VERSION 3.5 · NOVEMBER 2026

Auftragsverarbeitungsvertrag gemäß Art. 28 DSGVO

zwischen dem Kunden („**Verantwortlicher**“) und der BitHive UG (haftungsbeschränkt), Heisenbergstraße 3, 10587 Berlin („**Auftragsverarbeiter**“), für den BitHive Reporting Desk („**Dienst**“).

Version 3.5 · November 2026 · Ersetzt Version 3.4. Änderungen: Jira Cloud als Ziel (§ 1 Abs. 6, Anlage 1), Tests der Wiederherstellung (Anlage 2).

§ 1 Gegenstand, Dauer und Spezifizierung der Verarbeitung

(1) Der Auftragsverarbeiter verarbeitet personenbezogene Daten im Auftrag des Verantwortlichen, um den Dienst nach den Allgemeinen Geschäftsbedingungen („**Hauptvertrag**“) zu erbringen. Dieser Vertrag gilt für alle derartigen Verarbeitungen.

(2) Die Laufzeit dieses Vertrags entspricht der Laufzeit des Hauptvertrags. Pflichten, die ihrer Natur nach darüber hinaus fortbestehen (insbesondere §§ 8 und 9), bleiben wirksam.

(3) Art und Zweck der Verarbeitung, die Arten personenbezogener Daten und die Kategorien betroffener Personen ergeben sich aus Anlage 1.

(4) **Ort der Verarbeitung.** Der Dienst wird ausschließlich in Rechenzentren in Deutschland durch einen in Deutschland ansässigen Hosting-Anbieter betrieben. Alle im Dienst gespeicherten Daten, insbesondere SBOMs, Schwachstellenfälle, Meldungstexte und das Protokoll, verbleiben in Deutschland. E-Mails an die Support-Adresse des Auftragsverarbeiters werden in einem in Deutschland gehosteten Postfach des hierfür in Anlage 3 genannten Unterauftragsverarbeiters verarbeitet. E-Mails des Dienstes (Anmeldelinks und Benachrichtigungen) werden über den in Anlage 3 genannten E-Mail-Unterauftragsverarbeiter zugestellt, ein in Frankreich ansässiges Unternehmen, das sie in Rechenzentren in der Europäischen Union verarbeitet, ohne Verarbeitung in Drittländern. Jede Übermittlung personenbezogener Daten in ein Drittland bedarf der vorherigen Zustimmung des Verantwortlichen in Textform und erfolgt nur nach Maßgabe der Art. 44 bis 49 DSGVO.

(5) **Protokoll und Aufbewahrung.** Der Dienst führt ein unveränderbares Protokoll der Aktionen im Dienst als Nachweis darüber, wie der Verantwortliche seine Meldepflichten wahrnimmt. Einträge nennen die handelnde Person, können von Nutzern des Dienstes einzeln weder geändert noch gelöscht werden und behalten den Namen einer Person auch, nachdem sie als Nutzer entfernt wurde. Der Verantwortliche wählt im Dienst die Aufbewahrungsdauer für Protokolleinträge und Meldungsunterlagen (24 Monate oder 10 Jahre); nach deren Ablauf löscht der Auftragsverarbeiter die betroffenen Einträge. Die Wahl der Aufbewahrungsdauer ist eine Weisung des Verantwortlichen im Sinne von § 2 Abs. 1. Die Entfernung eines Moduls oder die Verkleinerung eines Tarifs verkürzt die Aufbewahrungsdauer nicht und löscht keine Einträge; dies bewirkt nur eine vom Verantwortlichen gewählte kürzere Aufbewahrungsdauer nach Maßgabe von § 7 Abs. 6 lit. c des Hauptvertrags. Entscheidet der Verantwortliche, dass ein Eintrag gelöscht oder pseudonymisiert werden muss, etwa auf Antrag einer betroffenen Person, führt der Auftragsverarbeiter dies auf Weisung des Verantwortlichen in Textform aus. Löscht der Inhaber des Verantwortlichen das Konto (§ 8 Abs. 6 des Hauptvertrags), wird das Protokoll mit dem Konto gelöscht; der zuvor angebotene Export enthält es. Nach Ende des Hauptvertrags gilt § 7.

