Vereinbarung zur Auftragsverarbeitung

für die Nutzung der SaaS-Anwendung Shiftio nach Art. 28 DSGVO

Anbieter: Marc Tutter und Thomas Bernhard, Wallgasse 14/34, 1060 Wien, gemeinsam auftretend unter der Geschäftsbezeichnung „Shiftio“
Stand: 02.10.2026, v1.0

Vertragsparteien

Rolle	Vertragspartei und Kontaktdaten
Verantwortlicher	der Kunde laut den Angaben bei der Online-Bestellung (Firma, Rechtsform, Anschrift, gegebenenfalls Firmenbuchnummer und UID-Nummer)
Auftragsverarbeiter	Marc Tutter und Thomas Bernhard, beide Wallgasse 14/34, 1060 Wien, Österreich, gemeinsam auftretend unter der Geschäftsbezeichnung „Shiftio“ (Gesellschaft bürgerlichen Rechts, nicht im Firmenbuch eingetragen); E-Mail: hallo@shiftio.at
Datenschutzkontakte	Verantwortlicher: die bei der Online-Bestellung angegebene E-Mail-Adresse des Administrators, sofern der Kunde keinen anderen Kontakt in Textform mitteilt. Auftragsverarbeiter: hallo@shiftio.at

Diese Vereinbarung ergänzt den Vertrag über die Nutzung von Shiftio einschließlich der Allgemeinen Geschäftsbedingungen. Sie gilt, soweit der Auftragsverarbeiter personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet. Die Anlagen sind Bestandteil dieser Vereinbarung.

1. Gegenstand und Anwendungsbereich

1.1 Der Auftragsverarbeiter stellt dem Verantwortlichen die cloudbasierte Dienstplanungssoftware Shiftio bereit. Gegenstand, Art, Zweck, Datenkategorien und betroffene Personen sind in Anlage 1 beschrieben.

1.2 Der Verantwortliche bestimmt die Zwecke und wesentlichen Mittel der Verarbeitung. Der Auftragsverarbeiter verarbeitet personenbezogene Daten ausschließlich auf dokumentierte Weisung des Verantwortlichen, soweit nicht eine Verpflichtung nach Unionsrecht oder österreichischem Recht besteht. In diesem Fall informiert der Auftragsverarbeiter den Verantwortlichen vor der Verarbeitung über die betreffende Rechtspflicht, sofern das Recht eine solche Information nicht aus wichtigen Gründen des öffentlichen Interesses untersagt.

1.3 Als dokumentierte Weisungen gelten diese Vereinbarung, der Hauptvertrag, die AGB, die vom Verantwortlichen vorgenommenen Einstellungen und seine rechtmäßige Nutzung der vorgesehenen Funktionen. Zusätzliche Weisungen sind in Textform an hallo@shiftio.at zu richten.

1.4 Hält der Auftragsverarbeiter eine Weisung für datenschutzrechtswidrig, informiert er den Verantwortlichen unverzüglich. Er darf die Ausführung aussetzen, bis die Weisung bestätigt, geändert oder zurückgenommen wurde.

2. Dauer der Verarbeitung

2.1 Die Auftragsverarbeitung beginnt mit der Freischaltung eines Kundenkontos oder dem sonst vereinbarten Beginn und dauert grundsätzlich bis zur vollständigen Rückgabe oder Löschung der Auftragsdaten nach Vertragsende.

2.2 Für Export, Löschung und Sicherungskopien gelten die in Anlage 1 festgelegten Fristen. Gesetzliche Aufbewahrungspflichten des Auftragsverarbeiters für eigene Geschäftsunterlagen bleiben unberührt; solche Daten werden für andere Zwecke gesperrt und nicht als Auftragsdaten weiterverarbeitet.

3. Pflichten des Verantwortlichen

3.1 Der Verantwortliche gewährleistet die Rechtmäßigkeit der Erhebung und Verarbeitung, erfüllt seine Informationspflichten und wahrt arbeitsrechtliche sowie betriebsverfassungsrechtliche Vorgaben. Er entscheidet insbesondere über Rechtsgrundlagen, Zugriffsberechtigungen und Aufbewahrungsfristen innerhalb der vertraglich vorgesehenen Möglichkeiten.

