



Vertrag über die Auftragsverarbeitung personenbezogener Daten

gemäß Art. 28 DSGVO

Stand: 10.03.2026

1. Einleitung, Geltungsbereich, Definitionen

1.1. Dieser Vertrag regelt die Rechte und Pflichten zwischen **Oliver Stang, handelnd unter Keybuki, Viersener Straße 318, 41063 Mönchengladbach** (im Folgenden „Auftragnehmer“) und dem **Kunden, der diesen Vertrag im Rahmen der Registrierung für die SaaS-Plattform Keybuki akzeptiert** (im Folgenden „Auftraggeber“), gemeinsam „Parteien“ genannt, im Rahmen einer Verarbeitung von personenbezogenen Daten im Auftrag im Sinne des Art. 28 der EU-Datenschutzgrundverordnung (im Folgenden „DSGVO“).

1.2. Dieser Vertrag findet auf alle Tätigkeiten Anwendung, bei denen der Auftragnehmer, seine Mitarbeiter oder durch ihn beauftragte Unterauftragnehmer (Subunternehmer) personenbezogene Daten des Auftraggebers verarbeiten.

1.3. In diesem Vertrag verwendete Begriffe sind entsprechend ihrer Definition in der DSGVO zu verstehen. Soweit Erklärungen im Folgenden „schriftlich“ zu erfolgen haben, ist die Schriftform nach § 126 BGB gemeint. Im Übrigen können Erklärungen auch in anderer Form erfolgen, soweit eine angemessene Nachweisbarkeit gewährleistet ist.

1.4. Dieser Vertrag wird mit Akzeptanz durch den Auftraggeber im Rahmen der Registrierung auf der SaaS-Plattform Keybuki in elektronischer Form gemäß Art. 28 Abs. 9 DSGVO geschlossen.

2. Gegenstand und Dauer der Verarbeitung

2.1. Der Auftragnehmer übernimmt folgende Verarbeitungen:

Die Erhebung/Erfassung, Speicherung, Verwendung, Organisation, Ordnen, Auslesen, Abfragen, Bereitstellung, Löschung und Vernichtung von **Personalstammdaten, Beschäftigungsdaten, Vergütungsdaten, Sozialversicherungsdaten, steuerlichen Daten, Gesundheitsdaten (Krankmeldungen, Atteste) und personalaktenbezogenen Dokumenten von Beschäftigten des Auftraggebers** zum Zwecke der **digitalen Personalaktenverwaltung im Rahmen der SaaS-Plattform „Keybuki“**.

Die Verarbeitung beruht auf dem zwischen den Parteien bestehenden Dienstleistungsvertrag „Keybuki – Digitale Personalakte (SaaS)“ vom Datum der Registrierung des Auftraggebers (im Folgenden „Hauptvertrag“).

2.2. Die Verarbeitung beginnt am Tag der Registrierung des Auftraggebers und erfolgt auf unbestimmte Zeit bis zur Kündigung dieses Vertrags oder des Hauptvertrags durch eine Partei.

3. Art und Zweck der Datenverarbeitung

3.1. Der Auftraggeber ist Arbeitgeber bzw. Steuerberater/Steuerberatungskanzlei, der/die die digitale Personalakte zur Verwaltung von Mitarbeiterdokumenten einsetzt. Der Auftragnehmer ist Betreiber der SaaS-Plattform „**Keybuki**“ (digitale Personalakte) unter dpa.keybuki.de.

3.2. Die Verarbeitung erfolgt in der Art der Speicherung, Organisation und Bereitstellung von Dokumenten und Stammdaten der Beschäftigten des Auftraggebers in einer cloudbasierten digitalen Personalakte. Der Auftraggeber lädt Dokumente über die Weboberfläche oder mobile Apps hoch. Der Auftragnehmer speichert diese auf seinen Servern und stellt sie dem Auftraggeber über die SaaS-Plattform zur Verfügung. Dokumente werden automatisiert mittels OCR und KI-gestützter Analyse klassifiziert. Die OCR/KI-Verarbeitung erfolgt ausschließlich lokal auf den Servern des Auftragnehmers in Deutschland, ohne Übermittlung an Dritte.

3.3. Die Verarbeitung dient dem Zweck der digitalen Personalaktenverwaltung, Dokumentenarchivierung und Stammdatenverwaltung für den Auftraggeber und erfolgt aufgrund dessen Interesses an der Rationalisierung und Digitalisierung der Personalaktenverwaltung, der Vereinfachung der Datenorganisation und der GoBD-konformen Dokumentenarchivierung.

