteilung von Auskünften	Hinderung der Kontrolle der Betroffenen über eigene Daten	1 - Vernachlässigbar	1 - Vernachlässigbar	2-3 - Geringes Risiko	Technische und Organisatorische Maßnahmen zum Schutz der Zugänge zur Server-Infrastruktur. Nur der CTO hat Zugriff auf die Datenbank. Datenschutzvereinbarung und Belehrung für alle Mitarbeiter Datensicherung

15	CTO Evermood	Unbeabsichtigte Löschung der Daten in der Anwendung	Verfügbarkeit	Nutzung Evermood nicht möglich, Einschränkungen bei der Erteilung von Auskünften	Hinderung der Kontrolle der Betroffenen über eigene Daten	1 - Vernachlässigbar	1 - Vernachlässigbar	2-3 - Geringes Risiko	Technische und Organisatorische Maßnahmen zum Schutz der Zugänge zur Server-Infrastruktur. Nur der CTO hat Zugriff auf die Datenbank. Eine Löschung muss mehrfach bestätigt werden. Datenschutzvereinbarung und Belehrung für alle Mitarbeiter Datensicherung
16	CTO Evermood	Vorsätzliche Löschung der Daten in der Datensicherung	Verfügbarkeit	Nutzung Evermood nicht möglich, Einschränkungen bei der Erteilung von Auskünften	Hinderung der Kontrolle der Betroffenen über eigene Daten	1 - Vernachlässigbar	2 - Begrenzt	2-3 - Geringes Risiko	Technische und Organisatorische Maßnahmen zum Schutz der Zugänge zur Server-Infrastruktur. Nur der CTO hat Zugriff auf die Datenbank. Datenschutzvereinbarung und Belehrung für alle Mitarbeiter Redundanz der Datensicherung
17	CTO Evermood	Unbeabsichtigte Löschung der Daten in der Datensicherung	Verfügbarkeit	Nutzung Evermood nicht möglich, Einschränkungen bei der Erteilung von Auskünften	Hinderung der Kontrolle der Betroffenen über eigene Daten	1 - Vernachlässigbar	2 - Begrenzt	2-3 - Geringes Risiko	Technische und Organisatorische Maßnahmen zum Schutz der Zugänge zur Server-Infrastruktur. Nur der CTO hat Zugriff auf die Datenbank. Eine Löschung muss mehrfach bestätigt werden. Datenschutzvereinbarung und Belehrung für alle Mitarbeiter Redundanz der Datensicherung
18	CTO Evermood	Nicht autorisierter Zugriff auf personenbezogene Daten	Integrität und Vertraulichkeit	Offenlegung von personenbezogenen Daten mit tlw. Sensiblem Inhalt	Diskriminierung, Rufschädigung	1 - Vernachlässigbar	2 - Begrenzt	2-3 - Geringes Risiko	Technische und Organisatorische Maßnahmen zum Schutz der Zugänge zur Server-Infrastruktur. Nur der CTO hat Zugriff auf die Datenbank. Datenschutzvereinbarung und Belehrung für alle Mitarbeiter
19	Mitarbeiter Hostingdienstleister	Unbeabsichtigte Löschung der Daten in der Anwendung	Verfügbarkeit	Nutzung Evermood nicht möglich, Einschränkungen bei der Erteilung von Auskünften	Hinderung der Kontrolle der Betroffenen über eigene Daten	1 - Vernachlässigbar	1 - Vernachlässigbar	2-3 - Geringes Risiko	Abschluss Auftragsverarbeitungsvereinbarung mit Hosting-Dienstleister. Umsetzung der Technischen und Organisatorischen Maßnahmen des Hosters. Regelmäßige Prüfung der Auditberichte des Hosters. Datensicherung
20	Mitarbeiter Hostingdienstleister	Vorsätzliche Löschung der Daten in der Anwendung	Verfügbarkeit	Nutzung Evermood nicht möglich, Einschränkungen bei der Erteilung von Auskünften	Hinderung der Kontrolle der Betroffenen über eigene Daten	1 - Vernachlässigbar	1 - Vernachlässigbar	2-3 - Geringes Risiko	Abschluss Auftragsverarbeitungsvereinbarung mit Hosting-Dienstleister. Umsetzung der Technischen und Organisatorischen Maßnahmen des Hosters. Regelmäßige Prüfung der Auditberichte des Hosters. Datensicherung
21	Mitarbeiter Hostingdienstleister	Vorsätzliche Löschung der Daten in der Datensicherung	Verfügbarkeit	Nutzung Evermood nicht möglich, Einschränkungen bei der Erteilung von Auskünften	Hinderung der Kontrolle der Betroffenen über eigene Daten	1 - Vernachlässigbar	2 - Begrenzt	2-3 - Geringes Risiko	Abschluss Auftragsverarbeitungsvereinbarung mit Hosting-Dienstleister. Umsetzung der Technischen und Organisatorischen Maßnahmen des Hosters. Regelmäßige Prüfung der Auditberichte des Hosters.
22	Mitarbeiter Hostingdienstleister	Unbeabsichtigte Löschung der Daten in der Datensicherung	Verfügbarkeit	Nutzung Evermood nicht möglich, Einschränkungen bei der Erteilung von Auskünften	Hinderung der Kontrolle der Betroffenen über eigene Daten	1 - Vernachlässigbar	2 - Begrenzt	2-3 - Geringes Risiko	Abschluss Auftragsverarbeitungsvereinbarung mit Hosting-Dienstleister. Umsetzung der Technischen und Organisatorischen Maßnahmen des Hosters. Regelmäßige Prüfung der Auditberichte des Hosters.
23	Mitarbeiter Hostingdienstleister	Nicht autorisierter Zugriff auf personenbezogene Daten	Integrität und Vertraulichkeit	Offenlegung und Veröffentlichung von personenbezogenen Daten mit tlw. sensiblem Inhalt	Diskriminierung, Rufschädigung	1 - Vernachlässigbar	3 - Wesentlich	4-6 - Risiko	Abschluss Auftragsverarbeitungsvereinbarung mit Hosting-Dienstleister. Umsetzung der Technischen und Organisatorischen Maßnahmen des Hosters. Regelmäßige Prüfung der Auditberichte des Hosters. Verschlüsselung der Daten im Rechenzentrum

