

# Auftragsverarbeitungsvertrag nach Art. 28 DSGVO

## für die Nutzung der Belegebox

Stand: 01.10.2026 · Version 2.0

### Parteien

---

Dieser Auftragsverarbeitungsvertrag (nachfolgend „Vertrag“ oder „AVV“) wird geschlossen zwischen:

dem Kunden der Belegebox gemäß Hauptvertrag, Angebot, Bestellformular, Online-Bestellung oder sonstiger Leistungsvereinbarung,

nachfolgend „Auftraggeber“ oder „Verantwortlicher“,

und

Docunout GmbH, Schwabacher Str. 3, 90439 Nürnberg, Deutschland, HRB 36224, Amtsgericht Nürnberg, E-Mail: [info@belegebox.de](mailto:info@belegebox.de), Tel.: +49 911 4771728-0, vertreten durch die Geschäftsführer Matthias Meyer und Alexander Steiß, USt-IdNr. DE323201649,

nachfolgend „Auftragnehmer“ oder „Auftragsverarbeiter“.

Datenschutzbeauftragter des Auftragnehmers: Oliver Fouquet, Rechtsanwalt  
KGH Anwaltskanzlei Kreuzer Goßler Horlamus und Partner mbB  
Registergericht Nürnberg PR 235, Fürther Straße 98 – 100 (Sitz), 90429 Nürnberg  
Telefon: +49(0)911 32386-0

Auftraggeber und Auftragnehmer werden gemeinsam auch „Parteien“ genannt.

### Präambel

---

Der Auftragnehmer stellt dem Auftraggeber die Software- und Cloud-Lösung „Belegebox“ zur Verfügung. Die Belegebox dient insbesondere der digitalen Erfassung, Speicherung, Verwaltung, Bearbeitung, Prüfung, Freigabe, Kommentierung, Suche, Archivierung und Weiterleitung von Belegen, Rechnungen, E-Rechnungen, Verträgen, Geschäftsdokumenten, E-Mails und sonstigen Unterlagen.

Im Rahmen dieser Leistungen verarbeitet der Auftragnehmer personenbezogene Daten im Auftrag des Auftraggebers. Dieser Vertrag konkretisiert die Rechte und Pflichten der Parteien nach Art. 28 DSGVO. Die Verarbeitung erfolgt ausschließlich auf dokumentierte Weisung des Auftraggebers, soweit keine gesetzliche Verarbeitungspflicht des Auftragnehmers besteht.

### § 1 Gegenstand, Dauer, Art und Zweck der Verarbeitung

---

(1) Gegenstand dieses Vertrags ist die Verarbeitung personenbezogener Daten durch den Auftragnehmer im Zusammenhang mit Bereitstellung, Betrieb, Wartung, Support und Weiterentwicklung der Belegebox.

(2) Die Verarbeitung umfasst insbesondere die Bereitstellung der Anwendung, Speicherung und Verwaltung von Dokumenten, Nutzer-, Rechte- und Rollenverwaltung, Upload, Import, Export und Weiterleitung von Dokumenten, Freigabe- und Prüfprozesse, Such-, Kommentar-

und Kommunikationsfunktionen, Schnittstellen, technische Protokollierung, Backup, Wiederherstellung, Support, Fehleranalyse, Wartung und Updates.

(3) Zweck der Verarbeitung ist die Erbringung der vertraglich vereinbarten Belegebox-Leistungen, insbesondere digitale Beleg- und Dokumentenverwaltung, Rechnungs- und E-Rechnungsprüfung, GoBD-orientierte Archivierung, Freigabe- und Kontrollprozesse, Suche und Wiederauffindbarkeit, Datensicherung sowie Support.

(4) Die Dauer der Verarbeitung richtet sich nach der Laufzeit des Hauptvertrags. Der Vertrag endet automatisch mit Beendigung aller Leistungen, bei denen personenbezogene Daten des Auftraggebers verarbeitet werden. Nachvertragliche Pflichten zur Rückgabe, Löschung, Dokumentation und Nachweiseerbringung bleiben unberührt.