3.4. Es werden folgende Kategorien personenbezogener Daten verarbeitet:

- Allgemeine Personendaten (Name, Geburtsdatum, Familienstand, Staatsangehörigkeit)
- Kommunikationsdaten (Anschrift, E-Mail-Adresse, Telefonnummer)
- Beschäftigungsdaten (Eintrittsdatum, Personalnummer, Abteilung)
- Steuer- und Sozialversicherungsdaten (Steuer-ID, Steuerklasse, SV-Nummer, Krankenkasse)
- Gesundheitsdaten (Krankmeldungen, Atteste) – besondere Kategorien gem. Art. 9 DSGVO
- Dokumente (Arbeitsverträge, Zeugnisse, Bescheinigungen, sonstige personalaktenbezogene Unterlagen)

3.5. Von der Verarbeitung betroffen sind:

- Beschäftigte des Auftraggebers (aktuelle und ehemalige Mitarbeiter)

4. Pflichten des Auftragnehmers

4.1. Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich wie vertraglich vereinbart oder wie vom Auftraggeber angewiesen, es sei denn, der Auftragnehmer ist gesetzlich zu einer bestimmten Verarbeitung verpflichtet. Sofern solche Verpflichtungen für ihn bestehen, teilt der Auftragnehmer diese dem Auftraggeber vor der Verarbeitung mit, es sei denn, die Mitteilung ist ihm gesetzlich verboten. Der Auftragnehmer verwendet darüber hinaus die zur Verarbeitung überlassenen Daten für keine anderen, insbesondere nicht für eigene Zwecke.

4.2. Der Auftragnehmer bestätigt, dass ihm die einschlägigen, allgemeinen datenschutzrechtlichen Vorschriften bekannt sind. Er beachtet die Grundsätze ordnungsgemäßer Datenverarbeitung.

4.3. Der Auftragnehmer verpflichtet sich, bei der Verarbeitung die Vertraulichkeit streng zu wahren.

4.4. Personen, die Kenntnis von den im Auftrag verarbeiteten Daten erhalten können, haben sich schriftlich zur Vertraulichkeit zu verpflichten, soweit sie nicht bereits gesetzlich einer einschlägigen Geheimhaltungspflicht unterliegen.

4.5. Der Auftragnehmer sichert zu, dass die bei ihm zur Verarbeitung eingesetzten Personen vor Beginn der Verarbeitung mit den relevanten Bestimmungen des Datenschutzes und dieses Vertrags vertraut gemacht wurden. Entsprechende Schulungs- und Sensibilisierungsmaßnahmen sind angemessen regelmäßig zu wiederholen. Der Auftragnehmer trägt dafür Sorge, dass zur Auftragsverarbeitung eingesetzte Personen hinsichtlich der Erfüllung der Datenschutzerfordernisse laufend angemessen angeleitet und überwacht werden.

4.6. Im Zusammenhang mit der beauftragten Verarbeitung hat der Auftragnehmer den Auftraggeber bei Erstellung und Fortschreibung des Verzeichnisses der Verarbeitungstätigkeiten sowie bei

Durchführung der Datenschutzfolgeabschätzung zu unterstützen. Alle erforderlichen Angaben und Dokumentationen sind vorzuhalten und dem Auftraggeber auf Anforderung unverzüglich zuzuleiten.

4.7. Wird der Auftraggeber durch Aufsichtsbehörden oder andere Stellen einer Kontrolle unterzogen oder machen betroffene Personen ihm gegenüber Rechte geltend, verpflichtet sich der Auftragnehmer den Auftraggeber im erforderlichen Umfang zu unterstützen, soweit die Verarbeitung im Auftrag betroffen ist.

4.8. Auskünfte an Dritte oder Betroffene darf der Auftragnehmer nur nach vorheriger Zustimmung durch den Auftraggeber erteilen. Direkt an ihn gerichtete Anfragen wird er unverzüglich an den Auftraggeber weiterleiten.

4.9. Soweit gesetzlich verpflichtet, bestellt der Auftragnehmer eine fachkundige und zuverlässige Person als Beauftragten für den Datenschutz. Es ist sicherzustellen, dass für den Beauftragten keine Interessenskonflikte bestehen. Der Auftragnehmer teilt dem Auftraggeber unverzüglich die Kontaktdaten des Datenschutzbeauftragten mit oder begründet, weshalb kein Beauftragter bestellt wurde.