3.2 Der Verantwortliche stellt sicher, dass nur erforderliche Daten eingegeben werden. Die Abwesenheitskategorie Krankheit kann Gesundheitsdaten nach Art. 9 DSGVO betreffen. Diagnosen, Krankheitsursachen, ärztliche Atteste oder sonstige medizinische Freitexte dürfen nicht eingegeben werden, sofern hierfür keine ausdrücklich freigegebene Funktion und gesonderte rechtliche Grundlage bestehen.

3.3 Der Verantwortliche verwaltet Administratoren, Rollen und Nutzer, schützt Zugangsdaten und meldet vermuteten Missbrauch sowie unrichtige oder unzulässige Daten unverzüglich.

4. Weisungsgebundene Verarbeitung und Vertraulichkeit

4.1 Der Auftragsverarbeiter verarbeitet Auftragsdaten nur zur Erbringung, Absicherung, Wartung und Unterstützung von Shiftio sowie zur Erfüllung dokumentierter Weisungen. Eine Nutzung zu eigenen Werbezwecken oder zum Training generativer KI-Modelle findet nicht statt, sofern dies nicht ausdrücklich, transparent und rechtswirksam gesondert vereinbart wird.

4.2 Der Auftragsverarbeiter stellt sicher, dass Personen mit Zugang zu Auftragsdaten zur Vertraulichkeit verpflichtet sind oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Zugriffe werden auf das für die jeweilige Aufgabe erforderliche Maß beschränkt.

4.3 Verarbeitung außerhalb des EWR oder Zugriff aus einem Drittland ist nur zulässig, wenn die Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind und der Verantwortliche entsprechend dieser Vereinbarung informiert wurde.

5. Sicherheit der Verarbeitung

5.1 Der Auftragsverarbeiter trifft unter Berücksichtigung des Stands der Technik, der Implementierungskosten, Art, Umfang, Umständen und Zwecken der Verarbeitung sowie der Risiken geeignete technische und organisatorische Maßnahmen nach Art. 32 DSGVO. Die vereinbarten Maßnahmen sind in der gesonderten Anlage Technische und organisatorische Maßnahmen beschrieben.

5.2 Die Maßnahmen dürfen weiterentwickelt werden, sofern das vereinbarte Schutzniveau nicht unterschritten wird. Wesentliche nachteilige Änderungen werden dem Verantwortlichen rechtzeitig mitgeteilt.

6. Unterauftragsverarbeiter

6.1 Der Verantwortliche erteilt eine allgemeine Genehmigung für die in Anlage 3 angeführten Unterauftragsverarbeiter.

6.2 Der Auftragsverarbeiter informiert den Verantwortlichen mindestens 30 Tage vor der beabsichtigten Hinzuziehung oder Ersetzung eines Unterauftragsverarbeiters in Textform. Bei

einer dringenden sicherheits- oder betriebsbedingten Änderung darf die Frist angemessen verkürzt werden; die Gründe sind mitzuteilen.

6.3 Der Verantwortliche kann aus konkreten datenschutzrechtlichen Gründen innerhalb von 14 Tagen widersprechen. Können die Parteien keine zumutbare Lösung finden, kann jede Partei den betroffenen Leistungsumfang außerordentlich kündigen. Weitergehende Rechte aus dem Hauptvertrag bleiben unberührt.

6.4 Unterauftragsverarbeiter werden durch Vertrag zu Datenschutzpflichten verpflichtet, die im Wesentlichen dem Schutzniveau dieser Vereinbarung entsprechen. Der Auftragsverarbeiter bleibt gegenüber dem Verantwortlichen für die Erfüllung der Pflichten des Unterauftragsverarbeiters verantwortlich.