## **§ 2 Kategorien personenbezogener Daten und betroffener Personen**

---

(1) Je nach Nutzung durch den Auftraggeber können insbesondere folgende Kategorien personenbezogener Daten verarbeitet werden:

- Stammdaten und Kontaktdaten, insbesondere Namen, Anschriften, E-Mail-Adressen, Telefonnummern, Firmenzugehörigkeit, Kunden-, Lieferanten-, Mandanten- und Geschäftspartnerdaten;
- Nutzer- und Berechtigungsdaten, insbesondere Benutzerkonten, Rollen, Berechtigungen, Login-Daten, technische Kennungen, IP-Adressen, Protokolldaten und Zeitstempel;
- Dokumenten- und Inhaltsdaten, insbesondere Rechnungen, Belege, Verträge, Lieferscheine, Angebote, E-Mails, E-Mail-Anhänge, Geschäftskorrespondenz, Kommentare, Notizen, Freigabeinformationen, OCR-Volltexte und Metadaten;
- Finanz-, Zahlungs-, Steuer- und Buchhaltungsdaten, soweit in Dokumenten oder Metadaten enthalten;
- Beschäftigtendaten sowie Reisekosten-, Auslagen-, Lohn- oder HR-Dokumente, soweit der Auftraggeber solche Daten verarbeitet;
- besondere Kategorien personenbezogener Daten nach Art. 9 DSGVO sowie Daten nach Art. 10 DSGVO, soweit der Auftraggeber solche Daten in die Belegebox einstellt.

(2) Betroffene Personen können insbesondere Beschäftigte, Organe und Beauftragte des Auftraggebers, Kunden, Mandanten, Patienten, Apothekenkunden, Lieferanten, Dienstleister, Geschäftspartner, Ansprechpartner bei Dritten, Steuerberater, Rechtsanwälte und sonstige Berater, Bewerber sowie sonstige natürliche Personen sein, deren Daten in den vom Auftraggeber verarbeiteten Dokumenten enthalten sind.

(3) Der Auftragnehmer bestimmt die konkreten Inhalte der vom Auftraggeber eingestellten Dokumente nicht. Der Auftraggeber bleibt dafür verantwortlich, welche Datenarten in die Belegebox eingestellt werden und ob deren Verarbeitung rechtmäßig ist.

## **§ 3 Weisungsbindung und Verantwortlichkeit**

---

(1) Der Auftraggeber ist Verantwortlicher im Sinne der DSGVO. Er ist für die Rechtmäßigkeit der Verarbeitung, die Zulässigkeit der Datenübermittlung an den Auftragnehmer und die Wahrung der Rechte betroffener Personen verantwortlich.

(2) Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich auf dokumentierte Weisung des Auftraggebers. Die Weisungen ergeben sich aus dem Hauptvertrag, diesem Vertrag, den vereinbarten Produktfunktionen sowie aus dokumentierten Einstellungen und Funktionsaktivierungen innerhalb der Belegebox.

(3) Einzelweisungen können schriftlich oder in Textform, insbesondere per E-Mail, Ticketsystem oder dokumentierter Produktfunktion, erteilt werden. Mündliche Weisungen sind vom Auftraggeber unverzüglich in Textform zu bestätigen.

(4) Der Auftragnehmer informiert den Auftraggeber unverzüglich, wenn er der Auffassung ist, dass eine Weisung gegen Datenschutzrecht verstößt. Er ist berechtigt, die Durchführung einer solchen Weisung bis zur Bestätigung oder Änderung auszusetzen.

(5) Der Auftragnehmer darf personenbezogene Daten nicht eigenmächtig löschen, verändern, herausgeben, übertragen oder Dritten zugänglich machen, außer dies ist zur Vertragserfüllung erforderlich, durch diesen Vertrag erlaubt oder vom Auftraggeber angewiesen.

## **§ 4 Vertraulichkeit und Berufsgeheimnisse**

---

(1) Der Auftragnehmer stellt sicher, dass alle Personen, die personenbezogene Daten des Auftraggebers verarbeiten oder darauf zugreifen können, zur Vertraulichkeit verpflichtet sind. Die Verpflichtung besteht auch nach Beendigung der Tätigkeit fort.

(2) Zugriffe auf personenbezogene Daten werden nach dem Need-to-know-Prinzip beschränkt. Beschäftigte werden regelmäßig zu Datenschutz, Informationssicherheit und Vertraulichkeit sensibilisiert.

(3) Soweit der Auftraggeber oder dessen Kunden einer Berufsverschwiegenheit nach § 203 StGB oder vergleichbaren berufsrechtlichen Pflichten unterliegen, verpflichtet der Auftragnehmer alle Beschäftigten und Unterauftragnehmer, die auf solche Daten zugreifen können, auf besondere Verschwiegenheit im Sinne des § 203 Abs. 4 StGB. Zugriffe auf diese Daten erfolgen nur im erforderlichen Umfang und werden dokumentiert. Der Auftraggeber bleibt für die Prüfung der berufsrechtlichen Zulässigkeit im konkreten Einsatzfall verantwortlich.