4.10. Die Auftragsverarbeitung erfolgt grundsätzlich innerhalb der EU oder des EWR. Jegliche Verlagerung in ein Drittland darf nur mit Zustimmung des Auftraggebers und unter den in Kapitel V der DSGVO enthaltenen Bedingungen sowie bei Einhaltung der Bestimmungen dieses Vertrags erfolgen.

5. Technische und organisatorische Maßnahmen

5.1. Die in Anlage 1 beschriebenen Datensicherheitsmaßnahmen (technische und organisatorische Maßnahmen) werden als verbindlich festgelegt. Sie definieren das vom Auftragnehmer geschuldete Minimum. Die Beschreibung der Maßnahmen muss so detailliert erfolgen, dass für einen sachkundigen Dritten allein aufgrund der Beschreibung jederzeit zweifelsfrei erkennbar ist, was das geschuldete Minimum sein soll.

5.2. Die Datensicherheitsmaßnahmen können der technischen und organisatorischen Weiterentwicklung entsprechend angepasst werden, solange das hier vereinbarte Niveau nicht unterschritten wird. Änderungen sind dem Auftraggeber unverzüglich mitzuteilen. Wesentliche Änderungen sind zwischen den Parteien zu vereinbaren.

5.3. Soweit die getroffenen Sicherheitsmaßnahmen den Anforderungen des Auftraggebers nicht oder nicht mehr genügen, benachrichtigt der Auftragnehmer den Auftraggeber unverzüglich.

5.4. Der Auftragnehmer sichert zu, dass die im Auftrag verarbeiteten Daten von sonstigen Datenbeständen strikt getrennt werden.

5.5. Kopien oder Duplikate werden ohne Wissen des Auftraggebers nicht erstellt. Ausgenommen sind technisch notwendige, temporäre Vervielfältigungen, soweit eine Beeinträchtigung des hier vereinbarten Datenschutzniveaus ausgeschlossen ist.

5.6. Die Verarbeitung von Daten im Auftrag in Privatwohnungen sowie die Verarbeitung von Daten im Auftrag mit Privatgeräten sind unter keinen Umständen gestattet.

5.7. Dedizierte Datenträger, die vom Auftraggeber stammen bzw. für den Auftraggeber genutzt werden, werden besonders gekennzeichnet und unterliegen der laufenden Verwaltung. Sie sind jederzeit angemessen aufzubewahren und dürfen unbefugten Personen nicht zugänglich sein.

5.8. Der Auftraggeber ist berechtigt, die Erfüllung der Pflichten durch den Auftragnehmer, insbesondere die vollständige Umsetzung der vereinbarten technischen und organisatorischen Maßnahmen sowie ihre Wirksamkeit, jederzeit zu kontrollieren und zu überprüfen.

6. Regelungen zur Berichtigung, Löschung und Sperrung von Daten

6.1. Im Rahmen des Auftrags verarbeitete Daten wird der Auftragnehmer nur entsprechend der getroffenen vertraglichen Vereinbarung oder nach Weisung des Auftraggebers berichtigen, löschen oder sperren.

6.2. Den entsprechenden Weisungen des Auftraggebers wird der Auftragnehmer jederzeit und auch über die Beendigung dieses Vertrages hinaus Folge leisten.

7. Unterauftragsverhältnisse

7.1. Die Beauftragung von Subunternehmern ist nur mit schriftlicher Zustimmung des Auftraggebers im Einzelfall zugelassen.

7.2. Die Zustimmung ist nur möglich, wenn dem Subunternehmer vertraglich mindestens Datenschutzpflichten auferlegt wurden, die den in diesem Vertrag vereinbarten vergleichbar sind. Der Auftraggeber erhält auf Verlangen Einsicht in die relevanten Verträge zwischen Auftragnehmer und Subunternehmer.

7.3. Die Rechte des Auftraggebers müssen auch gegenüber dem Subunternehmer wirksam ausgeübt werden können. Insbesondere muss der Auftraggeber berechtigt sein, jederzeit Kontrollen auch bei Subunternehmern durchzuführen oder durch Dritte durchführen zu lassen.

7.4. Die Verantwortlichkeiten des Auftragnehmers und des Subunternehmers sind eindeutig voneinander abzugrenzen.

7.5. Eine weitere Subbeauftragung durch den Subunternehmer ist nicht zulässig.

7.6. Der Auftragnehmer wählt den Subunternehmer unter besonderer Berücksichtigung der Eignung der vom Subunternehmer getroffenen technischen und organisatorischen Maßnahmen sorgfältig aus.

