Vereinbarung zur Auftragsverarbeitung nach Art. 28 DSGVO

Gegenstand: Nutzung der Softwareplattform Safetyeasy
Dokumentversion: 1.4
Stand: 16. August 2026

Vertragsparteien

[Firma des Auftraggebers], [Rechtsform]
[Straße und Hausnummer], [Postleitzahl und Ort], [Land]
vertreten durch [Name, Funktion]

– nachfolgend „Auftraggeber“ –

und

BLUVIT GmbH
Obergarten 22, 34253 Lohfelden, Deutschland
Amtsgericht Kassel, HRB 18250
vertreten durch den Geschäftsführer Timm Vollmer

– nachfolgend „Auftragnehmer“ oder „BLUVIT“ –

– gemeinsam „Parteien“ –

Präambel

Der Auftraggeber nutzt die von BLUVIT betriebene cloudbasierte Softwareplattform Safetyeasy. Bei der Bereitstellung, dem Betrieb, der Wartung, der Absicherung und der Unterstützung dieser Plattform verarbeitet BLUVIT personenbezogene Daten im Auftrag des Auftraggebers.

Diese Vereinbarung konkretisiert die Rechte und Pflichten der Parteien nach Art. 28 DSGVO. Sie gilt ergänzend zum Hauptvertrag über die Nutzung von Safetyeasy und geht diesem hinsichtlich der Auftragsverarbeitung vor.

§ 1 Gegenstand, Umfang und Abgrenzung

(1) BLUVIT stellt dem Auftraggeber Safetyeasy als Software-as-a-Service-Lösung zur Verfügung. Gegenstand der Auftragsverarbeitung sind die hierfür erforderlichen Tätigkeiten, insbesondere Bereitstellung und Betrieb der Anwendung, Hosting der Anwendungs-, Dokumenten- und Datenbankinhalte, Benutzer-, Mandanten- und Berechtigungsverwaltung, Datensicherung und Wiederherstellung, technischer Support einschließlich Fehleranalyse und Service-Desk-Bearbeitung, Wartungs- und Sicherheitsmaßnahmen, Versand transaktionaler

E-Mail-Benachrichtigungen, Protokollierung sicherheits- und betriebsrelevanter Ereignisse sowie Export, Berichtigung, Einschränkung und Löschung von Daten nach Weisung.

(2) Über die konkrete Nutzung von Safetyeasy und über die innerhalb der Plattform verarbeiteten Inhalte entscheidet allein der Auftraggeber. Die Einzelheiten der Verarbeitung ergeben sich aus Anlage 1.

(3) Diese Vereinbarung erfasst sämtliche Tätigkeiten, bei denen BLUVIT, ihre Beschäftigten oder eingesetzte Unterauftragsverarbeiter personenbezogene Daten aus dem Verantwortungsbereich des Auftraggebers verarbeiten.

(4) Nicht Gegenstand dieser Vereinbarung sind Verarbeitungen, bei denen BLUVIT selbst über Zwecke und wesentliche Mittel entscheidet und damit Verantwortlicher nach Art. 4 Nr. 7 DSGVO ist. Dies betrifft insbesondere Vertriebs- und Interessentendaten, Stammdaten von Kunden und Geschäftspartnern, geschäftliche Ansprechpartner, Angebote und Vertragsunterlagen, Bestellungen und Abonnements, Rechnungs-, Buchhaltungs-, Zahlungs- und Transaktionsdaten, die allgemeine Geschäftskommunikation, Daten zur Durchsetzung oder Abwehr rechtlicher Ansprüche sowie gesetzlich aufzubewahrende Geschäftsunterlagen. Diese Verarbeitungen sind in Anlage 3 dargestellt.

(5) BLUVIT setzt Odoo SaaS sowohl für den Service Desk zu Safetyeasy als auch für eigene CRM-, Angebots-, Vertrags-, Abonnement-, Rechnungs- und Buchhaltungsprozesse ein. Soweit im Service Desk personenbezogene Daten aus dem Verantwortungsbereich des Auftraggebers verarbeitet werden, handelt BLUVIT als Auftragsverarbeiter und Odoo als Unterauftragsverarbeiter nach Anlage 2. Für die übrigen in Absatz 4 genannten Zwecke handelt BLUVIT als eigener Verantwortlicher. Da beide Datenbestände in demselben System geführt werden können, richtet sich die datenschutzrechtliche Einordnung nach dem jeweiligen Verarbeitungszweck und dem konkreten Datensatz.

(6) In Odoo dürfen nur diejenigen Safetyeasy-Daten gespeichert werden, die für die Bearbeitung des jeweiligen Service-Desk-Vorgangs erforderlich sind. Eine routinemäßige Übernahme vollständiger Datenbestände oder Exporte aus Safetyeasy findet nicht statt. Passwörter, Authentifizierungsgeheimnisse, private Schlüssel, vollständige Zugriffstoken und vergleichbare Geheimnisse werden in Odoo nicht gespeichert.

(7) Stripe wird ausschließlich für eigene Zahlungs- und Abrechnungszwecke von BLUVIT eingesetzt und ist insoweit kein Unterauftragsverarbeiter des Auftraggebers.

(8) Für die in Safetyeasy bereitgestellten KI-Funktionen nutzt BLUVIT den IONOS AI Model Hub; eingesetzt wird derzeit das Modell Mistral Small 24B Instruct (mistralai/Mistral-Small-24B-Instruct). Das Modell verarbeitet textbasierte Eingaben und, soweit die betreffende Safetyeasy-Funktion aktiviert und genutzt wird, auch Bildinhalte; die Ausgabe erfolgt als Text. Werden dabei personenbezogene Daten des Auftraggebers als Prompt, Kontext, Dokumentauszug oder Bildinhalt übermittelt, erfolgt diese Verarbeitung im Auftrag des Auftraggebers; IONOS wird hierfür als Unterauftragsverarbeiter nach Anlage 2 eingesetzt. Übermittelt werden nur die für die jeweilige Funktion erforderlichen Daten; die Übermittlung vollständiger Safetyeasy-Datenbestände ist nicht vorgesehen.

(9) Ausgaben der KI-Funktionen sind automatisiert erzeugte Arbeitsergebnisse. Sie sind vor einer fachlich, rechtlich oder sicherheitsrelevanten Verwendung durch eine qualifizierte Person zu prüfen.

(10) BLUVIT darf das eingesetzte Modell durch ein funktional vergleichbares, ebenfalls über den IONOS AI Model Hub bereitgestelltes Modell ersetzen, sofern Unterauftragsverarbeiter, wesentlicher Verarbeitungszweck, Verarbeitungsort und Datenschutzniveau unverändert bleiben. Änderungen mit wesentlichen datenschutzrechtlichen Auswirkungen richten sich nach § 11.

§ 2 Dauer der Verarbeitung

(1) Die Auftragsverarbeitung beginnt mit der Bereitstellung von Safetyeasy, spätestens mit dem erstmaligen Zugriff von BLUVIT auf personenbezogene Daten des Auftraggebers, und erfolgt für die Dauer des Hauptvertrages.

(2) Diese Vereinbarung gilt über die Beendigung des Hauptvertrages hinaus fort, solange BLUVIT oder ein Unterauftragsverarbeiter personenbezogene Daten des Auftraggebers verarbeitet oder vorhält. Sie endet mit der vollständigen Rückgabe oder Löschung dieser Daten einschließlich des Ablaufs technisch bedingter Sicherungsfristen (§ 14).

§ 3 Weisungsrecht des Auftraggebers

(1) BLUVIT verarbeitet personenbezogene Daten des Auftraggebers ausschließlich auf dessen dokumentierte Weisung, zur Erfüllung des Hauptvertrages, nach Maßgabe dieser Vereinbarung oder aufgrund einer rechtlichen Verpflichtung.

(2) Als dokumentierte Weisung gilt die vertragsgemäße Nutzung und Konfiguration von Safetyeasy durch autorisierte Benutzer des Auftraggebers. Weisungen können darüber hinaus erfolgen durch Einstellungen innerhalb der Plattform, durch Bedienhandlungen autorisierter Benutzer, per E-Mail eines benannten Ansprechpartners, über die vereinbarten Supportkanäle sowie durch schriftliche oder elektronisch dokumentierte Zusatzvereinbarungen. Mündliche Weisungen sind vom Auftraggeber unverzüglich in Textform zu bestätigen.