7. Unterstützung des Verantwortlichen

7.1 Der Auftragsverarbeiter unterstützt den Verantwortlichen unter Berücksichtigung der Art der Verarbeitung und der verfügbaren Informationen bei der Erfüllung der Betroffenenrechte nach Kapitel III DSGVO. Anfragen betroffener Personen zu Auftragsdaten beantwortet er nicht eigenständig, sondern leitet sie unverzüglich an den Verantwortlichen weiter, sofern keine andere Weisung vorliegt.

7.2 Er unterstützt den Verantwortlichen außerdem bei Pflichten nach Art. 32 bis 36 DSGVO, insbesondere bei Sicherheitsbewertungen, Datenschutzverletzungen, Datenschutz-Folgenabschätzungen und vorherigen Konsultationen, soweit die Verarbeitung durch Shiftio betroffen ist.

7.3 Gesetzlich und vertraglich geschuldete Standardunterstützung ist mit dem Nutzungsentgelt abgegolten. Ein außergewöhnlicher, vom Verantwortlichen verursachter Zusatzaufwand kann nach vorheriger Abstimmung zu individuellen Stundensätzen verrechnet werden. Dies gilt nicht, soweit der Aufwand auf einem vom Auftragsverarbeiter zu vertretenden Verstoß beruht.

8. Datenschutzverletzungen

8.1 Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich, nachdem ihm eine Verletzung des Schutzes von Auftragsdaten bekannt wurde. Angestrebte Frist für eine erste Meldung: 24 Stunden.

8.2 Die Meldung enthält, soweit verfügbar, Art und Umfang des Vorfalls, betroffene Daten und Personengruppen, wahrscheinliche Folgen, bereits ergriffene oder vorgeschlagene Maßnahmen sowie einen Kontakt für Rückfragen. Fehlende Informationen werden ohne unangemessene Verzögerung nachgereicht.

8.3 Die Entscheidung über eine Meldung an Aufsichtsbehörden oder betroffene Personen obliegt dem Verantwortlichen, soweit der Auftragsverarbeiter nicht aufgrund eigener Verantwortlichkeit gesetzlich selbst verpflichtet ist.

9. Rückgabe, Löschung und Export

9.1 Während der Vertragslaufzeit stehen die vereinbarten Exportmöglichkeiten zur Verfügung. Nach Vertragsende gelten für Export und Anbieterwechsel die Übergangszeit von 30 Tagen und die anschließende Abrufzeit von mindestens 30 Tagen nach AGB Ziffer 10.3; der Export erfolgt im Format CSV.

9.2 Auftragsdaten in aktiven Systemen werden spätestens 30 Tage nach Ablauf der Abrufzeit, ohne Verlängerung der Übergangszeit also spätestens 90 Tage nach Vertragsende, gelöscht oder auf Weisung zurückgegeben, sofern keine gesetzliche Pflicht zur weiteren Speicherung besteht.

Daten in Sicherungskopien werden spätestens 30 Tage später durch rollierende Überschreibung entfernt.

9.3 Bis zur Löschung bleiben die Daten geschützt und dürfen nur für Wiederherstellung, Sicherheit und gesetzlich zulässige Zwecke verarbeitet werden. Eine selektive Löschung einzelner Datensätze aus unveränderlichen Sicherungskopien ist nicht geschuldet, sofern der Zugriff beschränkt bleibt und die Daten beim Wiederherstellen erneut gelöscht werden.

10. Nachweise und Kontrollen

10.1 Der Auftragsverarbeiter stellt dem Verantwortlichen alle Informationen zur Verfügung, die zum Nachweis der Pflichten nach Art. 28 DSGVO erforderlich sind. Er ermöglicht angemessene Prüfungen durch den Verantwortlichen oder einen zur Vertraulichkeit verpflichteten Prüfer.

10.2 Prüfungen sollen vorrangig durch aktuelle Dokumentationen, Fragebögen, Zertifikate oder Prüfberichte erfolgen. Vor-Ort-Prüfungen sind bei berechtigtem Anlass und grundsätzlich mit mindestens 15 Werktagen Vorankündigung während üblicher Geschäftszeiten möglich, ohne Sicherheit, Vertraulichkeit oder Rechte anderer Kunden zu beeinträchtigen.