(6) **Alarmkanäle und Jira.** Richtet der Verantwortliche im Dienst Alarmkanäle ein, etwa Slack, Microsoft Teams oder eine Webhook-Adresse, oder verbindet er seine eigene Jira-Cloud-Instanz, übermittelt der Auftragsverarbeiter Alarmnachrichten und, bei Jira, Vorgänge und Kommentare zu den Fällen des Verantwortlichen auf dessen Weisung an die von ihm angegebenen Ziele. Die Anbieter dieser Ziele (bei Jira: Atlassian) wählt der Verantwortliche; sie sind keine Unterauftragsverarbeiter des Auftragsverarbeiters. Für das Verhältnis zu ihnen, einschließlich einer etwaigen Übermittlung in ein Drittland, ist der Verantwortliche verantwortlich. Alarmnachrichten, Vorgänge und Kommentare enthalten die zum Handeln erforderlichen Angaben, etwa Produkt, Schwachstelle, Frist und einen Link zum Fall. Für die Verbindung mit Jira speichert der Auftragsverarbeiter den von Atlassian erteilten Zugriff verschlüsselt, nutzt ihn nur für diese Vorgänge und Kommentare und für das, was dazu nötig ist, und löscht ihn, sobald der Verantwortliche Jira trennt oder das Konto gelöscht wird.

(7) **Nutzung als Auftragsverarbeiter.** Verarbeitet der Verantwortliche selbst personenbezogene Daten im Auftrag eigener Kunden und erfasst er solche Daten im Dienst (insbesondere im Auftragsverarbeiter-Modus des DSGVO-Moduls), handelt der Auftragsverarbeiter als weiterer Auftragsverarbeiter (Unterauftragsverarbeiter) des Verantwortlichen im Sinne von Art. 28 Abs. 4 DSGVO; dieser Vertrag gilt als der danach erforderliche Vertrag. Der Verantwortliche sichert zu, nach seinen eigenen Verträgen zur Einschaltung des Auftragsverarbeiters und seiner Unterauftragsverarbeiter (Anlage 3) berechtigt zu sein, und informiert seine Kunden, soweit erforderlich. Weisungen erteilt allein der Verantwortliche.

§ 2 Weisungen

(1) Der Auftragsverarbeiter verarbeitet personenbezogene Daten nur auf dokumentierte Weisung des Verantwortlichen, sofern er nicht durch das Recht der Union oder der Mitgliedstaaten hierzu verpflichtet ist; in einem solchen Fall teilt er dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht verbietet. Der Hauptvertrag, dieser Vertrag und die Nutzung der Funktionen des Dienstes durch den Verantwortlichen stellen die Weisungen des Verantwortlichen dar.

(2) Weitere Weisungen erfolgen in Textform. Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich, wenn er der Auffassung ist, dass eine Weisung gegen Datenschutzvorschriften verstößt. Er darf die Ausführung der Weisung aussetzen, bis der Verantwortliche sie bestätigt oder ändert.

§ 3 Pflichten des Auftragsverarbeiters

(1) Der Auftragsverarbeiter gewährleistet, dass sich die zur Verarbeitung befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

(2) Der Auftragsverarbeiter ergreift alle gemäß Art. 32 DSGVO erforderlichen Maßnahmen. Die technischen und organisatorischen Maßnahmen sind in Anlage 2 beschrieben. Der Auftragsverarbeiter darf sie an den technischen Fortschritt anpassen, sofern das Schutzniveau nicht unterschritten wird.

(3) Der Auftragsverarbeiter unterstützt den Verantwortlichen angesichts der Art der Verarbeitung mit geeigneten technischen und organisatorischen Maßnahmen bei der Erfüllung seiner Pflicht zur Beantwortung von Anträgen betroffener Personen (Art. 12 bis 23 DSGVO). Wendet sich eine betroffene Person unmittelbar an den Auftragsverarbeiter, leitet er das Anliegen unverzüglich an den Verantwortlichen weiter.

(4) Der Auftragsverarbeiter unterstützt den Verantwortlichen unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen bei der Einhaltung der Pflichten aus Art. 32 bis 36 DSGVO.