(3) Ist BLUVIT der Auffassung, dass eine Weisung gegen die DSGVO oder sonstiges anwendbares Datenschutzrecht verstößt, informiert BLUVIT den Auftraggeber unverzüglich. BLUVIT ist berechtigt, die Ausführung der Weisung bis zu deren Bestätigung, Änderung oder Rücknahme auszusetzen.

(4) BLUVIT ist nicht verpflichtet, Weisungen auszuführen, die rechtswidrig oder technisch nicht umsetzbar sind oder die den sicheren Betrieb der Plattform, die Rechte anderer Kunden oder die Rechte betroffener Personen gefährden.

(5) Ist BLUVIT nach Unionsrecht oder dem Recht eines Mitgliedstaats zu einer Verarbeitung verpflichtet, teilt BLUVIT dem Auftraggeber die rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses untersagt.

(6) Aufwände, die durch individuelle Weisungen über die Standardfunktionen von Safetyeasy hinaus entstehen, können nach vorheriger Abstimmung nach Maßgabe des Hauptvertrages vergütet werden.

§ 4 Verantwortung und Mitwirkung des Auftraggebers

(1) Der Auftraggeber bleibt Verantwortlicher im Sinne des Art. 4 Nr. 7 DSGVO. Er verantwortet insbesondere die Rechtmäßigkeit der Verarbeitung und das Vorliegen geeigneter Rechtsgrundlagen, die Erfüllung der Informationspflichten und die Wahrung der Betroffenenrechte, die Richtigkeit der verarbeiteten Daten und die Einhaltung der Datenminimierung, die Festlegung von Aufbewahrungs- und Löschfristen, die Vergabe und Überprüfung von Benutzerrechten, die Durchführung erforderlicher Datenschutz-Folgenabschätzungen, die Rechtmäßigkeit seiner Weisungen sowie die Zulässigkeit der Verarbeitung besonderer Kategorien personenbezogener Daten.

(2) Der Auftraggeber stellt sicher, dass ausschließlich berechtigte Personen Zugang zu Safetyeasy erhalten. Benutzerkonten sind personenbezogen zu vergeben; gemeinsam genutzte Konten sind zu vermeiden. Nicht mehr erforderliche Konten und Berechtigungen sind unverzüglich zu sperren oder zu entfernen.

(3) Besondere Kategorien personenbezogener Daten nach Art. 9 DSGVO darf der Auftraggeber nur verarbeiten, soweit dies erforderlich und rechtlich zulässig ist und geeignete Schutzmaßnahmen bestehen. In transaktionalen E-Mail-Benachrichtigungen sind solche Daten sowie detaillierte Safetyeasy-Inhalte nicht aufzunehmen.

(4) Die weiteren Mitwirkungspflichten des Auftraggebers ergeben sich aus Anlage 4 Ziffer 24.

§ 5 Pflichten von BLUVIT

(1) BLUVIT verarbeitet personenbezogene Daten ausschließlich im vereinbarten Umfang und entsprechend den dokumentierten Weisungen des Auftraggebers. Eine Verarbeitung für eigene Werbezwecke, der Verkauf von Daten sowie nicht vereinbarte Profiling- oder Analysezwecke sind ausgeschlossen.

(2) BLUVIT gewährleistet, dass die zur Verarbeitung befugten Personen zur Vertraulichkeit verpflichtet wurden oder einer entsprechenden gesetzlichen Verschwiegenheitspflicht unterliegen. Der Zugriff wird über ein rollenbasiertes Berechtigungsmodell nach dem Need-to-know- und dem Least-Privilege-Prinzip auf diejenigen Personen beschränkt, die ihn zur Aufgabenerfüllung benötigen.

(3) Ein Zugriff von Beschäftigten der BLUVIT auf produktive Kundendaten erfolgt ausschließlich, soweit dies für Support, Fehleranalyse, Wartung, Sicherheitsmaßnahmen, Wiederherstellung, die Umsetzung von Weisungen oder zur Erfüllung gesetzlicher Pflichten erforderlich ist. Support- und Fehleranalysen werden, soweit möglich, mit anonymisierten, pseudonymisierten oder technisch reduzierten Informationen durchgeführt.

(4) Produktivdaten werden nicht für Entwicklungs- oder Testzwecke verwendet, es sei denn, sie wurden zuvor wirksam anonymisiert oder es liegt eine dokumentierte Weisung des Auftraggebers vor.

(5) BLUVIT berichtigt, löscht oder beschränkt personenbezogene Daten nach dokumentierter Weisung des Auftraggebers, soweit dieser die Maßnahme nicht selbst über die Funktionen von Safetyeasy vornehmen kann.

(6) BLUVIT führt ein Verzeichnis der Kategorien von Verarbeitungstätigkeiten nach Art. 30 Abs. 2 DSGVO und stellt dem Auftraggeber auf Anfrage die zur Erfüllung seiner Nachweispflichten erforderlichen Informationen zur Verfügung.

(7) Für den Service Desk gilt ergänzend: Es werden nur die zur Bearbeitung erforderlichen Angaben verarbeitet, insbesondere Kontakt- und Benutzerinformationen, Mandantenzuordnung, Fehlerbeschreibung, technische Metadaten, Kommunikation, Anhänge und Bearbeitungshistorie. Screenshots, Protokolldateien und sonstige Anhänge werden vor der Speicherung, soweit möglich, um nicht erforderliche personenbezogene Daten und um Geheimnisse bereinigt. Besondere Kategorien personenbezogener Daten werden nur gespeichert, soweit dies für die konkrete Supportbearbeitung zwingend erforderlich und rechtlich zulässig ist. Auftragsbezogene Service-Desk-Daten werden durch Rollen, organisatorische Vorgaben und getrennte Löschprozesse von den in § 1 Abs. 4 genannten eigenverantwortlichen Datenbeständen unterschieden.

(8) Für die KI-Funktionen gilt ergänzend: BLUVIT beschränkt Prompts, Kontextdaten und Dokumentauszüge auf das für die jeweilige Funktion erforderliche Maß und minimiert, pseudonymisiert oder entfernt personenbezogene Daten vor der Übermittlung, soweit dies technisch und fachlich möglich ist. Passwörter, private Schlüssel, API-Schlüssel, vollständige Zugriffstoken und vergleichbare Authentifizierungsgeheimnisse werden nicht an das Modell übermittelt. Modellausgaben werden nicht allein deshalb als sachlich richtig, vollständig oder verbindlich behandelt, weil sie automatisiert erzeugt wurden.

§ 6 Vertraulichkeit

(1) BLUVIT behandelt alle im Rahmen der Auftragsverarbeitung bekannt gewordenen Informationen vertraulich. Die Verpflichtung besteht nach Beendigung des Vertragsverhältnisses fort.

(2) Beschäftigte werden vor Aufnahme ihrer Tätigkeit auf die Vertraulichkeit verpflichtet und regelmäßig geschult.

(3) Eine Weitergabe personenbezogener Daten ist nur im Rahmen dokumentierter Weisungen, an genehmigte Unterauftragsverarbeiter oder aufgrund einer rechtlichen Verpflichtung zulässig.

---

§ 7 Technische und organisatorische Maßnahmen

(1) BLUVIT trifft die in Anlage 4 beschriebenen technischen und organisatorischen Maßnahmen nach Art. 32 DSGVO. Die Maßnahmen gewährleisten unter Berücksichtigung des Stands der Technik, der Implementierungskosten sowie der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung und der Eintrittswahrscheinlichkeit und Schwere der Risiken ein dem Risiko angemessenes Schutzniveau.

(2) Die Maßnahmen unterliegen der technischen Weiterentwicklung. BLUVIT darf einzelne Maßnahmen durch gleichwertige oder höherwertige ersetzen; das vereinbarte Schutzniveau darf dabei nicht unterschritten werden. Wesentliche Änderungen des Schutzniveaus teilt BLUVIT dem Auftraggeber mit.