24	IT-Infrastruktur (Evermood)	Ausfall der internen IT-Infrastruktur	Verfügbarkeit	Nutzung Evermood nicht möglich, Einschränkungen bei der Erteilung von Auskünften	Hinderung der Kontrolle der Betroffenen über eigene Daten	1 - Vernachlässigbar	1 - Vernachlässigbar	2-3 - Geringes Risiko	Anwendung wird autark von IT-Infrastruktur des Unternehmens in einem Rechenzentrum betrieben. Ausfall der Infrastruktur von Evermood hat keine Auswirkungen auf die Anwendung
25	IT-Infrastruktur (Evermood)	Ausfall der Kommunikationstechnologie	Verfügbarkeit	Einschränkung bei der Erteilung von Auskünften	Hinderung der Kontrolle der Betroffenen über eigene Daten	1 - Vernachlässigbar	2 - Begrenzt	2-3 - Geringes Risiko	Regelmäßige Prüfung und Wartung der Telekommunikationstechnologie
26	IT-Infrastruktur (Evermood)	Diebstahl von IT-Systemen	Integrität und Vertraulichkeit	Offenlegung und Veröffentlichung von personenbezogenen Daten mit tlw. sensiblem Inhalt	Diskriminierung, Rufschädigung	1 - Vernachlässigbar	1 - Vernachlässigbar	2-3 - Geringes Risiko	Technische und Organisatorische Maßnahmen zum Schutz vor Zugriff. Passwortschutz und Verschlüsselung von Datenträgern für alle Geräte. Es werden keine personenbezogenen Daten aus der Anwendung innerhalb der internen IT-infrastruktur gespeichert
27	IT-Infrastruktur (Rechenzentrum Hostingdienstleister)	Ausfall eines Rechenzentrum aufgrund einer Katastrophe	Verfügbarkeit	Nutzung Evermood nicht möglich, Einschränkungen bei der Erteilung von Auskünften	Hinderung der Kontrolle der Betroffenen über eigene Daten	1 - Vernachlässigbar	2 - Begrenzt	2-3 - Geringes Risiko	Verarbeitung der Daten in georedundanten Rechenzentren
28	IT-Infrastruktur (Rechenzentrum Hostingdienstleister)	Ausfall eines Anwendungsservers	Verfügbarkeit	Nutzung Evermood nicht möglich, Einschränkungen bei der Erteilung von Auskünften	Hinderung der Kontrolle der Betroffenen über eigene Daten	1 - Vernachlässigbar	2 - Begrenzt	2-3 - Geringes Risiko	Verarbeitung der Daten in georedundanten Rechenzentren Einsatz virtueller Server Spiegelung der Datenbestände
29	IT-Infrastruktur (Rechenzentrum Hostingdienstleister)	Diebstahl von IT-Systemen	Integrität und Vertraulichkeit	Offenlegung und Veröffentlichung von personenbezogenen Daten mit tlw. sensiblem Inhalt	Diskriminierung, Rufschädigung	1 - Vernachlässigbar	1 - Vernachlässigbar	2-3 - Geringes Risiko	Abschluss Auftragsverarbeitungsvereinbarung mit Hosting-Dienstleister. Umsetzung der Technischen und Organisatorischen Maßnahmen des Hosters. Regelmäßige Prüfung der Auditberichte des Hosters. Verschlüsselung der Daten im Rechenzentrum
30	IT-Infrastruktur (Rechenzentrum Hostingdienstleister)	Defekt von IT-Systemen	Verfügbarkeit	Nutzung Evermood nicht möglich, Einschränkungen bei der Erteilung von Auskünften	Hinderung der Kontrolle der Betroffenen über eigene Daten	1 - Vernachlässigbar	2 - Begrenzt	2-3 - Geringes Risiko	Abschluss Auftragsverarbeitungsvereinbarung mit Hosting-Dienstleister. Umsetzung der Technischen und Organisatorischen Maßnahmen des Hosters. Regelmäßige Prüfung der Auditberichte des Hosters. Verschlüsselung der Daten im Rechenzentrum Verarbeitung der Daten in georedundanten Rechenzentren Einsatz virtueller Server Spiegelung der Datenbestände
31	IT-Infrastruktur (Rechenzentrum Hostingdienstleister)	Korruption der Daten in der Anwendung durch Software- oder Hardwarefehler	Verfügbarkeit	Nutzung Evermood nicht möglich, Einschränkungen bei der Erteilung von Auskünften	Hinderung der Kontrolle der Betroffenen über eigene Daten	1 - Vernachlässigbar	2 - Begrenzt	2-3 - Geringes Risiko	Verarbeitung der Daten in georedundanten Rechenzentren Einsatz virtueller Server Spiegelung der Datenbestände
32	IT-Infrastruktur (Rechenzentrum Hostingdienstleister)	Unautorisierter physischer Zugang zu IT-Systemen	Integrität und Vertraulichkeit	Offenlegung und Veröffentlichung von personenbezogenen Daten mit tlw. sensiblem Inhalt	Diskriminierung, Rufschädigung	1 - Vernachlässigbar	1 - Vernachlässigbar	2-3 - Geringes Risiko	Abschluss Auftragsverarbeitungsvereinbarung mit Hosting-Dienstleister. Umsetzung der Technischen und Organisatorischen Maßnahmen des Hosters. Regelmäßige Prüfung der Auditberichte des Hosters. Zutrittsbeschränkungen des RZ-Betreibers Schutz der Daten durch Authentifizierungsmethoden Verschlüsselung der Daten im Rechenzentrum