10.3 Jede Partei trägt ihre eigenen Prüfungskosten. Verursacht eine Prüfung außergewöhnlichen Aufwand, kann dieser nach vorheriger Abstimmung verrechnet werden, außer die Prüfung weist einen wesentlichen vom Auftragsverarbeiter zu vertretenden Verstoß nach.

11. Haftung und Rangfolge

11.1 Zwingende Haftungsregelungen der DSGVO, insbesondere Art. 82 DSGVO, bleiben unberührt. Im Übrigen gelten die Haftungsregelungen des Hauptvertrags und der AGB, soweit sie auf das jeweilige Rechtsverhältnis wirksam anwendbar sind.

11.2 Bei datenschutzrechtlichen Widersprüchen geht diese Vereinbarung den AGB vor. Die TOM konkretisieren die Sicherheitsmaßnahmen; Anlage 1 konkretisiert Gegenstand und Umfang der Verarbeitung.

12. Schlussbestimmungen

12.1 Änderungen und Ergänzungen bedürfen zumindest der Textform, soweit nicht zwingendes Recht eine strengere Form verlangt. Elektronische Annahme und elektronischer Abschluss sind zulässig.

12.2 Es gilt österreichisches Recht unter Ausschluss seiner Verweisungsnormen. Gerichtsstand und Erfüllungsort richten sich nach dem Hauptvertrag, soweit gesetzlich zulässig.

12.3 Sollte eine Bestimmung unwirksam sein oder werden, bleibt der übrige Vertrag wirksam. An ihre Stelle tritt die gesetzliche Regelung.

Anlage 1: Beschreibung der Auftragsverarbeitung

Merkmal	Beschreibung
Gegenstand	Bereitstellung und Betrieb der browserbasierten SaaS-Anwendung Shiftio für Dienstplanung, Abwesenheiten, Arbeitszeiterfassung, Auswertungen, Kontoverwaltung, Support und Sicherheit.
Dauer	Vertragslaufzeit zuzüglich Export- und Löschfristen gemäß Ziffer 9 und dieser Anlage.
Art der Verarbeitung	Erheben, Erfassen, Ordnen, Strukturieren, Speichern, Anpassen, Auslesen, Abfragen, Verwenden, Übermitteln an autorisierte Empfänger, Einschränken, Exportieren, Löschen und Vernichten.
Zwecke	Verwaltung von Abteilungen sowie von Nutzern (auch ohne eigenen Zugang) einschließlich rollenbasierter Zugriffsrechte und abteilungsbezogener Planungsrechte; Schichtplanung im Wochenkalender einschließlich Prüfung auf Doppelbuchungen und genehmigte Abwesenheiten; Erstellung und Anwendung wiederkehrender Schichtvorlagen je Abteilung einschließlich Anzeige des Besetzungsstands; Bearbeitung von Abwesenheitsanträgen (insbesondere Urlaub und Krankenstand) mit Genehmigungsworkflow; Erfassung von Ein- und Auschecken am Diensttag; Erstellung von Berichten, insbesondere zu geplanten und geleisteten Stunden, Planungsdeckung und Abwesenheiten; technische Bereitstellung und Betrieb; Support; Missbrauchsabwehr; Datensicherung und Wiederherstellung; Versand transaktionaler Nachrichten.
Betroffene Personen	Beschäftigte, Auszubildende, Praktikanten, Leiharbeitskräfte, geringfügig Beschäftigte, regelmäßig eingebundene freie Mitarbeiter, Administratoren und sonstige vom Kunden autorisierte Nutzer.
Stammdaten	Name, geschäftliche E-Mail-Adresse, Nutzerkennung, Rolle, Abteilung, Organisation, Status des Nutzers.
Planungs- und Zeitdaten	Verfügbarkeiten, Dienstpläne, Schichten, Abteilungen, Ein- und Auscheckzeiten, geplante und geleistete Stunden, Freigaben und zugehörige Statusinformationen.
Abwesenheitsdaten	Abwesenheitsart, Zeitraum, Antrag, Genehmigungsstatus; Kategorie Krankheit als mögliches Gesundheitsdatum nach Art. 9 DSGVO. Keine Diagnosen, Atteste oder medizinischen Freitexte, sofern technisch ausgeschlossen beziehungsweise vertraglich untersagt.
Technische Daten	Anmelde- und Kontoereignisse, Zeitstempel, aufgerufene Ressource bzw. Route, HTTP-Status und Antwortzeiten, interne Nutzer- und Organisationskennung, Fehlerprotokolle sowie technische Ablaufprotokolle (Traces), soweit sie bei der Nutzung von Shiftio durch die Nutzer des Verantwortlichen entstehen. Zugriffs- und Sicherheitsprotokolle mit IP-Adresse verarbeitet der Auftragsverarbeiter als eigener Verantwortlicher zur Gewährleistung der Netz- und Informationssicherheit; dafür gilt die Datenschutzerklärung.
Kommunikationsdaten	Empfängeradresse, Versandstatus und Inhalt transaktionaler Nachrichten; Supportinhalte und Anhänge, soweit vom Kunden übermittelt.
Verarbeitungsorte	Nürnberg und Frankfurt, Deutschland; Wien und Microsoft-Rechenzentren in Österreich (Support)