(3) Die Maßnahmen von BLUVIT entbinden den Auftraggeber nicht von seiner Verantwortung für die eigenen Endgeräte, die eigene Identitäts- und Benutzerverwaltung, die eigenen Netzwerke und Benutzerrechte sowie für die Rechtmäßigkeit der eingegebenen Inhalte.

---

§ 8 Unterstützung bei Betroffenenrechten

(1) BLUVIT unterstützt den Auftraggeber unter Berücksichtigung der Art der Verarbeitung mit geeigneten technischen und organisatorischen Maßnahmen bei der Erfüllung der Betroffenenrechte nach Art. 12 bis 22 DSGVO, insbesondere bei Auskunft, Berichtigung, Löschung, Einschränkung, Datenübertragbarkeit, Widerspruch und Nachweis der Verarbeitung.

(2) Wendet sich eine betroffene Person unmittelbar an BLUVIT, leitet BLUVIT die Anfrage unverzüglich an den Auftraggeber weiter und trifft ohne dessen Weisung keine inhaltliche Entscheidung.

(3) Aufwände, die über die Standardfunktionen von Safetyeasy hinausgehen, können nach vorheriger Abstimmung vergütet werden.

---

§ 9 Verletzungen des Schutzes personenbezogener Daten

(1) BLUVIT informiert den Auftraggeber unverzüglich über jede Verletzung des Schutzes personenbezogener Daten, soweit Daten des Auftraggebers betroffen sind. Die Erstinformation erfolgt ohne schuldhaftes Zögern und, soweit nach den Umständen möglich, innerhalb von 24 Stunden nach Bekanntwerden bei BLUVIT.

(2) Die Erstinformation enthält, soweit verfügbar, Art und Umfang des Vorfalls, den Zeitpunkt oder vermuteten Zeitraum, die betroffenen Systeme und Datenkategorien, die Kategorien und die ungefähre Zahl betroffener Personen und Datensätze, die möglichen Folgen, die bereits ergriffenen oder geplanten Gegenmaßnahmen sowie die Kontaktdaten eines Ansprechpartners. Noch nicht verfügbare Informationen werden schrittweise und ohne unangemessene Verzögerung nachgereicht.

(3) BLUVIT unterstützt den Auftraggeber bei der Risikobewertung, bei der Meldung nach Art. 33 DSGVO und einer etwaigen Benachrichtigung nach Art. 34 DSGVO sowie bei Untersuchung, Eindämmung und Dokumentation des Vorfalls.

(4) Die Entscheidung über Meldungen an Aufsichtsbehörden oder Benachrichtigungen betroffener Personen obliegt

dem Auftraggeber, soweit BLUVIT nicht selbst gesetzlich verpflichtet ist.

---

§ 10 Datenschutz-Folgenabschätzung und vorherige Konsultation

(1) BLUVIT unterstützt den Auftraggeber unter Berücksichtigung der Art der Verarbeitung und der verfügbaren Informationen bei der Prüfung und Durchführung einer Datenschutz-Folgenabschätzung nach Art. 35 DSGVO sowie bei einer vorherigen Konsultation nach Art. 36 DSGVO.

(2) BLUVIT stellt hierfür insbesondere Informationen zu technischer Architektur, Verarbeitungstätigkeiten, Unterauftragsverarbeitern, Speicher- und Verarbeitungsorten, Sicherheitsmaßnahmen und bekannten Drittlandübermittlungen bereit.

(3) Darüber hinausgehende Beratungs-, Prüf- oder Dokumentationsleistungen können gesondert vergütet werden.

---

§ 11 Unterauftragsverarbeiter

(1) Der Auftraggeber erteilt BLUVIT eine allgemeine schriftliche Genehmigung zur Beauftragung der in Anlage 2 aufgeführten direkten Unterauftragsverarbeiter.

(2) BLUVIT informiert den Auftraggeber vor der Beauftragung eines neuen oder der Ersetzung eines bestehenden direkten Unterauftragsverarbeiters, grundsätzlich mindestens 30 Kalendertage vor dem beabsichtigten Einsatz. Die Information kann per E-Mail, über Safetyeasy, über eine dauerhaft verfügbare Unterauftragsverarbeiterliste oder durch eine aktualisierte Vertragsanlage erfolgen.

(3) Der Auftraggeber kann der beabsichtigten Beauftragung innerhalb von 14 Kalendertagen nach Zugang der Information aus einem wichtigen datenschutzrechtlichen Grund widersprechen. Der Widerspruch bedarf der Textform, hat den betroffenen Anbieter zu benennen und den konkreten datenschutzrechtlichen Grund darzulegen.

(4) Die Parteien bemühen sich in diesem Fall um eine einvernehmliche Lösung. Ist eine alternative Leistungserbringung technisch oder wirtschaftlich nicht zumutbar, kann jede Partei den betroffenen Dienst oder den Hauptvertrag außerordentlich kündigen.

(5) BLUVIT verpflichtet direkte Unterauftragsverarbeiter vertraglich auf ein im Wesentlichen gleichwertiges Datenschutzniveau und bleibt gegenüber dem Auftraggeber für die Erfüllung von deren Pflichten verantwortlich.

(6) BLUVIT dokumentiert die Verarbeitungskette einschließlich der bekannten weiteren Unterauftragsverarbeiter der direkten Anbieter. Diese werden dem Auftraggeber auf Anfrage mitgeteilt oder über die offiziellen Anbieterlisten zugänglich gemacht.

---

§ 12 Verarbeitungsorte und Drittlandübermittlungen

(1) Produktive Safetyeasy-Anwendungs-, Dokumenten- und Datenbankdaten werden in der vertraglich festgelegten IONOS-Cloud-Region in Deutschland verarbeitet.

(2) KI-Eingaben und -Ausgaben werden über den IONOS AI Model Hub verarbeitet. Nach der maßgeblichen IONOS-Produktbeschreibung werden die Dienste des AI Model Hub einschließlich der Inferenz-Endpunkte und etwaiger verwalteter Vektordatenbanken in Rechenzentren in Deutschland betrieben. Der Inferenzdienst wird zustandslos genutzt; Prompts und Modellausgaben werden nach Abschluss der jeweiligen Sitzung verworfen und

nicht zur Weiterentwicklung oder zum Training der bereitgestellten Modelle verwendet.

(3) Nutzt BLUVIT künftig die Data-Collections- oder RAG-Funktion des IONOS AI Model Hub, sind die dort gespeicherten Dokumente, Embeddings und Vektordaten als eigenständige auftragsbezogene Speicherung zu behandeln und in den Lösch-, Berechtigungs- und Dokumentationsprozessen zu berücksichtigen.

(4) Auftragsbezogene Service-Desk-Daten werden in Odoo SaaS verarbeitet. Für die eingesetzte Odoo-Datenbank liegt eine individuelle Anbieterbestätigung vor, wonach die Datenbank der Hostingregion Europa zugeordnet ist und Frankfurt als primärer Produktionsstandort verwendet wird. Diese Bestätigung beinhaltet keine Zusicherung, dass sämtliche Sicherungs-, Replikations-, Support- oder Notfallkopien ausschließlich in Frankfurt gespeichert oder ausschließlich von dort verarbeitet werden. Weitere Speicherorte, Sicherungskopien, Replikationen und administrative Zugriffe richten sich nach den jeweils geltenden Vertrags-, Datenschutz- und Unterauftragsverarbeiterbedingungen von Odoo; BLUVIT dokumentiert die Standortbestätigung und überprüft die maßgeblichen Angaben regelmäßig.

(5) Der Versand transaktionaler E-Mails erfolgt über Mailtrap. Mailtrap kann personenbezogene Daten außerhalb des Europäischen Wirtschaftsraums verarbeiten oder durch weitere Unterauftragsverarbeiter verarbeiten lassen.

(6) Soweit ein eingesetzter Unterauftragsverarbeiter personenbezogene Daten in einem Drittland verarbeitet oder von dort aus zugänglich macht, erfolgt dies nur unter den Voraussetzungen der Art. 44 bis 49 DSGVO. Als Übermittlungsgrundlage kommen insbesondere ein Angemessenheitsbeschluss der Europäischen Kommission, eine wirksame Zertifizierung nach dem EU-US Data Privacy Framework, die Standardvertragsklauseln der Europäischen Kommission, verbindliche interne Datenschutzvorschriften oder sonstige gesetzlich zulässige Garantien in Betracht. Die für den jeweiligen Anbieter maßgebliche Grundlage ist in Anlage 2 ausgewiesen.