7.7. Die Weiterleitung von im Auftrag verarbeiteten Daten an den Subunternehmer ist erst zulässig, wenn sich der Auftragnehmer dokumentiert davon überzeugt hat, dass der Subunternehmer seine Verpflichtungen vollständig erfüllt hat.

7.8. Die Beauftragung von Subunternehmern, die Verarbeitungen nicht ausschließlich aus dem Gebiet der EU oder des EWR erbringen, ist nur bei Beachtung der in Ziffer 4.10. genannten Bedingungen möglich.

7.9. Der Auftragnehmer hat die Einhaltung der Pflichten des Subunternehmers regelmäßig, spätestens alle 12 Monate, angemessen zu überprüfen.

7.10. Kommt der Subunternehmer seinen Datenschutzpflichten nicht nach, so haftet hierfür der Auftragnehmer gegenüber dem Auftraggeber.

7.11. Zurzeit sind die in Anlage 2 bezeichneten Subunternehmer mit der Verarbeitung von personenbezogenen Daten beschäftigt und durch den Auftraggeber genehmigt.

7.12. Unterauftragsverhältnisse im Sinne dieses Vertrags sind nur solche Leistungen, die einen direkten Zusammenhang mit der Erbringung der Hauptleistung aufweisen. Nebenleistungen sind nicht erfasst.

8. Rechte und Pflichten des Auftraggebers

8.1. Für die Beurteilung der Zulässigkeit der beauftragten Verarbeitung sowie für die Wahrung der Rechte von Betroffenen ist allein der Auftraggeber verantwortlich.

8.2. Der Auftraggeber erteilt alle Aufträge, Teilaufträge oder Weisungen dokumentiert. In Eilfällen können Weisungen mündlich erteilt werden. Solche Weisungen wird der Auftraggeber unverzüglich dokumentiert bestätigen.

8.3. Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Prüfung der Auftragsergebnisse feststellt.

8.4. Der Auftraggeber ist berechtigt, die Einhaltung der Vorschriften über den Datenschutz und der vertraglichen Vereinbarungen beim Auftragnehmer in angemessenem Umfang selbst oder durch Dritte zu kontrollieren.

8.5. Kontrollen beim Auftragnehmer haben ohne vermeidbare Störungen seines Geschäftsbetriebs zu erfolgen und finden nach angemessener Vorankündigung und zu Geschäftszeiten, sowie nicht häufiger als alle 12 Monate statt.

9. Mitteilungspflichten

9.1. Der Auftragnehmer teilt dem Auftraggeber Verletzungen des Schutzes personenbezogener Daten unverzüglich mit. Auch begründete Verdachtsfälle sind mitzuteilen. Die Mitteilung hat spätestens innerhalb von 24 Stunden ab Kenntnis des Auftragnehmers zu erfolgen. Sie muss mindestens folgende Angaben enthalten:

- eine Beschreibung der Art der Verletzung, soweit möglich mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen und Datensätze;
- den Namen und die Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle;
- eine Beschreibung der wahrscheinlichen Folgen der Verletzung;
- eine Beschreibung der ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung und Abmilderung.

9.2. Ebenfalls unverzüglich mitzuteilen sind erhebliche Störungen bei der Auftragserledigung sowie Verstöße gegen datenschutzrechtliche Bestimmungen oder die in diesem Vertrag getroffenen Festlegungen.

9.3. Der Auftragnehmer informiert den Auftraggeber unverzüglich von Kontrollen oder Maßnahmen von Aufsichtsbehörden, soweit diese Bezüge zur Auftragsverarbeitung aufweisen.

9.4. Der Auftragnehmer sichert zu, den Auftraggeber bei dessen Pflichten nach Art. 33 und 34 DSGVO im erforderlichen Umfang zu unterstützen.

10. Weisungen

10.1. Der Auftraggeber behält sich hinsichtlich der Verarbeitung im Auftrag ein umfassendes Weisungsrecht vor.

10.2. Auftraggeber und Auftragnehmer benennen die zur Erteilung und Annahme von Weisungen ausschließlich befugten Personen in Anlage 3.

10.3. Bei einem Wechsel oder einer längerfristigen Verhinderung der benannten Personen sind der anderen Partei Nachfolger bzw. Vertreter unverzüglich mitzuteilen.