33	IT-Infrastruktur (Rechenzentrum Hostingdienstleister)	Ausfall von IT-Systemen aufgrund von Schäden am Gebäude des Rechenzentrums	Verfügbarkeit	Nutzung Evermood nicht möglich, Einschränkungen bei der Erteilung von Auskünften	Hinderung der Kontrolle der Betroffenen über eigene Daten	1 - Vernachlässigbar	1 - Vernachlässigbar	2-3 - Geringes Risiko	Abschluss Auftragsverarbeitungsvereinbarung mit Hosting-Dienstleister. Umsetzung der Technischen und Organisatorischen Maßnahmen des Hosters. Regelmäßige Prüfung der Auditberichte des Hosters. Verarbeitung der Daten in georedundanten Rechenzentren Einsatz virtueller Server Spiegelung der Datenbestände
34	IT-Infrastruktur (Rechenzentrum Hostingdienstleister)	Ausfall von IT-Systemen aufgrund von Feuer	Verfügbarkeit	Nutzung Evermood nicht möglich, Einschränkungen bei der Erteilung von Auskünften	Hinderung der Kontrolle der Betroffenen über eigene Daten	1 - Vernachlässigbar	1 - Vernachlässigbar	2-3 - Geringes Risiko	Abschluss Auftragsverarbeitungsvereinbarung mit Hosting-Dienstleister. Umsetzung der Technischen und Organisatorischen Maßnahmen des Hosters. Regelmäßige Prüfung der Auditberichte des Hosters. Verarbeitung der Daten in georedundanten Rechenzentren Einsatz virtueller Server Spiegelung der Datenbestände
35	IT-Infrastruktur (Rechenzentrum Hostingdienstleister)	Ausfall der Internetverbindung zum Rechenzentrum	Verfügbarkeit	Nutzung Evermood nicht möglich, Einschränkungen bei der Erteilung von Auskünften	Hinderung der Kontrolle der Betroffenen über eigene Daten	1 - Vernachlässigbar	1 - Vernachlässigbar	2-3 - Geringes Risiko	Abschluss Auftragsverarbeitungsvereinbarung mit Hosting-Dienstleister. Umsetzung der Technischen und Organisatorischen Maßnahmen des Hosters. Regelmäßige Prüfung der Auditberichte des Hosters. Verarbeitung der Daten in georedundanten Rechenzentren Redundante Internetanbindung der Rechenzentren
36	IT-Infrastruktur (Rechenzentrum Hostingdienstleister)	Stromausfall im Rechenzentrum	Verfügbarkeit	Nutzung Evermood nicht möglich, Einschränkungen bei der Erteilung von Auskünften	Hinderung der Kontrolle der Betroffenen über eigene Daten	1 - Vernachlässigbar	1 - Vernachlässigbar	2-3 - Geringes Risiko	Abschluss Auftragsverarbeitungsvereinbarung mit Hosting-Dienstleister. Umsetzung der Technischen und Organisatorischen Maßnahmen des Hosters. Regelmäßige Prüfung der Auditberichte des Hosters. Verarbeitung der Daten in georedundanten Rechenzentren Notstromversorgung der Rechenzentren
37	IT-Infrastruktur (Evermood)	Verlust von IT-Systemen	Integrität und Vertraulichkeit	Offenlegung und Veröffentlichung von personenbezogenen Daten mit tlw. sensiblem Inhalt	Diskriminierung, Rufschädigung	2 - Begrenzt	1 - Vernachlässigbar	2-3 - Geringes Risiko	Technische und Organisatorische Maßnahmen zum Schutz vor Zugriff. Passwortschutz und Verschlüsselung von Datenträgern für alle Geräte. Es werden keine personenbezogenen Daten aus der Anwendung innerhalb der internen IT-infrastruktur gespeichert