(7) Der Auftraggeber weist BLUVIT an, die für den Versand transaktionaler E-Mails, für die Bearbeitung von Service-Desk-Vorgängen und für die Nutzung aktivierter KI-Funktionen erforderlichen Daten nach Maßgabe dieser Vereinbarung an Mailtrap, Odoo beziehungsweise den IONOS AI Model Hub zu übermitteln.

(8) E-Mail-, Service-Desk- und KI-Inhalte sind auf das erforderliche Mindestmaß zu beschränken. Besondere Kategorien personenbezogener Daten, detaillierte Unfallinformationen, Gesundheitsdaten und vollständige Safetyeasy-Dokumente werden nicht in transaktionalen E-Mails versandt; ihre Speicherung in einem Service-Desk-Vorgang ist nur zulässig, soweit sie für dessen Bearbeitung zwingend erforderlich ist.

---

§ 13 Kontroll- und Nachweisrechte

(1) BLUVIT stellt dem Auftraggeber alle Informationen zur Verfügung, die zum Nachweis der Einhaltung dieser Vereinbarung und der Anforderungen des Art. 28 DSGVO erforderlich sind. Als Nachweise kommen insbesondere Zertifikate, Audit- und Prüfberichte, Sicherheitskonzepte, Auszüge aus Richtlinien, Selbstauskünfte und technische Dokumentationen in Betracht.

(2) Der Auftraggeber kann Prüfungen selbst oder durch einen unabhängigen, zur Vertraulichkeit verpflichteten Prüfer durchführen lassen. Prüfungen erfolgen während der üblichen Geschäftszeiten, nach Ankündigung mit einer Frist von mindestens 14 Kalendertagen, ohne unverhältnismäßige Beeinträchtigung des Betriebs und unter Wahrung der Rechte anderer Kunden. Sie sollen vorrangig auf vorhandene Dokumentationen, Zertifikate und Auditberichte gestützt werden.

(3) Eine unangekündigte Prüfung ist zulässig, wenn konkrete Anhaltspunkte für eine erhebliche Verletzung des Schutzes personenbezogener Daten bestehen und eine vorherige Ankündigung den Prüfzweck gefährden würde.

(4) Ein unmittelbarer Zutritt zu Rechenzentren oder Systemen von Unterauftragsverarbeitern ist nur im Rahmen der dort geltenden Sicherheits- und Vertragsbedingungen möglich.

(5) Die Kosten einer vom Auftraggeber veranlassten Prüfung trägt dieser, soweit die Prüfung keinen

wesentlichen Verstoß von BLUVIT feststellt. Gesetzliche Kontrollrechte der Aufsichtsbehörden bleiben unberührt.

§ 14 Rückgabe und Löschung

(1) Nach Beendigung des Hauptvertrages stellt BLUVIT dem Auftraggeber die vorhandenen Standardexportfunktionen für 30 Kalendertage in einem auf den Export beschränkten Zugang zur Verfügung. Für die rechtzeitige Sicherung beziehungsweise den Export seiner Daten ist der Auftraggeber verantwortlich.

(2) Mit Ablauf des Exportzeitraums, also 30 Kalendertage nach Vertragsende, werden die produktiven Kundendaten gelöscht, soweit keine abweichende Vereinbarung getroffen wurde und keine gesetzliche Aufbewahrungspflicht entgegensteht. Daten in Sicherungskopien werden im Rahmen der regulären Sicherungszyklen überschrieben oder gelöscht; die maximale Vorhaltezeit beträgt 90 Tage, soweit die eingesetzte technische Plattform keine kürzere Frist vorsieht.

(3) Bis zur endgültigen Löschung unterliegen die Daten weiterhin den Schutzmaßnahmen dieser Vereinbarung. Gesetzlich aufzubewahrende Daten werden für die operative Verarbeitung gesperrt und ausschließlich für den gesetzlichen Zweck verarbeitet.

(4) BLUVIT bestätigt die Löschung auf begründete Anfrage in Textform.

(5) Die eigenen Vertrags-, CRM-, Rechnungs-, Buchhaltungs- und Zahlungsdaten von BLUVIT (§ 1 Abs. 4, Anlage 3) unterfallen dieser Löschregelung nicht.

§ 15 Haftung

(1) Für die Haftung gelten die gesetzlichen Bestimmungen, insbesondere Art. 82 DSGVO, sowie ergänzend die Regelungen des Hauptvertrages. Die Parteien haften entsprechend ihren jeweiligen Verantwortungs- und Verursachungsbeiträgen.

(2) Der Auftraggeber haftet insbesondere für rechtswidrige Inhalte, unzulässige Weisungen und fehlende Rechtsgrundlagen in seinem Verantwortungsbereich.

(3) BLUVIT haftet für Verstöße gegen die speziell an Auftragsverarbeiter gerichteten Pflichten sowie für Verarbeitungen außerhalb rechtmäßiger Weisungen.

§ 16 Schlussbestimmungen

(1) Änderungen und Ergänzungen dieser Vereinbarung bedürfen mindestens der Textform.

(2) Ist eine Bestimmung dieser Vereinbarung ganz oder teilweise unwirksam, bleibt die Wirksamkeit der übrigen Bestimmungen unberührt.

(3) Bei Widersprüchen zwischen dem Hauptvertrag und dieser Vereinbarung geht diese Vereinbarung hinsichtlich der Auftragsverarbeitung vor. Bei Widersprüchen zwischen dieser Vereinbarung und zwingendem Datenschutzrecht geht das zwingende Datenschutzrecht vor.

(4) Es gilt das Recht der Bundesrepublik Deutschland. Gerichtsstand ist, soweit gesetzlich zulässig, Kassel.

(5) Die Vereinbarung kann elektronisch abgeschlossen und signiert werden.

(6) Bestandteil dieser Vereinbarung sind die Anlagen 1 bis 4.

Anlage 1 – Beschreibung der Verarbeitung

1. Gegenstand und Zweck

Bereitstellung, Hosting, Betrieb, Wartung, Absicherung und Unterstützung der Software-as-a-Service-Plattform Safetyeasy einschließlich Service Desk.

Die Verarbeitung dient je nach gebuchten und konfigurierten Modulen dem HSE- und Arbeitsschutzmanagement, der Erstellung und Pflege von Gefährdungsbeurteilungen, dem Maßnahmen- und Aufgabenmanagement, dem Ereignis- und Unfallmanagement, dem Unterweisungs- und Schulungsmanagement, dem Audit- und Compliance-Management, der Dokumenten- und Nachweisverwaltung, dem Betrieb von Managementsystemen einschließlich Umwelt-, Energie- und Qualitätsmanagement, der Lift- und Anlagen-Compliance, dem Informationssicherheits- und Risikomanagement, der Benutzer-, Mandanten- und Berechtigungsverwaltung, dem technischen Support sowie der KI-gestützten Analyse, Generierung, Zusammenfassung, Strukturierung und Klassifizierung von Inhalten über den IONOS AI Model Hub.

2. Art der Verarbeitung

Erheben, Erfassen, Strukturieren, Organisieren, Speichern, Abfragen, Anzeigen, Verwenden, Verknüpfen, Übermitteln innerhalb konfigurierter Workflows, Exportieren, Berichtigen, Einschränken, Löschen, Sichern, Wiederherstellen und Protokollieren; Bearbeitung und Dokumentation von Service-Desk-Anfragen; Übermittlung erforderlicher Prompts und Kontextdaten an das KI-Modell sowie automatisierte Erzeugung und Rückgabe von Modellausgaben.