Merkmal	Beschreibung
Export	Der Kunde kann während der Vertragslaufzeit sowie in der Übergangs- und Abrufzeit nach AGB Ziffer 10.3 (zusammen mindestens 60 Tage nach Vertragsende) per E-Mail an hallo@shiftio.at einen Export seiner Daten anfordern. Der Anbieter stellt die Daten innerhalb von 15 Werktagen in einem gängigen, maschinenlesbaren Format (CSV) über E-Mail bereit. Umfang wie AGB Ziffer 10.3: Organisation, Nutzer mit Rollen und Abteilungszuordnung, Abteilungen, Dienstpläne und Schichten samt Notizen und Markierungen, Schichtvorlagen samt Ausnahmen, Ein- und Auscheckzeiten samt Pausen und Kommentaren sowie Abwesenheiten samt Status und Notizen.
Löschung	Nach Ablauf der Abrufzeit löscht der Anbieter die Produktivdaten des Kunden innerhalb von 30 Tagen, auf Wunsch des Kunden auch früher. Sicherungskopien, einschließlich vorübergehender Sicherungen im Rahmen der Löschung, werden spätestens 30 Tage nach Löschung der Produktivdaten gelöscht. Technische Protokolle und Telemetriedaten werden spätestens 14 Tage nach ihrer Erstellung gelöscht. Daten, für die gesetzliche Aufbewahrungspflichten bestehen (insbesondere Rechnungs- und Zahlungsdaten), werden bis zum Ablauf dieser Pflichten aufbewahrt und für andere Zwecke gesperrt. Auf Anfrage bestätigt der Anbieter die Löschung in Textform.

Anlage 2: Technische und organisatorische Maßnahmen

Es gilt das am Ende dieses Dokuments beigefügte Dokument „Technische und organisatorische Maßnahmen“ in der bei Vertragsschluss bereitgestellten Fassung 1.0 (Stand 10.10.2026).