(4) Docunout ist bekannt, dass Mitarbeitern des Berufsträgers und allen sonstigen Personen, die bei dessen beruflicher Tätigkeit mitwirken, ein Zeugnisverweigerungsrecht über solche Vorgänge zusteht, die im Zusammenhang mit der Durchführung ihrer Dienstleistung stehen, und diese über solche Vorgänge gegenüber Dritten - auch gegenüber Gerichten - im Zweifel nur dann Auskünfte erteilen dürfen, wenn sie von der Verpflichtung zur Verschwiegenheit entbunden sind.

(5) Docunout ist berechtigt, Dritte zur Vertragserfüllung heranzuziehen. Beim Einsatz von Dritten verpflichtet sich die Docunout, diese in Textform unter Belehrung über die strafrechtlichen Folgen einer Pflichtverletzung zur Verschwiegenheit zu verpflichten, soweit diese im Rahmen ihrer Tätigkeit Kenntnis von fremden Geheimnissen im Sinne dieser Zusatzvereinbarung erlangen könnten. In Bezug auf ihre Arbeitskräfte erfüllt die Docunout die rechtlichen Anforderungen.

## **§ 5 Technische und organisatorische Maßnahmen**

---

(1) Der Auftragnehmer trifft geeignete technische und organisatorische Maßnahmen nach Art. 32 DSGVO, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Die Maßnahmen ergeben sich aus Anlage 2 und bilden das vereinbarte Mindestschutzniveau.

(2) Der Auftragnehmer darf die Maßnahmen weiterentwickeln und anpassen, sofern das vereinbarte Sicherheitsniveau nicht unterschritten wird. Wesentliche Änderungen werden dokumentiert und dem Auftraggeber auf Anfrage mitgeteilt.

## **§ 6 Unterauftragnehmer**

---

(1) Der Auftraggeber erteilt dem Auftragnehmer eine allgemeine Genehmigung zum Einsatz von Unterauftragnehmern. Die jeweils aktuelle Unterauftragnehmerliste wird dem Auftraggeber gemäß Anlage 3 zugänglich gemacht.

(2) Der Auftragnehmer informiert den Auftraggeber über jede beabsichtigte Hinzuziehung oder Ersetzung eines Unterauftragnehmers in Textform, in der Regel mindestens vier Wochen vor der geplanten Beauftragung, unter Angabe von Name, Anschrift, Sitzland und vorgesehener Leistung.

(3) Der Auftraggeber kann der Hinzuziehung oder Ersetzung innerhalb von vier Wochen nach Zugang der Information aus wichtigem datenschutzrechtlichem Grund in Textform widersprechen. Erfolgt innerhalb dieser Frist kein Widerspruch, gilt der Unterauftragnehmer als genehmigt. Bei berechtigtem Widerspruch werden sich die Parteien um eine einvernehmliche Lösung bemühen; kommt eine solche nicht zustande und kann der Auftragnehmer die betroffene Leistung nicht ohne den Unterauftragnehmer erbringen, steht dem Auftraggeber hinsichtlich der betroffenen Leistung ein Sonderkündigungsrecht zu.

(4) Der Auftragnehmer verpflichtet Unterauftragnehmer vertraglich mindestens auf dieselben Datenschutzpflichten, die in diesem Vertrag vereinbart sind, und bleibt gegenüber dem Auftraggeber für deren Einhaltung verantwortlich.

(5) Reine Nebenleistungen ohne Zugriff auf personenbezogene Inhaltsdaten, insbesondere Post-, Telekommunikations-, Bank-, Entsorgungs-, Gebäude- oder allgemeine Verwaltungsdienstleistungen, gelten nicht als genehmigungspflichtige Unterauftragnehmer.

(6) DATEV, lexware office, sevDesk, Invoicefetcher, Treuhand Hannover, Innotax oder andere Drittsysteme gelten nicht automatisch als Unterauftragnehmer des Auftragnehmers. Erfolgt eine Übertragung an solche Systeme ausschließlich auf Weisung und im Verantwortungsbereich des Auftraggebers, handelt es sich um Empfänger oder Systeme des Auftraggebers. Beauftragt der Auftragnehmer solche Dienste im eigenen Namen zur Erbringung der Belegebox-Leistung, werden sie als Unterauftragnehmer behandelt.

## **§ 7 Ort der Verarbeitung und Drittlandtransfers**

---

(1) Die Verarbeitung personenbezogener Daten erfolgt grundsätzlich in der Bundesrepublik Deutschland oder innerhalb der Europäischen Union bzw. des Europäischen Wirtschaftsraums. Produktive Inhaltsdaten der Belegebox werden in Deutschland verarbeitet.