3. Kategorien personenbezogener Daten

Kategorie ? Inhalte

---?---

Stammdaten ? Vor- und Nachname, Anrede, Titel, Personal- oder Benutzernummer, organisatorische Zuordnung, Arbeitgeber, Standort, Abteilung, Funktion

Kontaktdaten ? Geschäftliche E-Mail-Adresse und Telefonnummer, Anschrift, weitere vom Auftraggeber hinterlegte Kontaktdaten

Benutzer- und Berechtigungsdaten ? Benutzername, Rollen, Gruppen, Berechtigungen, Authentifizierungsinformationen, Kontostatus, Anmelde- und Zugriffszeitpunkte

Beschäftigungs- und Organisationsdaten ? Tätigkeit, Qualifikation, Unterweisungs- und Schulungsstatus, Zuständigkeit, organisatorische Einheit, Einsatz- und Arbeitsbereich

HSE- und Arbeitsschutzdaten ? Gefährdungen, Schutzmaßnahmen, Unterweisungen, Qualifikationen, Ereignisse, Beinaheunfälle, Unfälle, Beteiligte und Zeugen, Maßnahmen, Fristen, Verantwortlichkeiten

Gesundheitsbezogene Daten ? Soweit vom Auftraggeber zulässigerweise verarbeitet: Verletzungsart, gesundheitliche Folgen eines Arbeitsunfalls, Angaben zu Arbeitsfähigkeit oder Einschränkungen, erforderliche Schutzmaßnahmen, arbeitsmedizinisch relevante Statusinformationen

Audit-, Risiko- und Compliance-Daten ? Feststellungen, Abweichungen, Maßnahmen, Bewertungen, Nachweise, Freigaben, Verantwortlichkeiten, Kommentare, Prüfergebnisse

Dokumente und Anhänge ? Hochgeladene Dateien, Formulare, Nachweise, Bilder, Protokolle, Berichte, Zertifikate und sonstige vom Auftraggeber gespeicherte Unterlagen

Technische und Service-Desk-Daten ? IP-Adresse, Zeitstempel, Browser- und Geräteinformationen, Session- und Authentifizierungsdaten, System- und Anwendungsprotokolle, Fehler- und Sicherheitsereignisse, Betreff und Beschreibung eines Vorgangs, Kommunikation, Screenshots und Anhänge, Bearbeitungsstatus und -historie

KI-Verarbeitungsdaten ? Text-Prompts und Anweisungen, Bildinhalte bei aktivierter Funktion, erforderliche Kontextinformationen und Auszüge aus Safetyeasy-Inhalten einschließlich der darin enthaltenen personenbezogenen Angaben,

Modellausgaben sowie technische Metadaten zur API-Nutzung

4. Kategorien betroffener Personen

Beschäftigte und ehemalige Beschäftigte des Auftraggebers, Bewerber (soweit vom Auftraggeber verarbeitet), Leiharbeitnehmer, freie Mitarbeiter, externe Dienstleister und Auftragnehmer, Lieferantenkontakte, Besucher, Schulungs- und Unterweisungsteilnehmer, Zeugen sowie verletzte oder an einem Ereignis beteiligte Personen, Administratoren und Benutzer der Plattform, Auditoren und Prüfer, Ansprechpartner von Kunden und Geschäftspartnern sowie sonstige Personen, deren Daten der Auftraggeber rechtmäßig verarbeitet.

5. Besondere Kategorien personenbezogener Daten

Je nach Nutzung können Gesundheitsdaten im Sinne des Art. 9 DSGVO verarbeitet werden, insbesondere im Rahmen des Ereignis- und Unfallmanagements.

6. Dauer

Für die Dauer des Hauptvertrages zuzüglich der in § 14 vereinbarten Export-, Rückgabe-, Lösch- und Sicherungsfristen.

7. Ansprechpartner bei BLUVIT

Anliegen ? Kontakt

---?---

Datenschutz, Betroffenenrechte, Weisungen nach § 3 ? datenschutz@bluvit.de

Meldung von Sicherheitsvorfällen ? datenschutz@bluvit.de

Technischer Support und Service Desk ? service@bluvit.de, +49 561 94026666 (Mo. – Fr. 08:00 – 16:30 Uhr)

Vertrag und kaufmännische Anliegen ? info@bluvit.de

Postanschrift: BLUVIT GmbH, Obergarten 22, 34253 Lohfelden, Deutschland.

Geschäftsräume: Am alten Rathaus 5a, 34253 Lohfelden, Deutschland.

Ansprechpartner des Auftraggebers werden gesondert benannt.

Anlage 2 – Genehmigte direkte Unterauftragsverarbeiter

1. IONOS Cloud GmbH (Infrastruktur)

?

---?---

Anbieter ? IONOS Cloud GmbH, Elgendorfer Straße 57, 56410 Montabaur, Deutschland

Leistung ? Rechenzentrums- und Cloudinfrastruktur, virtuelle Rechenzentren, Netzwerk- und Speicherinfrastruktur, Managed Kubernetes, Datenbankdienste, Objektspeicher, Sicherungs- und Wiederherstellungsdienste, technische Plattform- und Supportleistungen

Datenkategorien ? Sämtliche in Safetyeasy gespeicherten Anwendungs-, Datenbank-, Dokumenten-, Benutzer-, Mandanten-, Protokoll- und Verbindungsdaten einschließlich Sicherungskopien

Verarbeitungsort ? Deutschland, entsprechend der von BLUVIT gewählten und vertraglich vereinbarten IONOS-Cloud-Region

Drittlandbezug ? Keiner

2. IONOS SE – AI Model Hub (KI-Inferenz)

?

----------?----------

Anbieter ? IONOS SE, Elgendorfer Straße 57, 56410 Montabaur, Deutschland. Weist der maßgebliche Vertrag über den AI Model Hub eine andere IONOS-Gesellschaft als Vertragspartner aus, ist diese Gesellschaft maßgeblich.

Leistung ? Bereitstellung des IONOS AI Model Hub und Inferenz über Mistral Small 24B Instruct (mistralai/Mistral-Small-24B-Instruct); Verarbeitung von Text-Prompts, erforderlichen Kontextinformationen und – soweit in Safetyeasy aktiviert – Bildinhalten; Erzeugung von Textausgaben, Zusammenfassungen, Klassifizierungen, Strukturierungen und Vorschlägen; gegebenenfalls Embeddings, Data Collections oder Retrieval-Augmented Generation, sofern diese Funktionen aktiviert werden

Datenkategorien ? Prompts und Anweisungen, Bildinhalte bei aktivierter Funktion, Kontext- und Referenzinformationen, Auszüge aus Safetyeasy-Inhalten und die darin enthaltenen personenbezogenen Daten, Modellausgaben, technische Nutzungs-, Sicherheits- und Abrechnungsmetadaten

Betroffene Personen ? Benutzer und Administratoren von Safetyeasy sowie Personen, deren Daten in den übermittelten Inhalten enthalten sind

Verarbeitungsort ? Deutschland; nach der IONOS-Produktbeschreibung werden Inferenz-Endpunkte und verwaltete Vektordatenbanken in Rechenzentren in Deutschland betrieben

Drittlandbezug ? Keiner

Datenverwendung ? Zustandsloser Betrieb des Inferenzdienstes; Prompts und Ausgaben werden nach Abschluss der Sitzung verworfen und nicht zum Training oder zur Weiterentwicklung der Modelle verwendet. Bei Nutzung von Data Collections oder RAG werden eingestellte Dokumente und daraus erzeugte Vektordaten gesondert gespeichert und unterliegen eigenen Lösch- und Berechtigungsvorgaben.

Besondere Vorgaben: Datenminimierung vor Übermittlung; keine Übermittlung von Passwörtern, privaten Schlüsseln, API-Schlüsseln, vollständigen Zugriffstoken oder vergleichbaren Geheimnissen; besondere Kategorien personenbezogener Daten nur bei Erforderlichkeit und rechtlicher Zulässigkeit; keine routinemäßige Übermittlung vollständiger Datenbestände; fachliche Prüfung automatisiert erzeugter Ergebnisse vor deren Verwendung; Modellwechsel innerhalb des AI Model Hub zulässig nach Maßgabe des § 1 Abs. 10.

3. Odoo S.A. (Service Desk)

?