Anlage 3: Genehmigte Unterauftragsverarbeiter

Unternehmen	Leistung	Ort	Daten und Schutzmechanismus
Hetzner Online GmbH, Gunzenhausen	Hosting und Infrastruktur (Server, Datenbank, Speicher)	Rechenzentrum Nürnberg, Deutschland	Sämtliche Kundendaten sowie technische Protokolle; AVV gem. Art. 28 DSGVO; Verarbeitung ausschließlich in der EU
Amazon Web Services EMEA SARL, Luxemburg	(1) Amazon SES für transaktionale E-Mails; (2) Amazon S3 für verschlüsselte Datenbank-Sicherungen	Region eu-central-1 (Frankfurt, Deutschland)	(1) Empfängeradresse, Name, Nachrichteninhalt, Zustellmetadaten; (2) sämtliche Kundendaten als Sicherungskopie; AVV/DPA gem. Art. 28 DSGVO; Verschlüsselung im Ruhezustand (AES-256); für mögliche Zugriffe aus Drittländern: EU-Standardvertragsklauseln und EU-US Data Privacy Framework
Microsoft Ireland Operations Limited, Dublin	E-Mail-Postfach und Dateiablage (Microsoft 365) für Supportanfragen	Österreich (zugesagt EU/EFTA)	Inhalte von Supportanfragen inkl. Anhänge; DPA gem. Art. 28 DSGVO; EU-Standardvertragsklauseln und EU-US Data Privacy Framework

Anlage 4: Ansprechpartner und Weisungen

Funktion	Verantwortlicher	Auftragsverarbeiter
Vertragskontakt	Administrator laut Online-Bestellung	Marc Tutter, hallo@shiftio.at
Datenschutzkontakt	Administrator laut Online-Bestellung oder ein in Textform mitgeteilter Kontakt	Marc Tutter, hallo@shiftio.at
Sicherheitsvorfälle	Administrator laut Online-Bestellung oder ein in Textform mitgeteilter Kontakt	Thomas Bernhard, hallo@shiftio.at; Bearbeitung an Werktagen, an Wochenenden und Feiertagen nach bestem Bemühen
Weisungen	Administratoren des Kunden	Marc Tutter und Thomas Bernhard, Weisungen in Textform an hallo@shiftio.at

Technische und organisatorische Maßnahmen

Anlage 2 zur Vereinbarung zur Auftragsverarbeitung für Shiftio (Art. 28 Abs. 3 lit. c und Art. 32 DSGVO)

Anbieter: Marc Tutter und Thomas Bernhard, Wallgasse 14/34, 1060 Wien, gemeinsam auftretend unter der Geschäftsbezeichnung „Shiftio“
Stand: 10.10.2026, Fassung 1.0

1. Geltung und Schutzbedarf

Diese Anlage beschreibt die Maßnahmen, mit denen der Auftragsverarbeiter die Sicherheit der Auftragsdaten nach Art. 32 DSGVO gewährleistet. Sie gilt für die Anwendung, ihre Infrastruktur, Sicherungskopien, Support und administrative Zugänge.

Der Schutzbedarf für Vertraulichkeit und Integrität ist hoch, weil Beschäftigtendaten mehrerer Arbeitgeber verarbeitet werden und die Abwesenheitskategorie Krankheit ein Gesundheitsdatum nach Art. 9 DSGVO sein kann. Der Schutzbedarf für die Verfügbarkeit ist normal.

2. Vertraulichkeit

Maßnahme	Ausgestaltung
Zutritt	Produktivsysteme und Sicherungskopien liegen in nach ISO/IEC 27001 zertifizierten Rechenzentren der Unterauftragsverarbeiter (Anlage 3). Der Auftragsverarbeiter hat keinen eigenen physischen Zugang zu Servern. Arbeitsgeräte sind persönlich zugeordnet, verschlüsselt und durch eine automatische Bildschirmsperre geschützt.
Zugang	Personenbezogene Konten; Mehrfaktor-Authentifizierung für alle administrativen Konten. Verwaltungszugriffe sind nur über ein privates, verschlüsseltes Netz von freigegebenen Geräten oder von freigegebenen Adressen aus möglich; Verwaltungsoberflächen und Datenbanken sind aus dem Internet nicht erreichbar. Passwörter der Nutzer werden nur als Hash nach dem Stand der Technik gespeichert; wiederholte Fehlversuche bei der Anmeldung führen zu einer vorübergehenden Sperre.
Zugriff	Rollenmodell nach dem Erforderlichkeitsprinzip (Administrator, Manager, Mitarbeiter, mit Abteilungsbezug); Rollen vergibt der Administrator des Kunden. Administrativen Zugriff auf die Systeme haben nur die beiden Gesellschafter. Neue Zugänge werden nur mit Zustimmung beider erteilt und bei Wegfall der Berechtigung sofort entzogen.
Trennung	Logische Trennung der Daten je Kunde, die bei jeder Änderung automatisiert geprüft wird. Entwicklung und Tests laufen getrennt von der Produktion und nur mit synthetischen Daten.
Personal	Alle Personen mit Zugang sind vor dem ersten Zugriff schriftlich zur Vertraulichkeit verpflichtet (Datengeheimnis nach § 6 DSG) und werden jährlich zu Datenschutz und Informationssicherheit unterwiesen.