Anhang 3 - Löschkonzept

1. Präambel

1.1. Dieses Löschkonzept behandelt die von Evermood im Rahmen unserer Kundenbeziehungen verarbeiteten Daten von Beschäftigten des Kunden und dient dem Kunden in seiner Rolle als "Verantwortlicher" i.S.d. DSGVO als Informationsquelle.

2. Einführung und Grundlagen

2.1. Personenbezogene Daten (pbD) dürfen gem. Art. 17 DSGVO nur so lange gespeichert werden, wie sie für die vorab festgelegten Zwecke benötigt werden oder eine gesetzliche Aufbewahrungspflicht dies verlangt. Sollten diese Zwecke nicht mehr bestehen und keine gesetzlichen Vorgaben entgegenstehen, müssen die pbD gelöscht werden. Eine unbegrenzte Aufbewahrung von pbD ist nicht zulässig.

2.2. Eine Löschung kann darüber hinaus aus einem der folgenden Gründe notwendig sein:

2.2.1. Die betroffene Person zieht ihre Einwilligung zurück oder legt Widerspruch gegen die Verarbeitung ein.

2.2.2. Die Datenverarbeitung war von vorneherein unzulässig.

2.2.3. Es besteht eine Rechtspflicht zur Löschung der pbD.

2.2.4. Der Rückbau von Systemen erfordert die Löschung von pbD.

2.3. Zweck dieses Löschkonzepts ist die Einhaltung der gesetzlichen Vorgaben sowie die Sicherstellung der Datensicherheit und des Datenschutzes der einzelnen Person. In diesem Löschkonzept werden daher Löschregeln festgelegt, die den verschiedenen Datenarten jeweils eine Regellöschfrist sowie einen definierten Startzeitpunkt für diese Frist zuweisen. Darüber hinaus finden sich in diesem Löschkonzept Vorgaben zur Implementierung der Löschregeln, zur Dokumentation von Löschvorgängen, zu Verantwortlichkeiten sowie zur regelmäßigen Pflege dieses Dokuments und der definierten Prozesse.