----------?----------

Anbieter ? Odoo S.A., Chaussée de Namur 40, 1367 Grand-Rosière, Belgien

Leistung ? Service Desk und Ticketverwaltung für Safetyeasy, Dokumentation und Bearbeitung technischer und fachlicher Supportanfragen, Kommunikation mit autorisierten Ansprechpartnern, Fehleranalyse und Nachverfolgung, Verwaltung erforderlicher Anhänge und Protokollauszüge, Dokumentation von Bearbeitungsstatus, Verantwortlichkeiten und Maßnahmen

Datenkategorien ? Name und geschäftliche Kontaktdaten, Benutzerkennung und organisatorische Zuordnung, Kunden-, Mandanten- und Vertragsreferenz, Betreff, Beschreibung und Kommunikation eines Vorgangs, System-, Browser-, Geräte- und Verbindungsinformationen, Fehlercodes, Zeitstempel und Protokollauszüge, Screenshots und sonstige Anhänge, Bearbeitungs-, Eskalations- und Statusinformationen

Betroffene Personen ? Benutzer und Administratoren von Safetyeasy, Beschäftigte und Ansprechpartner des Auftraggebers sowie in einem Supportvorgang genannte oder erkennbare Personen

Verarbeitungsort ? Hostingregion Europa; primärer Produktionsstandort Frankfurt gemäß individueller Anbieterbestätigung für die eingesetzte Datenbank; weitere Sicherungs-, Replikations- und Supportstandorte nach den jeweils geltenden Odoo-Bedingungen

Drittlandbezug ? Nach den geltenden Odoo-Unterauftragsverarbeiterbedingungen möglich, insbesondere bei Support- und Replikationszugriffen; abgesichert über die Standardvertragsklauseln der Europäischen Kommission

Besondere Vorgaben: Speicherung nur der für den jeweiligen Vorgang erforderlichen Daten; keine routinemäßige Übernahme vollständiger Safetyeasy-Datenbestände; keine Speicherung von Passwörtern, privaten Schlüsseln, vollständigen Zugriffstoken oder vergleichbaren Geheimnissen; Bereinigung von Screenshots und Protokolldateien vor Übermittlung, soweit möglich; besondere Kategorien personenbezogener Daten nur bei zwingender Erforderlichkeit; rollenbasierter Zugriff und regelmäßige Berechtigungsprüfung; dokumentierte Löschung oder Anonymisierung nach Wegfall des Bearbeitungs- und Nachweiszwecks.

4. Mailtrap (Railsware Products Studio LLC) – Transaktionale E-Mails

?

----------?----------

Anbieter ? Railsware Products Studio LLC, handelnd unter „Mailtrap“, 117 E Colorado Boulevard, Suite 600, Office 650, Pasadena, California 91105, USA

Leistung ? Versand transaktionaler E-Mails, technische Zustellungsanalyse, Bounce- und Fehlermanagement, Versandprotokollierung, Missbrauchs- und Spamprävention

Datenkategorien ? Empfängername (soweit verwendet), E-Mail-Adresse, Absenderinformationen, Betreff, E-Mail-Inhalt, Versandzeitpunkt, Zustellstatus sowie technische Versand-, Verbindungs- und Protokolldaten

Verarbeitungsort ? USA sowie weitere Staaten entsprechend der jeweils aktuellen Unterauftragsverarbeiterliste und technischen Infrastruktur von Mailtrap

Drittlandbezug ? Ja. Übermittlungsgrundlage sind die Standardvertragsklauseln der Europäischen Kommission (Durchführungsbeschluss (EU) 2021/914, Modul 3) nebst ergänzenden Maßnahmen und einer dokumentierten Transfer-Folgenabschätzung.

Besondere Beschränkungen: keine Passwörter oder Authentifizierungsgeheimnisse in E-Mails; keine vollständigen Unfallberichte; keine detaillierten Gesundheitsdaten; keine vollständigen Safetyeasy-Dokumente oder Exporte; neutral formulierte Benachrichtigungen mit Link auf den geschützten Bereich.

Anlage 3 – Dienstleister außerhalb der Safetyeasy-Auftragsverarbeitung

Die nachfolgenden Dienstleister verarbeiten Daten für Zwecke, über die BLUVIT als eigener Verantwortlicher entscheidet. Sie sind keine Unterauftragsverarbeiter des Auftraggebers.

1. Odoo S.A. – Verarbeitungen in eigener Verantwortung von BLUVIT

Odoo wird neben dem Service Desk für CRM, Interessenten- und Kundenverwaltung, die Verwaltung geschäftlicher Ansprechpartner, Angebotserstellung, Vertrags- und Abonnementverwaltung, Erstellung und Vorhaltung von Rechnungen, Buchhaltungs- und Zahlungsstatusverwaltung, die allgemeine Kundenkommunikation sowie zur Erfüllung handels- und steuerrechtlicher Aufbewahrungspflichten eingesetzt.

Für diese Verarbeitungen bestimmt BLUVIT Zwecke und wesentliche Mittel und handelt als Verantwortlicher. Odoo ist insoweit Auftragsverarbeiter der BLUVIT, nicht Unterauftragsverarbeiter des Safetyeasy-Kunden.

2. Stripe

Stripe wird für Zahlungsabwicklung und -bestätigung, Betrugsprävention, Rückerstattungen, die Verwaltung von Zahlungsmethoden und die Bearbeitung von Zahlungsstörungen eingesetzt. Fachliche Safetyeasy-Inhaltsdaten werden nicht an Stripe übermittelt. Vollständige Kreditkartennummern und Kartenprüfnummern werden weder in Safetyeasy noch in Odoo gespeichert.

Anlage 4 – Technische und organisatorische Maßnahmen nach Art. 32 DSGVO

1. Geltungsbereich

Diese Maßnahmen gelten für die Verarbeitung personenbezogener Daten im Rahmen von Safetyeasy einschließlich Service Desk. Sie beziehen sich auf den Verantwortungsbereich der BLUVIT GmbH sowie auf die von ihr kontrollierten Anwendungs-, Verwaltungs- und Betriebsprozesse. Maßnahmen im Verantwortungsbereich der Unterauftragsverarbeiter ergeben sich aus den mit diesen geschlossenen Vereinbarungen und den dort nachgewiesenen Zertifizierungen.

2. Informationssicherheitsorganisation

Verantwortlichkeiten für Informationssicherheit und Datenschutz sind definiert und dokumentiert. Es bestehen dokumentierte Sicherheitsrichtlinien sowie Betriebs- und Administrationsverfahren, ein Verfahren für regelmäßige Risikobewertungen, ein Lieferanten- und Dienstleistermanagement, ein geregelter Prozess zur Behandlung von Sicherheitsvorfällen und dokumentierte Freigabe- und Änderungsprozesse. Benutzeraufnahme, Rollenänderung und Benutzerentfernung sind geregelt. Beschäftigte werden auf Vertraulichkeit verpflichtet und regelmäßig geschult; die Wirksamkeit der Maßnahmen wird regelmäßig überprüft.

3. Zutrittskontrolle

Die produktive Infrastruktur wird in Rechenzentren der IONOS Cloud betrieben; die physische Zutrittskontrolle liegt im Verantwortungsbereich von IONOS.

Für die Geschäftsräume der BLUVIT in Lohfelden, Am alten Rathaus 5a, gelten eine geregelte Schlüssel- und Zutrittsvergabe, Zutritt nur für berechtigte Personen, die Begleitung betriebsfremder Personen, das Verschließen von Arbeits- und Technikbereichen außerhalb der Nutzungszeiten, Clean-Desk- und Clear-Screen-Regelungen, die sichere Aufbewahrung vertraulicher Unterlagen sowie die geregelte Vernichtung von Papierunterlagen und Datenträgern.

4. Zugangskontrolle

Personalisierte Benutzerkonten, sichere Passwortrichtlinien und Mehrfaktor-Authentisierung für administrative und privilegierte Zugänge; geregelte Identitäts- und Berechtigungsverwaltung mit zeitnaher Sperrung ausgeschiedener Benutzer und regelmäßiger Überprüfung aktiver Konten; Schutz vor Brute-Force-Angriffen, zeitlich begrenzte Sitzungen und ein sicheres Verfahren zur Passwortzurücksetzung; keine Speicherung von Passwörtern im Klartext, sondern ausschließlich als Hash nach aktuellem Stand der Technik; Beschränkung administrativer Schnittstellen und ausschließlich verschlüsselte administrative Zugriffe.