(5) Der Auftragsverarbeiter meldet dem Verantwortlichen eine Verletzung des Schutzes personenbezogener Daten, die Daten des Verantwortlichen betrifft, unverzüglich, spätestens jedoch innerhalb von 24 Stunden, nachdem sie ihm bekannt geworden ist. Die Meldung erfolgt per E-Mail an den Inhaber und alle Administratoren des Kontos des Verantwortlichen. Sie enthält, soweit verfügbar, die in Art. 33 Abs. 3 DSGVO genannten Informationen; noch nicht verfügbare Informationen werden unverzüglich nachgereicht, sobald sie vorliegen.

(6) Verlangt eine Behörde eines Drittlands die Herausgabe personenbezogener Daten des Verantwortlichen, informiert der Auftragsverarbeiter den Verantwortlichen unverzüglich, sofern dies nicht gesetzlich untersagt ist, geht gegen das Verlangen vor, soweit hierfür vertretbare Gründe bestehen, und gibt nur das unbedingt Erforderliche heraus. Entsprechende Verlangen, die einen Unterauftragsverarbeiter erreichen, leitet der Auftragsverarbeiter weiter.

(7) Ansprechpartner für den Datenschutz beim Auftragsverarbeiter: contact@bithive-it.com. Der Auftragsverarbeiter ist zur Benennung eines Datenschutzbeauftragten nicht verpflichtet, solange die gesetzlichen Voraussetzungen hierfür nicht vorliegen.

§ 4 Unterauftragsverarbeiter

(1) Der Verantwortliche erteilt die allgemeine Genehmigung zum Einsatz der in Anlage 3 aufgeführten Unterauftragsverarbeiter.

(2) Der Auftragsverarbeiter informiert den Verantwortlichen mindestens vier Wochen vorher oder, wenn ein Unterauftragsverarbeiter dem Auftragsverarbeiter eine kürzere Frist setzt, unverzüglich nach deren Eingang in Textform über jede beabsichtigte Hinzuziehung oder Ersetzung eines Unterauftragsverarbeiters. Der Verantwortliche kann der Änderung innerhalb dieser Frist aus wichtigem datenschutzrechtlichem Grund widersprechen. Sieht der Auftragsverarbeiter von der Änderung nicht ab, kann der Verantwortliche den Hauptvertrag zum Zeitpunkt der Änderung kündigen.

(3) Der Auftragsverarbeiter erlegt jedem Unterauftragsverarbeiter vertraglich dieselben Datenschutzpflichten auf, die in diesem Vertrag festgelegt sind, insbesondere hinreichende Garantien für geeignete technische und organisatorische Maßnahmen, und stellt sicher, dass Standardvertragsklauseln bestehen, soweit ein Unterauftragsverarbeiter oder einer von dessen Unterauftragsverarbeitern Daten in einem oder aus einem Drittland verarbeitet. Der Auftragsverarbeiter haftet gegenüber dem Verantwortlichen für die Einhaltung der Pflichten des Unterauftragsverarbeiters.

(4) Nebenleistungen, die der Auftragsverarbeiter in Anspruch nimmt, etwa Telekommunikations- oder Postdienstleistungen, sind keine Unterauftragsverarbeitung im Sinne dieses Paragrafen.

§ 5 Rechte und Pflichten des Verantwortlichen

(1) Der Verantwortliche ist für die Rechtmäßigkeit der Verarbeitung, einschließlich der Rechtmäßigkeit der Übermittlung personenbezogener Daten an den Auftragsverarbeiter, sowie für die Wahrung der Rechte der betroffenen Personen verantwortlich.

(2) Der Verantwortliche informiert den Auftragsverarbeiter unverzüglich, wenn er Fehler oder Unregelmäßigkeiten in den Verarbeitungsergebnissen feststellt.

§ 6 Kontrollen

(1) Der Auftragsverarbeiter stellt dem Verantwortlichen alle erforderlichen Informationen zum Nachweis der Einhaltung der Pflichten aus Art. 28 DSGVO zur Verfügung, insbesondere diesen Vertrag, die Beschreibung der technischen und organisatorischen Maßnahmen sowie, soweit vorhanden, Zertifikate oder Prüfberichte, einschließlich derjenigen seiner Unterauftragsverarbeiter.