2.4. Das Löschkonzept wurde hierfür in Anlehnung an die Vorgaben der DIN 66398 erstellt.

2.5. Gegenstand dieses Löschkonzepts sind diejenigen pbD, die Evermood als "Auftragsverarbeiter" i.S.d. DSGVO vom Kunden und dessen Beschäftigten im Rahmen der Nutzung der Evermood Plattform erhält und verarbeitet.

2.6. Kunden von Evermood sind als "Verantwortlicher" i.S.d. DSGVO grundsätzlich für die Umsetzung und Einhaltung geeigneter Maßnahmen zum Schutz der Daten ihrer Beschäftigten verantwortlich. Beschäftigte können daher ihre Rechte als "betroffene Person" i.S.d. DSGVO grundsätzlich nur gegenüber dem Kunden geltend machen. Dieses Löschkonzept dient dem Kunden hierfür als Informationsquelle.

3. Begriffe

3.1. Sofern nicht explizit anderweitig definiert, gelten die Begriffsdefinitionen der DSGVO.

3.2. PbD gelten dann als gelöscht, wenn sie nach der Löschung nicht mehr vorhanden sind, unkenntlich sind und nicht mehr verwendet werden können. Dies kann z. B. durch das physische Überschreiben von Daten erreicht werden. Eine andere Option ist die geeignete Zerstörung des Datenträgers, auf dem sich die pbD befinden. Die Löschung von Daten ist unwiderruflich, das heißt gelöschte Daten können nicht wiederhergestellt werden. Die Löschung von Daten kann je nach Datenart auf Anfrage eines Users, Power-Users oder nach Ablauf gesetzter Fristen automatisch erfolgen.

3.3. **Ressourcen** sind sämtliche Dateien, Links und ähnliche Materialien, die von Evermood hochgeladen und den Beschäftigten zur Verfügung gestellt werden. Ressourcen können aus Textbausteinen, Links oder Dokumenten bestehen.

3.4. **Organisationsdaten** beinhalten sämtliche erfasste Informationen über den Kunden als Organisation. Daten in diesem Kontext können sein:

3.4.1. Name und Rechtsform der Organisation

3.4.2. Logo

3.4.3. Adresse (z. B. Sitz, Rechnungsadresse, Postadresse)

3.4.4. Telefonnummer(n) und E-Mail-Adresse(n)

3.4.5. Anzahl der Beschäftigten

3.5. **User** sind Beschäftigte des Kunden, die die Evermood Plattform nutzen.

3.6. **Power-User** können Beschäftigte des Kunden sowie externe natürliche oder juristische Personen sein. Power-User können je nach Berechtigung die Evermood Plattform verwalten, Nutzungsstatistiken einsehen und/oder Beratungsleistungen für User erbringen. Von Power-Usern erhobene Daten können sein:

3.6.1. Vorname

3.6.2. Nachname

3.6.3. E-Mail-Adresse

3.6.4. Telefonnummer

3.6.5. Passwort

3.6.6. Profilfoto

3.6.7. Datum des letzten Logins

3.6.8. Datum der Profilerstellung

3.6.9. Datum der letzten Aktualisierung der Profilinformationen

3.7. **Anliegen** sind jegliche Kontaktanfragen, die von Usern über Evermood an Power-User gesendet werden oder von Power-Usern in der Evermood Plattform dokumentiert werden. Daten in diesem Kontext können sein:

3.7.1. Freitext- und Multiple-Choice-Angaben

3.7.2. Chatnachrichten (inkl. Zeitstempel)

3.7.3. Metadaten zum Anliegen

4. Löschregeln nach Datenarten

4.1. Tabellarische Übersicht

4.1.1. Die nachfolgende Tabelle zeigt eine Übersicht der Löschregeln nach Datenart. Die genauen Bedingungen sind in den nachfolgenden Ziff. 4.2 bis 4.6 näher erläutert.