5. Zugriffskontrolle

Rollenbasiertes Berechtigungskonzept nach dem Least-Privilege- und dem Need-to-know-Prinzip; Trennung administrativer und regulärer Benutzerkonten sowie von Kunden-, Support- und Plattformadministrationsrollen; restriktive Vergabe von Super-Administratorrechten und regelmäßige Überprüfung privilegierter Rollen; mandantenbezogene, serverseitig durchgesetzte Berechtigungsprüfung; geregelte Freigabe von Datenexporten; Zugriff auf Produktivdaten nur bei betrieblicher Erforderlichkeit; Protokollierung wesentlicher administrativer Zugriffe.

6. Mandanten- und Trennungskontrolle

Logische Trennung der Kundendaten mit eindeutiger Mandantenzuordnung und mandantenbezogener Berechtigungsprüfung; technische Verhinderung mandantenübergreifender Datenabfragen; Trennung von Produktions- und Stagingumgebungen mit jeweils getrennten Konfigurations-, Zugangs- und Geheimnisdaten; keine Verwendung produktiver Kundendaten in Entwicklungsumgebungen, sondern Einsatz anonymisierter oder synthetischer Testdaten.

7. Übertragungskontrolle und Verschlüsselung

Verschlüsselte Übertragung über HTTPS/TLS mit aktueller Konfiguration; verschlüsselte administrative Verbindungen und abgesicherte Kommunikation mit Datenbanken und Infrastrukturkomponenten, soweit unterstützt; Verschlüsselung gespeicherter Daten durch die eingesetzte Infrastruktur, soweit verfügbar; sichere Schlüssel- und Geheimnisverwaltung ohne Ablage von Geheimnissen im Quellcode, unter Nutzung geschützter CI/CD-Variablen oder eines Secret-Management-Verfahrens; Beschränkung von Datenexporten auf berechtigte Personen und Empfängerprüfung vor der Übermittlung personenbezogener Daten.

8. E-Mail-Sicherheit

E-Mail-Benachrichtigungen werden auf das erforderliche Mindestmaß beschränkt; fachliche Inhalte verbleiben in Safetyeasy, die Benachrichtigung enthält vorzugsweise einen Link auf den geschützten Bereich und eine neutral formulierte Betreffzeile. Nicht übermittelt werden Passwörter und Authentifizierungsgeheimnisse, vollständige Unfallberichte, detaillierte Gesundheitsinformationen sowie vollständige Dokumente oder Exporte. Das Mailtrap-Konto wird rollenbasiert verwaltet, mit Mehrfaktor-Authentisierung abgesichert, soweit verfügbar; SMTP- und API-Zugangsdaten werden geschützt und regelmäßig rotiert. Produktive Empfängerlisten werden nicht in Entwicklungs- oder Testumgebungen verwendet.

9. Service Desk und kaufmännische Prozesse in Odoo

Für auftragsbezogene Service-Desk-Daten gilt: eindeutige Zuordnung jedes Vorgangs zu Kunde und Mandant; Verarbeitung nur der für Analyse, Bearbeitung, Kommunikation und Nachweis erforderlichen Daten; keine routinemäßige Synchronisation vollständiger Safetyeasy-Datenbestände nach Odoo; keine Nutzung von Service-Desk-Inhalten für Werbe- oder Vertriebszwecke; Bereinigung von Screenshots, Exporten und Protokollauszügen, soweit möglich; keine Speicherung von Passwörtern, privaten Schlüsseln, vollständigen Zugriffstoken, API-Schlüsseln oder vergleichbaren Geheimnissen; besondere Kategorien personenbezogener Daten nur bei zwingender Erforderlichkeit und rechtlicher Zulässigkeit; Beschränkung von Anhängen und Exportfunktionen; personalisierte Odoo-Benutzerkonten mit rollenbasierten Berechtigungen, Mehrfaktor-Authentisierung, soweit verfügbar, und regelmäßiger Überprüfung von Benutzern, Gruppen und Rollen; Dokumentation wesentlicher Bearbeitungs- und Statusänderungen; Löschung oder Anonymisierung nach Wegfall des Bearbeitungs- und Nachweiszwecks.

Für CRM-, Vertrags-, Abonnement-, Rechnungs- und Buchhaltungsdaten gilt ergänzend: Verarbeitung ausschließlich für eigene Geschäfts-, Vertrags-, Abrechnungs- und Nachweiszwecke von BLUVIT; Aufbewahrung nach den gesetzlichen Fristen; keine Vermischung fachlicher Safetyeasy-Inhalte mit Rechnungs- oder Abonnementdatensätzen ohne Erforderlichkeit; Zugriff nur für die hierfür zuständigen Beschäftigten; getrennte Rollen für Vertrieb, Support, Administration und Buchhaltung, soweit organisatorisch und technisch möglich.

Zur Lieferantensteuerung gehören die dokumentierte Aufbewahrung der Standortbestätigung für die eingesetzte Datenbank, die regelmäßige Prüfung der geltenden Odoo-Vertragsbedingungen, Datenschutzinformationen, Unterauftragsverarbeiter und Backupstandorte, die Bewertung und Absicherung möglicher Drittlandübermittlungen nach Art. 44 bis 49 DSGVO sowie die Einbeziehung von Odoo in das Lieferanten-, Sicherheitsvorfall- und Notfallmanagement von BLUVIT.

10. KI-Verarbeitung über den IONOS AI Model Hub

Eingesetzt wird der IONOS AI Model Hub als kontrollierter Inferenzdienst mit dem Modell Mistral Small 24B Instruct; die Inferenzdaten werden nach der IONOS-Produktbeschreibung in Deutschland verarbeitet und die Übertragung zwischen Safetyeasy und dem AI Model Hub erfolgt verschlüsselt.

Übermittelte Inhalte werden auf den erforderlichen Prompt-, Kontext- und gegebenenfalls Bildumfang beschränkt; vollständige Mandanten- oder Datenbankbestände werden nicht übertragen. Passwörter, private Schlüssel, API-Schlüssel, vollständige Zugriffstoken und vergleichbare Geheimnisse werden nicht übermittelt. Nicht erforderliche personenbezogene Angaben werden pseudonymisiert, anonymisiert oder entfernt, soweit dies technisch und fachlich möglich ist; besondere Kategorien personenbezogener Daten werden nur bei dokumentierter Erforderlichkeit und rechtlicher Zulässigkeit übermittelt.

Die IONOS-Authentifizierungs- und API-Token werden geschützt verwaltet; Zugriffsrechte bestehen nur für die für Betrieb und Administration erforderlichen Personen und Systeme. Prompts und Modellausgaben werden nach Maßgabe der IONOS-Produktbeschreibung nicht zum Training der bereitgestellten Modelle verwendet; die zustandslose Verarbeitung ist im Datenschutz- und Löschkonzept berücksichtigt. Bei künftiger Nutzung von Data Collections oder RAG werden Speicherzweck, Berechtigungen, Löschfristen und Datenminimierung gesondert geregelt.

KI-Ausgaben werden organisatorisch als automatisiert erzeugte Arbeitsergebnisse behandelt und vor einer sicherheits-, rechts-, compliance- oder entscheidungsrelevanten Nutzung fachlich geprüft. Eine ausschließlich automatisierte Entscheidung mit rechtlicher oder vergleichbar erheblicher Wirkung findet nicht statt, solange hierfür keine gesonderte rechtliche und technische Freigabe erfolgt ist.

11. Zahlungsdaten

Zahlungsdaten werden unmittelbar über die dafür vorgesehenen Stripe-Komponenten verarbeitet. Vollständige Kreditkartennummern und Kartenprüfnummern werden weder in Safetyeasy noch in Odoo gespeichert; dort verbleiben ausschließlich die notwendigen Zahlungsmetadaten. Der Zugriff auf das Stripe-Dashboard ist rollenbasiert und durch Mehrfaktor-Authentisierung geschützt. API-Schlüssel und Webhook-Geheimnisse werden sicher verwaltet, eingehende Webhook-Nachrichten validiert und Test- und Produktivschlüssel getrennt geführt.

12. Eingabe- und Protokollierungskontrolle

Personenbezogene Benutzerkonten und Zeitstempel für wesentliche Vorgänge ermöglichen die Nachvollziehbarkeit von Eingaben und Änderungen. Protokolliert werden insbesondere Anmeldeereignisse, administrative Änderungen, Rollen- und Berechtigungsänderungen sowie sicherheitsrelevante Systemereignisse. Protokolle sind gegen unbefugte Veränderung geschützt, unterliegen einem rollenbasierten Zugriff und werden nach 30 Tagen gelöscht, soweit sie nicht zur Aufklärung eines Sicherheitsvorfalls länger benötigt werden. Passwörter, Tokens und vollständige Geheimnisse werden nicht protokolliert.