(2) Eine Verarbeitung in Drittländern oder durch Empfänger in Drittländern ist nur zulässig, wenn der Auftraggeber dies zuvor angewiesen oder ihr zugestimmt hat, die Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind und geeignete Garantien bestehen, insbesondere ein Angemessenheitsbeschluss, EU-Standardvertragsklauseln oder ein anderer zulässiger Mechanismus.

(3) Der Auftragnehmer informiert den Auftraggeber vor jeder geplanten dauerhaften Verlagerung von Verarbeitungstätigkeiten in ein Drittland und stellt sicher, dass Unterauftragnehmer an die Vorgaben dieses Paragraphen gebunden werden.

## **§ 8 Support, Fernwartung und Produktivdatenzugriff**

---

(1) Support- und Wartungszugriffe erfolgen nur, soweit sie zur Vertragserfüllung, Fehleranalyse, Sicherheit oder auf Grundlage einer dokumentierten Weisung erforderlich sind.

(2) Zugriffe auf Produktivdaten werden auf das erforderliche Maß beschränkt, angemessen abgesichert und protokolliert. Soweit möglich, erfolgen Fehleranalysen ohne Zugriff auf personenbezogene Inhaltsdaten.

(3) Kopien von Produktivdaten zu Test-, Entwicklungs- oder Fehleranalysezwecken sind zu vermeiden. Soweit sie ausnahmsweise erforderlich sind, werden sie nach Zweckerreichung gelöscht oder anonymisiert. Produktivdaten dürfen nicht ohne dokumentierte Weisung in Entwicklungs-, Test- oder Schulungssysteme übernommen werden.

## **§ 9 OCR-, E-Rechnungsprüfungs-, Automatisierungs- und KI-Funktionen**

---

(1) Soweit die Belegebox OCR-, E-Rechnungsprüfungs-, Klassifizierungs-, Automatisierungs- oder KI-Funktionen bereitstellt, erfolgen diese Verarbeitungen als Bestandteil der Belegebox-Leistung im Auftrag des Auftraggebers. Eigenentwickelte KI- und Klassifizierungsfunktionen werden innerhalb der vom Auftragnehmer kontrollierten Systemumgebung betrieben.

(2) Der Auftragnehmer verwendet personenbezogene Kundendaten nicht für Werbung, Profilbildung, eigene Analysen mit Personenbezug oder für das Training allgemeiner oder externer KI-Modelle.

(3) Eine Nutzung von Kundendaten zur Verbesserung der Erkennung von Belegtypen, der Klassifizierung oder von OCR-/KI-Funktionen erfolgt nur auf Grundlage einer ausdrücklichen, gesondert dokumentierten und jederzeit widerruflichen Weisung des Auftraggebers.

(4) Externe OCR-, KI- oder Analyseanbieter dürfen nur eingesetzt werden, wenn sie als Unterauftragnehmer nach § 6 genehmigt sind.

## **§ 10 Rechte betroffener Personen und Unterstützungspflichten**

---

(1) Wendet sich eine betroffene Person unmittelbar an den Auftragnehmer, leitet dieser die Anfrage unverzüglich an den Auftraggeber weiter, sofern eine Zuordnung möglich ist. Der Auftragnehmer beantwortet Betroffenenanfragen nicht eigenständig, es sei denn, der Auftraggeber weist ihn hierzu an oder eine gesetzliche Pflicht besteht.

(2) Der Auftragnehmer unterstützt den Auftraggeber angemessen bei der Erfüllung von Betroffenenrechten, bei Datenschutz-Folgenabschätzungen und vorheriger Konsultation, bei der Zusammenarbeit mit der Aufsichtsbehörde nach Art. 31 DSGVO, beim Nachweis der Einhaltung von Art. 28 DSGVO sowie bei Rückgabe und Löschung von Daten.

(3) Soweit die Unterstützung über die vertraglich geschuldete Standardleistung hinausgeht, können Aufwand und Vergütung gesondert vereinbart werden, soweit gesetzlich zulässig.

## **§ 11 Datenschutzverletzungen**

---

(1) Der Auftragnehmer informiert den Auftraggeber unverzüglich, sobald ihm eine Verletzung des Schutzes personenbezogener Daten oder ein begründeter Verdacht hierauf bekannt wird.

(2) Die Information erfolgt in der Regel innerhalb von 24 Stunden nach Kenntnisnahme. Stehen einer vollständigen Meldung innerhalb dieser Frist außergewöhnliche Umstände entgegen, erfolgt zunächst eine vorläufige Meldung; fehlende Informationen werden unverzüglich nachgereicht.