10.4. Der Auftragnehmer wird den Auftraggeber unverzüglich darauf aufmerksam machen, wenn eine erteilte Weisung seiner Meinung nach gegen gesetzliche Vorschriften verstößt. Der Auftragnehmer ist berechtigt, die Durchführung solange auszusetzen, bis sie bestätigt oder geändert wird.

10.5. Der Auftragnehmer hat ihm erteilte Weisungen und deren Umsetzung zu dokumentieren.

11. Beendigung des Auftrags

11.1. Bei Beendigung des Auftragsverhältnisses oder jederzeit auf Verlangen des Auftraggebers hat der Auftragnehmer die im Auftrag verarbeiteten Daten nach Wahl des Auftraggebers entweder zu vernichten oder an den Auftraggeber zu übergeben. Ebenfalls zu vernichten sind sämtliche vorhandene Kopien der Daten. Die Vernichtung hat so zu erfolgen, dass eine Wiederherstellung auch von Restinformationen mit vertretbarem Aufwand nicht mehr möglich ist.

11.2. Der Auftragnehmer ist verpflichtet, die unverzügliche Rückgabe bzw. Löschung auch bei Subunternehmern herbeizuführen.

11.3. Der Auftragnehmer hat den Nachweis der ordnungsgemäßen Vernichtung zu führen und dem Auftraggeber unverzüglich vorzulegen.

11.4. Dokumentationen, die dem Nachweis der ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer den jeweiligen Aufbewahrungsfristen entsprechend auch über das Vertragsende hinaus aufzubewahren.

12. Vergütung

Die Vergütung des Auftragnehmers ist abschließend im Hauptvertrag geregelt. Eine gesonderte Vergütung oder Kostenerstattung im Rahmen dieses Vertrages erfolgt nicht.

13. Haftung

13.1. Für den Ersatz von Schäden, die eine Person wegen einer unzulässigen oder unrichtigen Datenverarbeitung im Rahmen des Auftragsverhältnisses erleidet, haften Auftraggeber und Auftragnehmer als Gesamtschuldner.

13.2. Der Auftragnehmer trägt die Beweislast dafür, dass ein Schaden nicht Folge eines von ihm zu vertretenden Umstandes ist, soweit die relevanten Daten von ihm unter dieser Vereinbarung verarbeitet wurden.

13.3. Der Auftragnehmer haftet dem Auftraggeber für Schäden, die der Auftragnehmer, seine Mitarbeiter bzw. die von ihm eingesetzten Subdienstleister im Zusammenhang mit der Erbringung der beauftragten vertraglichen Leistung schuldhaft verursachen.

13.4. Die Ziffern 13.2. und 13.3 gelten nicht, soweit der Schaden durch die korrekte Umsetzung der beauftragten Dienstleistung oder einer vom Auftraggeber erteilten Weisung entstanden ist.

14. Sonderkündigungsrecht

14.1. Der Auftraggeber kann den Hauptvertrag und diese Vereinbarung jederzeit ohne Einhaltung einer Frist kündigen („außerordentliche Kündigung“), wenn ein schwerwiegender Verstoß des Auftragnehmers gegen Datenschutzvorschriften oder die Bestimmungen dieser Vereinbarung vorliegt, der Auftragnehmer eine rechtmäßige Weisung des Auftraggebers nicht ausführen kann oder will oder der Auftragnehmer Kontrollrechte des Auftraggebers vertragswidrig verweigert.

14.2. Ein schwerwiegender Verstoß liegt insbesondere vor, wenn der Auftragnehmer die in dieser Vereinbarung bestimmten Pflichten, insbesondere die vereinbarten technischen und organisatorischen Maßnahmen, in erheblichem Maße nicht erfüllt oder nicht erfüllt hat.

14.3. Bei unerheblichen Verstößen setzt der Auftraggeber dem Auftragnehmer eine angemessene Frist zur Abhilfe. Erfolgt die Abhilfe nicht rechtzeitig, so ist der Auftraggeber zur außerordentlichen Kündigung berechtigt.

14.4. Der Auftragnehmer hat dem Auftraggeber alle Kosten zu erstatten, die diesem durch die verfrühte Beendigung in Folge einer außerordentlichen Kündigung durch den Auftraggeber entstehen.

15. Sonstiges

15.1. Beide Parteien sind verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen der jeweils anderen Partei auch über die Beendigung des Vertrages vertraulich zu behandeln.