Datenart	Fristbeginn	Frist
Ressourcen	Löschantrag durch Evermood	Unmittelbar
	Vertragsende	1 Jahr
Organisationsdaten	Ende des Kalenderjahres, in dem der entsprechende Beleg entstanden ist.	10 Jahre
Power-User (Vollständiges Profil)	Löschantrag durch Evermood oder Power-User, Vertragsende	1 Jahr
Power-User (Optionale Einzeldaten)	Löschantrag durch Power-User oder Evermood (bspw. die Löschung einer Telefonnummer)	Unmittelbar
Anliegen	Löschantrag durch User oder Power-User	30 Tage
	Letzter Statuswechsel zu "abgeschlossen"	6, 12 oder 24 Monate

Authentifizierungs-Session	Schließen des Browser-Fensters	Unmittelbar

4.1.2. Die Daten können bis zu 14 Tage über die oben angegebenen Fristen hinaus aus einem Backup wiederhergestellt werden.

4.2. Ressourcen

4.2.1. Ressourcen können ausschließlich von Evermood hochgeladen werden.

4.2.2. Ressourcen werden in Absprache mit dem Kunden durch den Löschantrag von Evermood unmittelbar gelöscht.

4.2.3. Ressourcen werden nach Vertragsende 1 Jahr archiviert und anschließend gelöscht (zum Zweck einer einfachen Wiederherstellung des Systems bei einer etwaigen Wiederaufnahme des Kundenverhältnisses).

4.3. Organisationsdaten

4.3.1. Organisationsdaten können von ausgewählten Power-Usern oder von Evermood hochgeladen werden.

4.3.2. Organisationsdaten sind als Teil der von Evermood ausgestellten Rechnungen buchhaltungsrelevant und werden daher gemäß den gesetzlichen Aufbewahrungsvorschriften 10 Jahre archiviert und anschließend gelöscht.

4.4. Power-User

4.4.1. Daten von Power-Usern können von Evermood sowie teilweise von dem jeweiligen Power-User erstellt und gelöscht werden.

4.4.2. Vollständige Profile von Power-Usern werden nach Löschantrag oder nach Vertragsende 1 Jahr archiviert und anschließend gelöscht.

4.4.3. Vor- und Nachname des Power-Users werden auch nach Löschung des Profils weiterhin als Eigenschaft vergangener Anliegen gespeichert, in denen die Person aktiv war. Dies gilt für die gesamte Speicherdauer des betroffenen Anliegens.

4.4.4. Optionale Daten (d. h. deren Angabe nicht zwingend notwendig ist) werden durch den Löschantrag des Power-Users oder Evermoods unmittelbar gelöscht.

4.5. Anliegen

4.5.1. Anliegen können von Usern und Power-Usern erstellt werden.

4.5.2. User und Power-User, die ein Anliegen erstellt haben, können die Löschung von potenziell pbD (Freitext-Angaben und Chatnachrichten) beantragen, indem sie in dem jeweiligen Anliegen auf den Button "Meine Daten löschen" klicken.

4.5.3. Ausschließlich Power-User können den Bearbeitungsstatus eines Anliegens ändern. Wählt ein Power-User den Bearbeitungsstatus "abgeschlossen" aus, so gilt das Anliegen als "abgeschlossen", andernfalls gilt das Anliegen als "nicht abgeschlossen".

4.5.4. Alle potenziell pbD eines abgeschlossenen Anliegens werden nach der letzten Änderung des Bearbeitungsstatus von "nicht abgeschlossen" zu "abgeschlossen" 6, 12 oder 24 Monate archiviert und dann gelöscht. Die Frist bestimmt der Kunde.

4.5.5. Alle potenziell pbD eines Anliegens werden durch den Löschantrag des Users oder Power-Users 30 Tage archiviert und dann gelöscht.

4.5.6. Sofern sowohl der Bearbeitungsstatus des Anliegens "abgeschlossen" ist als auch ein Löschantrag durch den User oder Power-User gestellt wurde, so gilt das jeweils frühere Datum der Löschung.

4.6. Authentifizierung

4.6.1. Zur Authentifizierung von Usern wird ein JSON Web Token verwendet. Dieser wird bei jeder Anmeldung automatisch vom System erzeugt und nach Schließen des Browser-Fensters unmittelbar gelöscht.