(3) Die Meldung enthält, soweit verfügbar, Art des Vorfalls, betroffene Systeme und Datenarten, betroffene Personengruppen, geschätzten Umfang, wahrscheinliche Folgen, ergriffene und empfohlene Maßnahmen sowie einen Ansprechpartner.

(4) Der Auftragnehmer unterstützt den Auftraggeber bei der Erfüllung der Pflichten nach Art. 33 und 34 DSGVO und dokumentiert Sicherheitsvorfälle und getroffene Maßnahmen. Meldungen an Aufsichtsbehörden oder betroffene Personen erfolgen durch den Auftraggeber, sofern der Auftragnehmer nicht gesetzlich verpflichtet ist oder ausdrücklich angewiesen wird.

## **§ 12 Nachweise, Kontrollen und Audits**

---

(1) Der Auftragnehmer stellt dem Auftraggeber auf Anfrage alle erforderlichen Informationen zum Nachweis der Einhaltung dieses Vertrags zur Verfügung. Der Nachweis kann insbesondere durch TOM-Dokumentation, Selbstauskünfte, Sicherheitskonzepte, Auditberichte, Zertifikate, Unterauftragnehmerinformationen sowie Lösch- und Backupkonzepte erfolgen.

(2) Der Auftraggeber ist berechtigt, die Einhaltung der datenschutzrechtlichen Vorgaben selbst oder durch einen geeigneten unabhängigen Prüfer zu kontrollieren. Der eingesetzte Prüfer darf kein Wettbewerber des Auftragnehmers sein und ist vor Beginn der Prüfung zur Vertraulichkeit zu verpflichten.

(3) Vor-Ort-Kontrollen sind rechtzeitig anzukündigen und so durchzuführen, dass Betriebsabläufe sowie Sicherheits- und Geheimhaltungsinteressen des Auftragnehmers nicht unangemessen beeinträchtigt werden. Bei konkretem Verdacht auf schwerwiegende Verstöße oder Sicherheitsvorfälle sind Kontrollen auch kurzfristig zulässig.

(4) Der Auftraggeber trägt die ihm durch eine Kontrolle entstehenden eigenen Kosten selbst. Für den über eine angemessene Mitwirkung hinausgehenden Aufwand des Auftragnehmers, insbesondere bei mehr als einer Vor-Ort-Kontrolle je Kalenderjahr, kann der Auftragnehmer eine angemessene Vergütung verlangen, soweit gesetzlich zulässig.

## **§ 13 Rückgabe und Löschung**

---

(1) Während der Vertragslaufzeit löscht, berichtigt, sperrt oder exportiert der Auftragnehmer personenbezogene Daten nur nach Weisung des Auftraggebers oder soweit dies vertraglich vorgesehen ist.

(2) Nach Beendigung des Hauptvertrags löscht der Auftragnehmer diese Daten unwiederbringlich. Die Dateien sind während der Vertragslaufzeit zum Download bereitgestellt. Produktivdaten werden spätestens innerhalb von 30 Tagen nach Vertragsende gelöscht, sofern keine andere Weisung oder gesetzliche Pflicht besteht.

(3) Backups werden nach Ablauf des regulären Backup-Lebenszyklus überschrieben oder gelöscht, spätestens innerhalb von 10 Tagen nach Vertragsende, sofern keine gesetzliche Aufbewahrungspflicht entgegensteht.

(4) Der Auftragnehmer bestätigt die Löschung auf Anfrage in Textform. Dokumentationen, die dem Nachweis ordnungsgemäßer Verarbeitung dienen, dürfen im erforderlichen Umfang über das Vertragsende hinaus aufbewahrt werden. Ein Zurückbehaltungsrecht an personenbezogenen Daten des Auftraggebers ist ausgeschlossen, soweit gesetzlich zulässig.

## **§ 14 Pflichten des Auftraggebers und Freistellung**

---

(1) Der Auftraggeber ist insbesondere verantwortlich für die Rechtmäßigkeit der Verarbeitung, die Zulässigkeit der Datenübermittlung, die Erfüllung von Informationspflichten, die Vergabe und Verwaltung von Nutzerrechten sowie die Prüfung besonderer Datenkategorien und Berufsgeheimnisse. Er stellt sicher, dass nur erforderliche Daten in die Belegebox eingestellt werden und dass die Zugänge seiner Nutzer geschützt und nicht unbefugt weitergegeben werden.