(2) Der Verantwortliche oder ein von ihm beauftragter, zur Verschwiegenheit verpflichteter Prüfer kann Kontrollen durchführen, in der Regel nach einer Ankündigung von mindestens vier Wochen, während der üblichen Geschäftszeiten, ohne Störung des Betriebsablaufs und höchstens einmal pro Kalenderjahr, sofern keine konkreten Anhaltspunkte für einen Verstoß vorliegen. Kontrollen bei Unterauftragsverarbeitern erfolgen anhand von deren Zertifikaten und Prüfberichten.

(3) Für den Aufwand bei der Unterstützung von Kontrollen, die über Abs. 1 hinausgehen, kann der Auftragsverarbeiter eine angemessene Vergütung verlangen, es sei denn, die Kontrolle ergibt einen Verstoß des Auftragsverarbeiters.

§ 7 Löschung und Rückgabe

(1) Nach Abschluss der Erbringung der Leistungen wählt der Verantwortliche zwischen der Rückgabe der personenbezogenen Daten durch Export, der 30 Tage nach Ende des Hauptvertrags möglich ist (§ 8 Abs. 5 des Hauptvertrags), und ihrer früheren Löschung auf Weisung in Textform. Nach Ablauf dieser Frist oder auf diese Weisung löscht der Auftragsverarbeiter alle im Auftrag verarbeiteten personenbezogenen Daten, sofern nicht nach dem Recht der Union oder der Mitgliedstaaten eine Pflicht zur Speicherung besteht. Der Auftragsverarbeiter bestätigt die Löschung auf Verlangen in Textform.

(2) Sicherungskopien werden im regulären Sicherungszyklus überschrieben, spätestens 35 Tage nach der Löschung im Produktivsystem.

(3) Löscht der Inhaber des Verantwortlichen das Konto (§ 8 Abs. 6 des Hauptvertrags), wird die Löschung 14 Tage nach ihrer Bestätigung wirksam; bis dahin kann der Verantwortliche seine Daten exportieren oder die Löschung widerrufen. Die bestätigte Löschung ist eine Weisung im Sinne von Abs. 1.

§ 8 Haftung

Die Haftung richtet sich nach Art. 82 DSGVO. Im Innenverhältnis der Parteien gelten die Haftungsregelungen des Hauptvertrags, soweit zwingendes Recht nichts anderes bestimmt.

§ 9 Schlussbestimmungen

(1) Bei Widersprüchen gehen die Regelungen dieses Vertrags zum Datenschutz den Regelungen des Hauptvertrags vor.

(2) Änderungen und Ergänzungen dieses Vertrags bedürfen der Textform.

(3) Es gilt das Recht der Bundesrepublik Deutschland. Der Gerichtsstand richtet sich nach dem Hauptvertrag.

(4) Dieser Vertrag liegt in deutscher und englischer Sprache vor. Maßgeblich ist die Fassung in der Vertragssprache des Hauptvertrags. Vertragssprache ist die des Hauptvertrags (§ 12 Abs. 6 des Hauptvertrags). Fassungen in anderen Sprachen dienen nur der Information.

(5) Hat der Verantwortliche seinen Sitz in einem Drittland, für das kein Angemessenheitsbeschluss besteht, und unterliegt seine Verarbeitung nicht der DSGVO, werden die durch den Durchführungsbeschluss (EU) 2021/914 der Kommission erlassenen Standardvertragsklauseln, Modul 4 (Übermittlung vom Auftragsverarbeiter an den Verantwortlichen), in diesen Vertrag einbezogen. Dabei ist der Auftragsverarbeiter Datenexporteur und der Verantwortliche Datenimporteur; die fakultative Klausel 7 findet keine Anwendung; für Klausel 17 wählen die Parteien das Recht der Bundesrepublik Deutschland und für Klausel 18 die Gerichte in Berlin; die nach den Anhängen der Klauseln erforderlichen Angaben ergeben sich aus den Anlagen 1 bis 3 dieses Vertrags. Bei Widersprüchen gehen die Standardvertragsklauseln vor. Für Verantwortliche, die der UK GDPR unterliegen, beziehen sich Verweise auf die DSGVO auch auf die entsprechenden Bestimmungen der UK GDPR.