5. Implementierungsvorgaben

5.1. Die oben gelisteten Daten werden von Evermood ausschließlich in digitaler Form vorgehalten. Die regelmäßige Löschung wird daher grundsätzlich durch automatisierte Systeme unter Aufsicht der Beschäftigten von Evermood durchgeführt und dokumentiert. Diese Systeme werden entsprechend der obigen Löschregeln konfiguriert.

5.2. Um der Speicherbegrenzung gerecht zu werden, werden vor Inbetriebnahme einer wiederhergestellten Datensicherung die für pbD relevanten, automatisierten Sperr- und Löschregeln auf die Daten angewandt. Hierdurch wird sichergestellt, dass Daten, welche zwischenzeitlich gelöscht wurden, aber in der Sicherung noch vorhanden waren, erneut gelöscht werden (Art. 5 DSGVO).

5.3. Die Löschung einzelner Daten, die Bestandteil einer Sicherungskopie sind, ist nicht möglich.

6. Sonderfälle

6.1. Sollten Daten in Ausnahmefällen in einem vom Regelbetrieb abweichenden Prozess verwendet werden (z. B. Gerichtsverfahren), so können sie für diese Verarbeitung einer anderen Datenart zugeordnet und folglich abweichend von obigen Löschfristen vorgehalten und verarbeitet werden, soweit dies nach den einschlägigen Rechtsvorschriften zulässig oder gefordert ist.

6.2. Zur Behandlung von Störfällen kann die Löschung zeitweise ausgesetzt werden.

6.3. Im Falle eines berechtigten Einzelbegehrens (Zurückziehung der Einwilligung oder Widerruf) einer betroffenen Person oder einer gesetzlichen Anordnung kann die Löschung von Daten manuell von entsprechend berechtigten Beschäftigten von Evermood durchgeführt werden. Eine solche Löschung wird schnellstmöglich, spätestens jedoch innerhalb von 30 Tagen nach Eingang des Begehrens vorgenommen, solange gesetzlich nichts anderes bestimmt ist.

6.4. Der Rückbau von Systemen kann gegebenenfalls die Löschung bestimmter Daten bedingen. In einem solchen Fall können Daten auch abweichend von den obigen Löschfristen vorgehalten und gelöscht werden, solange dies verhältnismäßig ist und im Rahmen der gesetzlichen Vorgaben liegt.

7. Dokumentation von Löschungen

7.1. Jegliche Löschung von Daten wird in einem Löschprotokoll dokumentiert. Dies gilt sowohl für die regelmäßige Löschung als auch für Sonderlöschungen i.S.d. vorigen Abschnittes. Löschprotokolle werden 3 Jahre getrennt vom laufenden Geschäftsbetrieb aufbewahrt.

8. Verantwortlichkeiten

8.1. Die Kunden von Evermood sind als "Verantwortlicher" i.S.d. DSGVO grundsätzlich für die Umsetzung und Einhaltung geeigneter Maßnahmen zum Schutz der Daten ihrer Beschäftigten verantwortlich. Beschäftigte können daher ihre Rechte als "betroffene Person" i.S.d. DSGVO grundsätzlich nur gegenüber dem Kunden geltend machen. Evermood stellt den Kunden als "Auftragsverarbeiter" i.S.d. DSGVO dieses Löschkonzept als Informationsquelle bereit.

8.2. Verantwortlich für die Festlegung der Bestimmungen dieses Dokuments, deren Einhaltung sowie die Pflege und regelmäßige Aktualisierung ist der/die Datenschutzbeauftragte von Evermood.

8.3. Der/Die Datenschutzbeauftragte ist ebenfalls zuständig für die Klärung von Anliegen und Beantwortung von Fragen zu diesem Löschkonzept.

8.4. Der/Die aktuelle Datenschutzbeauftragte wird im Auftragsverarbeitungsvertrag genannt.

9. Schlussbestimmungen

9.1. Dieses Löschkonzept wird einmal jährlich geprüft und bei Bedarf aktualisiert. Bei Änderungen in der Organisationsstruktur, Gestaltung der Produkte, Geschäftsabläufe, gesetzlicher Vorgaben oder sonstiger Gegebenheiten, die Auswirkungen auf die Bestimmungen dieses Dokuments haben oder haben könnten, wird ebenfalls eine Prüfung und Aktualisierung dieses Löschkonzepts vorgenommen.