(2) Verstößt der Auftraggeber gegen die ihm obliegenden Pflichten, insbesondere indem er rechtswidrig personenbezogene Daten in die Belegebox einstellt oder rechtswidrige Weisungen erteilt, stellt er den Auftragnehmer von Ansprüchen Dritter und betroffener Personen frei, die hierauf beruhen. Dies umfasst auch gegen den Auftragnehmer verhängte Bußgelder, soweit diese auf dem Pflichtverstoß des Auftraggebers beruhen. Die Freistellung gilt nicht, soweit der Auftragnehmer den Verstoß zu vertreten hat oder unter Verstoß gegen rechtmäßige Weisungen oder seine speziellen Pflichten als Auftragsverarbeiter gehandelt hat.

## **§ 15 Haftung, Vertragsrangfolge und Schlussbestimmungen**

(1) Für die Haftung gelten die gesetzlichen Regelungen, insbesondere Art. 82 DSGVO, sowie die Regelungen des Hauptvertrags, soweit diese zwingenden datenschutzrechtlichen Vorschriften nicht widersprechen.

(2) Bei Widersprüchen zwischen diesem Vertrag und dem Hauptvertrag gehen die Regelungen dieses Vertrags in datenschutzrechtlichen Fragen vor. Kommerzielle, leistungs- und haftungsbezogene Regelungen des Hauptvertrags bleiben unberührt, soweit sie diesem Vertrag nicht widersprechen.

(3) Änderungen und Ergänzungen dieses Vertrags bedürfen der Textform. Der elektronische Abschluss dieses Vertrags ist zulässig; eine elektronische Annahme tritt an die Stelle einer handschriftlichen Unterschrift. Die Anlagen sind Bestandteil dieses Vertrags.

(4) Es gilt deutsches Recht. Gerichtsstand ist, soweit gesetzlich zulässig, der Sitz des Auftragnehmers.

(5) Sollten einzelne Bestimmungen dieses Vertrags unwirksam sein oder werden, bleibt die Wirksamkeit der übrigen Bestimmungen unberührt. Die Parteien werden eine unwirksame Bestimmung durch eine wirksame Regelung ersetzen, die dem wirtschaftlichen und datenschutzrechtlichen Zweck möglichst nahekommt.

## **Unterschriften**

Soweit dieser Vertrag nicht elektronisch abgeschlossen wird, erfolgt die Unterzeichnung wie folgt:

**Auftraggeber**

**Auftragnehmer: Docunout GmbH**

Ort, Datum: \_\_\_\_\_

Ort, Datum: Nürnberg, 01.10.2026

Name/Funktion: \_\_\_\_\_

Name/Funktion: Matthias Meyer Geschäftsführer

Unterschrift: \_\_\_\_\_

Unterschrift: \_\_\_\_\_

Docunout GmbH  
Schwabacher Str. 1  
90439 Nürnberg  
Tel: +49 911 9264 400  
Mail: [info@belegebox.de](mailto:info@belegebox.de)  
Web: [www.belegebox.de](http://www.belegebox.de)



## **Anlage 1 – Beschreibung der Verarbeitung**

---

### **1. Gegenstand der Verarbeitung**

Bereitstellung, Betrieb, Wartung, Support und Weiterentwicklung der Belegebox als Cloud-/SaaS-Lösung für digitales Dokumenten-, Beleg-, Rechnungs-, E-Rechnungs-, Archivierungs- und Freigabemanagement.

### **2. Zweck der Verarbeitung**

- digitale Beleg- und Dokumentenverwaltung
- Rechnungs-, E-Rechnungs- und Belegprüfung
- Freigabe-, Kontroll- und Wiedervorlageprozesse
- GoBD-orientierte Archivierung
- Kommunikation und Kommentierung zu Dokumenten
- Suche, OCR-Volltext und Wiederauffindbarkeit
- Nutzer-, Rollen- und Rechteverwaltung
- Schnittstellen zu Buchhaltungs-, Steuerberater- und Drittsystemen auf Weisung des Auftraggebers
- technischer Betrieb, Wartung, Support, Fehlerbehebung, Backup und Wiederherstellung

### **3. Art der Verarbeitung**

Erheben, Erfassen, Speichern, Ordnen, Strukturieren, Anzeigen, Abfragen, Verwenden, Übermitteln auf Weisung, Bereitstellen, Einschränken, Löschen, Vernichten und Protokollieren.

### **4. Datenarten und betroffene Personen**

Es gelten die in § 2 dieses Vertrags genannten Kategorien personenbezogener Daten und betroffener Personen.

## Anlage 2 – Technische und organisatorische Maßnahmen TOM

---

Die folgenden Maßnahmen bilden das vereinbarte Mindestschutzniveau. Der Auftragnehmer hält sie während der Vertragslaufzeit aufrecht und passt sie dem Stand der Technik sowie dem Risiko der Verarbeitung angemessen an.