13. Verfügbarkeitskontrolle

Regelmäßige automatisierte Datensicherungen mit getrennter Speicherung von Produktivdaten und Sicherungskopien sowie Überwachung der Sicherungsvorgänge; dokumentierte Wiederherstellungsverfahren und regelmäßige Wiederherstellungstests; Überwachung zentraler Plattformkomponenten mit Alarmierung bei kritischen Zuständen; geregeltes Patch- und Wartungsmanagement, Notfall- und Wiederanlaufverfahren, Schutz vor Schadsoftware sowie Kapazitäts- und Ressourcenüberwachung.

14. Datensicherung und Wiederherstellung

Die produktiven Daten werden in definierten Intervallen gesichert; Aufbewahrungsfristen sind dokumentiert. Der Zugriff auf Sicherungskopien ist berechtigten Administratoren vorbehalten. Wiederherstellungen erfolgen nur aus betrieblichem Grund oder auf dokumentierte Weisung und werden dokumentiert. Abgelaufene Sicherungen werden automatisiert überschrieben oder gelöscht.

15. Patch- und Schwachstellenmanagement

Regelmäßige Prüfung auf bekannte Schwachstellen mit Bewertung nach Kritikalität und Exposition und priorisierter Behandlung kritischer Sicherheitslücken; regelmäßige Aktualisierung von Systemen und Komponenten einschließlich der eingesetzten Abhängigkeiten; Container- und Image-Scanning; Überwachung veröffentlichter Sicherheitsmeldungen; geregelter Prozess für Sicherheitsupdates; Härtung von Systemkonfigurationen und Beschränkung offen erreichbarer Schnittstellen.

16. Sichere Softwareentwicklung

Dokumentierter Entwicklungs- und Änderungsprozess mit Versionsverwaltung und nachvollziehbarer Änderungshistorie; Code-Reviews für wesentliche Änderungen; getrennte Entwicklungs-, Test- und Produktionsumgebungen; automatisierte Tests und Sicherheitsprüfungen in der CI/CD-Pipeline; keine Ablage produktiver Geheimnisse im Quellcode; definierter Freigabeprozess vor der Produktivbereitstellung sowie Rückfall- und Rollbackverfahren.

17. Datenschutz durch Technikgestaltung und Voreinstellungen

Datensparsame Standardkonfiguration mit rollenbasierten Standardberechtigungen und Mandantentrennung; keine öffentliche Freigabe von Daten als Voreinstellung; Minimierung erhobener Pflichtfelder; konfigurierbare Aufbewahrungs- und Löschprozesse; Verwendung von Referenzen statt vollständiger Inhalte in Benachrichtigungen; Beschränkung von Exportfunktionen; Pseudonymisierung oder Anonymisierung, soweit sachlich möglich.

18. Löschkontrolle

Löschprozesse sind dokumentiert. Die Löschung erfolgt durch berechtigte Benutzer oder durch BLUVIT auf Weisung. Produktive Daten und Sicherungskopien werden getrennt geführt; abgelaufene Sicherungen werden automatisiert überschrieben. Protokolldaten werden nach definierten Fristen gelöscht, nicht mehr benötigte Exporte sicher entfernt. Bestehen gesetzliche Aufbewahrungspflichten, tritt an die Stelle der Löschung eine Sperrung.

Datenbestand ? Frist

---?---

Exportzugang nach Vertragsende ? 30 Kalendertage

Produktive Kundendaten ? Löschung mit Ablauf des Exportzugangs, 30 Kalendertage nach Vertragsende

Reguläre Sicherungskopien ? höchstens 90 Tage

Technische Protokolle ? 30 Tage, soweit nicht zur Aufklärung eines Sicherheitsvorfalls länger erforderlich

Temporäre Exporte ? unverzüglich nach Wegfall des Zwecks

Service-Desk-Dateien ? nach Abschluss und Wegfall des Bearbeitungs- und Nachweiszwecks

19. Auftragskontrolle

Schriftliche Auftragsverarbeitungsvereinbarung mit dokumentierten Weisungswegen und klar definierten Verantwortlichkeiten; sorgfältige Auswahl der Unterauftragsverarbeiter und Abschluss geeigneter Vereinbarungen; regelmäßige Lieferantenbewertung unter Prüfung verfügbarer Zertifikate und Auditberichte; Dokumentation der Verarbeitungskette; vereinbarte Kontroll- und Nachweisrechte; geregelte Rückgabe- und Löschprozesse.

20. Sicherheitsvorfallmanagement

Dokumentierter Prozess zur Erkennung und Behandlung von Sicherheitsvorfällen mit definierten Eskalationswegen und einer Bewertung nach Schwere und Auswirkung; unverzügliche Eindämmung, Sicherung relevanter Protokolle und Beweismittel, Ursachenanalyse und dokumentierte Gegenmaßnahmen; Information betroffener Auftraggeber nach § 9; Nachbereitung und Auswertung der gewonnenen Erkenntnisse.

21. Personalsicherheit

Verpflichtung auf Vertraulichkeit, Datenschutz- und Sicherheitsschulungen sowie rollenbezogene Einweisung; geregelte Vergabe von Berechtigungen und unverzüglicher Entzug bei Ausscheiden einschließlich der Rückgabe von Geräten und Zugangsmitteln; Verpflichtung zur Meldung von Sicherheitsvorfällen; Vorgaben zur sicheren mobilen Arbeit sowie Sensibilisierung gegen Social Engineering und Phishing.

22. Mobile Arbeit und Endgerätesicherheit

Verwaltete Geräte mit Festplattenverschlüsselung, Bildschirmsperre, aktuellen Sicherheitsupdates sowie Schadsoftware- und Endpunktschutz; beschränkte lokale Administratorrechte und sichere Grundkonfiguration; abgesicherte Fernzugriffe; definierter Melde- und Sperrprozess bei Verlust oder Diebstahl; sichere Löschung ausgemusterter Geräte; keine dauerhafte lokale Speicherung von Kundendaten, soweit vermeidbar.

23. Regelmäßige Überprüfung

Die Wirksamkeit der Maßnahmen wird durch interne Kontrollen, Risikobewertungen, technische Sicherheitsprüfungen und Schwachstellenscans, Berechtigungsreviews, Lieferantenbewertungen, Wiederherstellungstests und die Auswertung von Sicherheitsvorfällen überprüft. Die Richtlinien werden regelmäßig aktualisiert und an technische und regulatorische Entwicklungen angepasst.

24. Mitwirkungspflichten des Auftraggebers

Der Auftraggeber verwaltet seine Benutzer sicher, sperrt ausgeschiedene Benutzer unverzüglich und vergibt nur die minimal erforderlichen Berechtigungen. Er schützt seine Endgeräte und E-Mail-Konten, setzt Mehrfaktor-Authentisierung ein, soweit angeboten, und bewahrt Zugangsdaten sicher auf. Er prüft Exportempfänger, konfiguriert die Anwendung rechtmäßig, gibt ausschließlich erforderliche Daten ein, legt geeignete Löschfristen fest und meldet erkannte Sicherheitsvorfälle unverzüglich an BLUVIT.

Unterzeichnung

Auftraggeber

Angabe ? Wert

---?---

Ort, Datum ? _____
Name ? _____
Funktion ? _____
Firma ? _____
E-Mail ? _____
Art der Annahme ? _____
Zeitstempel der Registrierung ? _____

Die Felder werden bei der elektronischen Annahme über die Registrierung ausgefüllt.

BLUVIT GmbH

Angabe ? Wert

---?---

Ort, Datum ? Lohfelden, 12. August 2026
Name ? Timm Vollmer
Funktion ? Geschäftsführer
Annahme ? Gegenzeichnung durch Bereitstellung der Plattform und elektronische Vertragsannahme

Dieses Dokument wird bei der Registrierung mit den Stammdaten der Organisation und dem Annahmezeitstempel ausgefüllt und im Bereich „Organisation“ der Plattform bereitgestellt.