3. Verschlüsselung und Pseudonymisierung

Maßnahme	Ausgestaltung
Übertragung	Alle Verbindungen über das Internet und zwischen den Servern sind nach dem Stand der Technik verschlüsselt.

Maßnahme	Ausgestaltung
Speicherung	Datenträger der Server und Sicherungskopien sind verschlüsselt, Sicherungskopien mit AES-256. Zugangsschlüssel werden in einem gesonderten Schlüsselspeicher verwaltet und nicht im Quellcode abgelegt.
Datenexporte	Exporte werden nur als verschlüsseltes Archiv an die hinterlegte Administratoradresse gesendet; das Passwort wird auf getrenntem Weg übermittelt.
Pseudonymisierung	Technische Protokolle enthalten statt Namen und E-Mail-Adressen nur interne Kennungen.

4. Integrität

Maßnahme	Ausgestaltung
Änderungen am System	Änderungen an Software, Konfiguration und Infrastruktur erfolgen nur über eine Versionsverwaltung mit automatisierten Tests und sind mit Zeitpunkt und Autor nachvollziehbar.
Nachvollziehbarkeit	Anfragen an die Anwendung werden mit Zeitpunkt und interner Nutzerkennung protokolliert; die Protokolle werden 14 Tage aufbewahrt.
Schwachstellen	Automatische Sicherheitsanalyse des Quellcodes, regelmäßige Sicherheitstests der Anwendung und laufende Aktualisierung von Abhängigkeiten und Betriebssystemen; kritische Sicherheitsupdates werden vorrangig eingespielt.

5. Verfügbarkeit, Belastbarkeit und Wiederherstellung

Maßnahme	Ausgestaltung
Datensicherung	Tägliche Sicherung der Datenbanken und laufende Sicherung aller Änderungen, sodass bei einem Ausfall höchstens wenige Minuten an Daten verloren gehen. Die Sicherungen liegen verschlüsselt bei einem anderen Anbieter und an einem anderen Standort als die Produktivsysteme; aus den Produktivsystemen heraus können sie nicht sofort endgültig gelöscht werden. Sicherungen werden spätestens 30 Tage nach ihrer Erstellung gelöscht.
Ausfallsicherheit	Redundanter Betrieb von Anwendung und Datenbanken; automatische Überwachung mit Alarmierung bei Störungen.
Wiederherstellung	Ziel ist die Wiederherstellung des Betriebs innerhalb eines Werktags. Die Wiederherstellung aus Sicherungen wird regelmäßig getestet.

6. Regelmäßige Überprüfung

Kontrolle	Intervall
Berechtigungen und Zugangsschlüssel	halbjährlich
Wiederherstellung aus Sicherungen	halbjährlich
Sicherheitstests der Anwendung	mindestens jährlich
Unterauftragsverarbeiter (Verträge, Nachweise, Speicherorte)	jährlich

Kontrolle	Intervall
Diese Maßnahmen insgesamt	jährlich und nach wesentlichen Änderungen

Die Ergebnisse werden mit Datum dokumentiert.

7. Weitere Regelungen

Unterauftragsverarbeiter: Ziffer 6 und Anlage 3 der Vereinbarung. Datenschutzverletzungen: Ziffer 8; der Ablauf ist intern dokumentiert. Rückgabe und Löschung: Ziffer 9 und Anlage 1; Löschungen erfolgen nach einem dokumentierten Verfahren, werden je Vorgang protokolliert und auf Anfrage in Textform bestätigt.