Die gesamte Server- und Backup-Infrastruktur ist in den Rechenzentren von Hetzner in Nürnberg, Falkenstein und Finnland verankert. Für die Sicherheit der Strukturen hat Hetzner eine ausführliche Aufstellung der technischen und organisatorischen Maßnahmen auf Ihrer Homepage unter <https://www.hetzner.com/AV/TOM.pdf>

### 1. Zutritts-, Zugangs- und Zugriffskontrolle

- gesicherte Büro-, Betriebs- und Serverstandorte
- personenbezogene Benutzerkonten und rollenbasierte Berechtigungskonzepte
- Multifaktor-Authentifizierung für administrative Zugänge
- Need-to-know-Prinzip und regelmäßige Prüfung administrativer Berechtigungen
- Mandanten- bzw. Kundentrennung

### 2. Weitergabe-, Eingabe- und Auftragskontrolle

- Transportverschlüsselung (TLS/HTTPS) bei Übertragung über öffentliche Netze
- kontrollierte Schnittstellen, Exporte und Downloads
- Protokollierung sicherheitsrelevanter Nutzer- und Administrationsvorgänge
- Unterauftragnehmermanagement und Vertraulichkeitsverpflichtungen

### 3. Verfügbarkeit, Belastbarkeit und Wiederherstellung

- Backup- und Wiederherstellungsprozesse mit regelmäßiger Prüfung der Wiederherstellbarkeit
- Systemmonitoring, Patch- und Schwachstellenmanagement
- Schutz vor Schadsoftware, Firewall- und Netzwerkschutz
- Incident-Response-Prozess für Sicherheitsvorfälle

### 4. Trennung, Verschlüsselung und Organisation

- Trennung von Produktiv-, Test- und Entwicklungsumgebungen
- Verschlüsselte Backups
- Pseudonymisierung oder Anonymisierung bei Tests, Analysen und Fehlerbehebungen, soweit möglich
- benannte Verantwortlichkeiten für Datenschutz und Informationssicherheit
- regelmäßige Sensibilisierung zu Datenschutz und Informationssicherheit

## Anlage 3 – Unterauftragnehmer

Der Auftragnehmer führt eine aktuelle Unterauftragnehmerliste mit mindestens folgenden Angaben: Name und Anschrift, Sitzland, Leistung/Zweck, betroffene Datenkategorien, Verarbeitungsort und etwaiger Drittlandbezug.

Die jeweils aktuelle Liste wird dem Auftraggeber in Textform, über eine vom Auftragnehmer bereitgestellte Informationsseite oder auf Anfrage zur Verfügung gestellt. Änderungen werden gemäß § 6 mitgeteilt. Externe OCR-, KI- oder Analyseanbieter werden nur eingesetzt, wenn sie als Unterauftragnehmer genehmigt sind.

Bei Vertragsschluss sind folgende Unterauftragnehmer benannt:

| Unterauftragnehmer          | Leistung / Zweck                                                                                                                                                                                          | Sitz /<br>Verarbeitungs<br>ort          | Datenkategorien                                                        | Drittlandtransfer         |
|-----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------|------------------------------------------------------------------------|---------------------------|
| Page one GmbH               | IT-Leistungen, Betrieb, Wartung, Support, technische Betreuung                                                                                                                                            | Schwabacher Str. 3<br>90439<br>Nürnberg | technische Daten, Protokolldaten, im Supportfall ggf. Inhaltsdaten     | kein<br>Drittlandtransfer |
| Hezner.com                  | Hosting, Serverbetrieb, Netzwerk, Infrastruktur, Backup                                                                                                                                                   | Nürnberg, Falkenstein, Finnland         | Produktivdaten, Metadaten, technische Daten, Backups                   | kein<br>Drittlandtransfer |
| IONOS                       | System-E-Mails, Einladungen, Benachrichtigungen                                                                                                                                                           | Montabaur                               | E-Mail-Adressen, technische Versanddaten                               | kein<br>Drittlandtransfer |
| GitLab                      | Entwickler-Pipeline, CI/CD-Pipelines, Projektmanagement (Issues)                                                                                                                                          | Page one<br>internes<br>Rechenzentrum   | Keine Kundendaten! Entwickler-Metadaten (2FA Pflicht, Secret-Scanning) | kein<br>Drittlandtransfer |
| bunny.net                   | Content Delivery Network (CDN), Asset-Caching, Dateiverteilung, Auslastungsoptimierung. Physische PoPs gesteuert über Routing-Filter (EU). IP-Anonymisierung, SSL/TLS-Erzwingung, dediziertes EU-Routing. | Slowenien (EU)                          | Rein statische Inhalte wie Logos, Icons, Textbausteine o.ä.            | kein<br>Drittlandtransfer |
| <b>Selbstbetriebe Tools</b> |                                                                                                                                                                                                           |                                         |                                                                        |                           |
| Grafana                     | Systemsüberwachung, Fehleranalyse                                                                                                                                                                         | Hetzner                                 | technische Daten, Protokolldaten                                       | kein<br>Drittlandtransfer |
| Wazuh                       | s. unten                                                                                                                                                                                                  | Page one<br>internes<br>Rechenzentrum   | Sicherheits-Check                                                      | kein<br>Drittlandtransfer |