Anlage 1: Spezifizierung der Verarbeitung

Punkt	Beschreibung
Art und Zweck	Hosting und Betrieb des Dienstes: Nutzerverwaltung, Einladungen und Anmeldung, Speicherung und Auswertung von SBOMs, Abgleich mit Schwachstelleninformationen, Versand von Benachrichtigungen, Fristenverfolgung, Vorbereitung von Meldungstexten, Protokoll, Support. Fallbearbeitung für Vorfälle, Verletzungen des Schutzes personenbezogener Daten und vertragliche Mitteilungen (vom Verantwortlichen gebuchte Module): Erfassung von Ereignissen, Fristberechnung, Entwürfe, Alarme und Nachweisunterlagen. Soweit der Verantwortliche seine Jira-Cloud-Instanz verbindet: Anlegen von Vorgängen und Kommentaren zu seinen Fällen in dieser Instanz.
Arten personenbezogener Daten	Nutzerstammdaten (Name, geschäftliche E-Mail-Adresse, Rolle, Team); Einladungen (E-Mail-Adresse, Name und Rolle der eingeladenen Person, Status und Ablaufdatum); Authentifizierungsdaten (Anmeldelinks, gehashte API-Tokens); Nutzungs- und Protokolldaten (Zeitstempel, IP-Adressen, Aktionen im Dienst); von Nutzern eingegebene Inhalte (Kommentare, Meldungstexte, die Namen von Ansprechpartnern enthalten können); Kontaktdaten von Empfängern von Benachrichtigungen; soweit der Verantwortliche eine Funktion zur Entgegennahme von Schwachstellenmeldungen nutzt: Name und Kontaktdaten meldender Personen sowie der Inhalt ihrer Meldungen; Beschreibungen von Vorfällen und Datenschutzverletzungen, die die Kategorien und die ungefähre Zahl der betroffenen Personen und Datensätze sowie in Ausnahmefällen begrenzte identifizierende Angaben enthalten können, die der Verantwortliche zur Dokumentation für erforderlich hält (Art. 33 Abs. 5 DSGVO); Namen und geschäftliche Kontaktdaten von Ansprechpartnern bei Behörden, Verantwortlichen, Auftragsverarbeitern und sonstigen Empfängern von Meldungen und Mitteilungen; soweit der Verantwortliche seine Jira-Cloud-Instanz verbindet: der von Atlassian erteilte Zugriff (OAuth-Token, verschlüsselt gespeichert), der die Atlassian-Konto-ID des Nutzers enthält, der die Verbindung hergestellt hat.
Kategorien betroffener Personen	Mitarbeiter und Beauftragte des Verantwortlichen, die den Dienst nutzen, dazu eingeladen werden oder Benachrichtigungen erhalten; in Meldungen genannte Ansprechpartner; Personen, die dem Verantwortlichen über den Dienst Schwachstellen melden; von einem vom Verantwortlichen erfassten Vorfall oder einer Datenschutzverletzung betroffene Personen (als Kategorien, siehe

Punkt	Beschreibung
	oben); Ansprechpartner der Kunden und Lieferanten des Verantwortlichen sowie der zuständigen Behörden.
Besondere Kategorien (Art. 9 DSGVO)	Nicht vorgesehen. Der Verantwortliche gibt solche Daten nicht in den Dienst ein. Aufzeichnungen zu Datenschutzverletzungen beschreiben die Kategorien der betroffenen Daten; sie dürfen die besonderen Kategorien personenbezogener Daten selbst nicht enthalten.

Anlage 2: Technische und organisatorische Maßnahmen (Art. 32 DSGVO)

Vertraulichkeit

- **Zutrittskontrolle:** Der Dienst läuft ausschließlich in Rechenzentren in Deutschland des in Anlage 3 genannten Hosting-Anbieters, der eine physische Zutrittskontrolle betreibt und dessen Informationssicherheits-Managementsystem nach ISO/IEC 27001 zertifiziert ist. Der Auftragsverarbeiter betreibt keine eigenen Serverräume. Der Hosting-Anbieter verfügt zudem über ein BSI-C5:2020-Testat (Typ 2) für Cloud-Server, Block- und Objektspeicher.
- **Zugangskontrolle:** Administrativer Zugang nur über persönliche Konten mit Mehrfaktor-Authentifizierung; keine geteilten Konten; Zugangsschlüssel verschlüsselt gespeichert; Prinzip der minimalen Rechte.
- **Zugriffskontrolle:** Strikte Trennung der Kunden (Mandanten): Jeder Datensatz trägt eine Mandantenkennung, und die Datenbank erzwingt die Trennung zusätzlich zur Anwendung durch Row-Level-Security; Nutzer melden sich ohne Passwort über Einmal-Links an; API-Tokens werden nur als kryptografische Hashwerte gespeichert und können eingeschränkt und widerrufen werden.
- **Trennungskontrolle:** Produktiv-, Test- und Entwicklungsumgebungen sind getrennt; keine Kundendaten in Test oder Entwicklung.