15.2. Sollte Eigentum des Auftraggebers beim Auftragnehmer durch Maßnahmen Dritter gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich zu verständigen.

15.3. Für Nebenabreden ist die Schriftform erforderlich.

15.4. Die Einrede des Zurückbehaltungsrechts im Sinne des § 273 BGB wird hinsichtlich der im Auftrag verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen.

15.5. Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht.

Anlage 1

Technische und organisatorische Maßnahmen

Im Folgenden werden die technischen und organisatorischen Maßnahmen zur Gewährleistung von Datenschutz und Datensicherheit festgelegt, die der Auftragnehmer mindestens einzurichten und laufend aufrecht zu erhalten hat.

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

Zutrittskontrolle

- Server-Standort: Hetzner Online GmbH, Rechenzentren in Deutschland (ISO 27001 zertifiziert)
- Physischer Zugang ausschließlich durch Hetzner-Personal (biometrische Zugangskontrolle, Videoüberwachung)

Zugangskontrolle

- SSH-Only-Zugang zum Server (SSH-Key-Authentifizierung, kein Passwort-Login)
- UFW-Firewall mit Whitelist-Konfiguration (nur Ports 80, 443, 22)
- JWT-basierte Authentifizierung für alle API-Zugriffe
- Cookie-basiertes SSO für domainübergreifende Authentifizierung
- Refresh-Token mit SHA-256-gehashter Speicherung

Zugriffskontrolle

- Mandantentrennung auf Datenbankebene (mandant_id)
- Rollenbasiertes Berechtigungssystem (Admin, HR-Mitarbeiter)
- Audit-Log aller Zugriffe inkl. Lesezugriffe (Zeitstempel, IP-Adresse, User-Agent)

Trennungskontrolle

- Logische Trennung der Mandantendaten über mandant_id in der Datenbank
- Separate Dokumentenverzeichnisse pro Mandant im Dateisystem

2. Integrität (Art. 32 Abs. 1 lit. b DSGVO)

Weitergabekontrolle

- SSL/TLS-Verschlüsselung (HTTPS) für sämtliche Datenübertragungen
- CORS-Konfiguration mit Whitelist erlaubter Origins
- OCR/KI-Verarbeitung ausschließlich lokal, keine Übermittlung an Dritte

Eingabekontrolle

- Vollständiger Audit-Trail aller Dokumentenoperationen
- SHA-256-Hashwerte für jedes Dokument bei Upload (GoBD-konform)
- Dokumentenversionierung mit Vorgänger-Referenz

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)

- Garantierte Verfügbarkeit von 99,5 %
- Tägliche AES-256-verschlüsselte Backups auf externe Hetzner Storage Box
- Backup-Rotation: 7 tägliche, 4 wöchentliche, 1 monatliche Sicherung, max. 60 Tage
- Tägliche automatisierte Integritätsprüfung aller Dokumente (SHA-256-Abgleich)

- E-Mail-Benachrichtigung bei Integritätsverletzungen
- Soft-Delete mit 30-tägigem Papierkorb

4. Verfahren zur regelmäßigen Überprüfung (Art. 32 Abs. 1 lit. d DSGVO)

- Regelmäßige Überprüfung und Aktualisierung der Sicherheitsmaßnahmen
- Automatisierte tägliche Integritätsprüfung aller gespeicherten Dokumente
- Monitoring der Server-Verfügbarkeit

Anlage 2

Zugelassene Subdienstleister

Der Auftraggeber genehmigt den Einsatz der folgenden Subdienstleister durch den Auftragnehmer:

Subdienstleister	Anschrift	Auftragsinhalt
Hetzner Online GmbH	Industriestr. 25, 91710 Gunzenhausen	Server-Hosting, Backup-Storage
Sendinblue GmbH (Brevo)	Köpenicker Str. 126, 10179 Berlin	Transaktionale E-Mails
Stripe Payments Europe Ltd.	1 Grand Canal Street Lower, Dublin, D02 H210, Irland	Zahlungsabwicklung

Anlage 3

Weisungsberechtigte Personen

Folgende Personen sind zur Erteilung und Entgegennahme von Weisungen befugt:

1. Weisungserteilung (Auftraggeber)

Der jeweilige Admin-Nutzer des Mandanten-Kontos bei Keybuki, identifiziert durch seine bei der Registrierung hinterlegte E-Mail-Adresse.

2. Weisungsentgegennahme (Auftragnehmer)

Oliver Stang

E-Mail: info@keybuki.de

Tel.: 015146338944