Wazuh als wichtiger Bestandteil der permanenten Überwachung der Sicherheitsstandards.

| Wazuh-Komponente / Funktion                    | Technischer Einsatzzweck & Nachweis                                                                                                                                            | Zugeordnetes Schutzziel (TOM)                                            |
|------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------|
| <b>Log Data Collection &amp; Analysis</b>      | Zentralisierte, revisionssichere Erfassung und automatische Analyse von System- und Anmelde-Logs (z. B. Windows Event Logs, Linux Syslog). Erkennung von unbefugten Zugriffen. | Vertraulichkeit<br>(Zugangs- & Zugriffskontrolle)                        |
| <b>File Integrity Monitoring (FIM)</b>         | Echtzeit-Überwachung von Systemdateien, Anwendungsdaten und Verzeichnissen auf Modifikation, Löschung oder Neuerstellung (inkl. Details zu Wer, Was, Wann).                    | Integrität<br>(Eingabe- & Weitergabekontrolle)                           |
| <b>Security Configuration Assessment (SCA)</b> | Kontinuierliche, automatisierte Überprüfung der Betriebssystem- und Anwendungskonfigurationen gegen etablierte Sicherheitsstandards (z. B. CIS-Benchmarks).                    | Verfahren zur regelmäßigen Überprüfung<br><br>(Sicherheitsmanagement)    |
| <b>Vulnerability Detection</b>                 | Täglicher, automatischer Scan der installierten Softwarekomponenten auf bekannten Schwachstellen durch Abgleich mit nationalen CVE-Datenbanken.                                | Verfahren zur regelmäßigen Überprüfung<br><br>(Schwachstellenmanagement) |
| <b>Active Response</b>                         | Automatische, skriptbasierte Abwehrmaßnahmen in Echtzeit (z. B. IP-Blockierung bei Brute-Force-Angriffen oder Stoppen von Prozessen bei Ransomware-Verhalten).                 | Verfügbarkeit & Belastbarkeit<br><br>(Bedrohungsabwehr)                  |
| <b>Malware &amp; Ransomware Detection</b>      | Verhaltensbasierte Erkennung von Schadsoftware, Anomalien und typischen Verschlüsselungsmustern auf Endpunkten.                                                                | Verfügbarkeit & Belastbarkeit<br><br>(Systemschutz)                      |
| <b>Dashboard RBAC &amp; Multi-Tenancy</b>      | Rollenbasierte Zugriffskontrolle auf die gesammelten Logdaten und logische Trennung von Systemumgebungen über Agent-Gruppen.                                                   | Vertraulichkeit<br>(Trennungskontrolle)                                  |
| <b>Sichere Agent-Kommunikation</b>             | Lückenlose, starke AES-Verschlüsselung aller Datenströme und Log-Übertragungen zwischen den überwachten Endpunkten und dem zentralen Wazuh-Server.                             |                                                                          |

## Anlage 4 – Rückgabe- und Löschkonzept

---

Während der Vertragslaufzeit kann der Auftraggeber Daten im Rahmen der Produktfunktionen exportieren oder löschen. Der Auftragnehmer unterstützt den Auftraggeber auf Weisung bei Export, Löschung oder Einschränkung der Verarbeitung.

Nach Vertragsende erhält der Auftraggeber die Möglichkeit zum Datenexport. Produktivdaten werden innerhalb von 30 Tagen gelöscht oder zurückgegeben. Backups werden innerhalb des regulären Backup-Zyklus, spätestens nach 10 Tagen, überschrieben oder gelöscht. Supportkopien, temporäre Exporte und Analysedaten werden nach Zweckerreichung gelöscht. Die Löschung wird auf Wunsch in Textform bestätigt.

Eine längere Speicherung ist nur zulässig, soweit gesetzliche Aufbewahrungspflichten bestehen, die Speicherung zur Rechtsverteidigung erforderlich ist, der Auftraggeber eine Aufbewahrung angewiesen hat oder technische Backup-Zyklen noch nicht abgelaufen sind.

*Stand: 01.10.2026*