Integrität

- **Weitergabekontrolle:** Alle Verbindungen sind mit TLS 1.2 oder höher verschlüsselt; E-Mail-Benachrichtigungen enthalten nur die notwendigen Angaben und verweisen auf den Dienst.
- **Eingabekontrolle:** Unveränderbares Protokoll relevanter Aktionen je Mandant mit Zeitstempel und Nutzer.
- **Software-Integrität:** Jede Änderung wird geprüft und durchläuft vor der Auslieferung automatisierte Tests, statische Analyse und eine Schwachstellenprüfung der Abhängigkeiten.

Verfügbarkeit und Belastbarkeit

- PostgreSQL-Datenbank mit fortlaufender Archivierung und Wiederherstellung zu einem beliebigen Zeitpunkt; Sicherungskopien werden vor dem Verlassen des Servers verschlüsselt und in Objektspeicher in Deutschland mit Schreibschutz gegen Änderung und Löschung abgelegt; Wiederherstellungsverfahren werden mindestens einmal in jedem Kalendermonat getestet; jeder Test wird dokumentiert.
- Verschlüsselung gespeicherter Daten: Das Speichervolume mit Datenbank, Anwendungsdaten und Protokollen ist verschlüsselt; die Systemplatte des Servers enthält keine personenbezogenen Daten; Sicherungskopien sind verschlüsselt.
- Verfügbarkeitsüberwachung mit Alarmierung: Lebenszeichen aller Hintergrundprozesse und eine Prüfung der öffentlichen Adresse mindestens einmal pro Minute. Der Überwachungsdienst erhält keine personenbezogenen Daten des Verantwortlichen. Ein dokumentiertes Verfahren zur Behandlung von Sicherheitsvorfällen besteht.

Verfahren zur regelmäßigen Überprüfung

- Überprüfung der Zugriffsrechte mindestens vierteljährlich; Überprüfung dieser Maßnahmen mindestens jährlich und nach wesentlichen Änderungen.

- Automatisierte Prüfung auf Aktualisierungen: Sicherheitsupdates des Betriebssystems werden automatisch installiert; Abhängigkeiten der Anwendung und Build-Werkzeuge werden mindestens monatlich geprüft.
- Datenschutzfreundliche Voreinstellungen: Es werden nur die für den Dienst erforderlichen Daten erhoben; kein Tracking, keine Werbung, keine Nutzung von Kundendaten für andere Zwecke, insbesondere nicht zum Training von KI-Modellen.

Anlage 3: Genehmigte Unterauftragsverarbeiter

Unterauftragsverarbeiter	Leistung	Ort der Verarbeitung	Garantien bei Drittlandbezug
Hetzner Online GmbH, Industriestr. 25, 91710 Gunzenhausen	Cloud-Hosting: Server, Speichervolumes, Objektspeicher für Backups	Deutschland (Rechenzentren in Nürnberg und Falkenstein)	Entfällt (keine Verarbeitung in Drittländern)
STRATO GmbH, Otto-Ostrowski-Straße 7, 10249 Berlin	Hosting des Support-Postfachs (E-Mails an die Support-Adresse)	Deutschland	Entfällt (keine Verarbeitung in Drittländern)
Scaleway SAS, 8 rue de la Ville l'Evêque, 75008 Paris, Frankreich	Versand transaktionaler E-Mails (Anmeldelinks, Benachrichtigungen)	Europäische Union (Rechenzentren in der Region Paris, Frankreich)	Entfällt (keine Verarbeitung in Drittländern)

Die Angaben entsprechen dem Stand der Auftragsverarbeitungsverträge der Unterauftragsverarbeiter im Oktober 2026.

Als PDF herunterladen·Alle Rechtstexte