BIBERTRON · RECHTLICHES

Vertrag über die Auftragsverarbeitung

nach Art. 28 DSGVO — gilt für alle Kunden des Baubegleiters ab Registrierung

FASSUNG	GILT FÜR
Stand 05.11.2026	**Unternehmer (B2B)**

§ 1 Vertragsparteien

(1) Auftragsverarbeiter im Sinne des Art. 4 Nr. 8 DSGVO ist die Bibertron UG (haftungsbeschränkt), Am Haag 8, 82166 Gräfelfing, vertreten durch die Geschäftsführerin Beata Krenzer, E-Mail hallo@bibertron.de (nachfolgend „Auftragsverarbeiter“).

(2) Verantwortlicher im Sinne des Art. 4 Nr. 7 DSGVO ist der Kunde des Nutzungsvertrages über die Anwendung „Bibertron Baubegleiter“ (nachfolgend „Verantwortlicher“). Er wird durch die in seinem Kundenkonto hinterlegten Angaben zu Firma, Rechtsform, Anschrift und vertretungsberechtigter Person bestimmt. Der Verantwortliche hält diese Angaben aktuell.

(3) Dieser Vertrag gilt für die Verarbeitung personenbezogener Daten in den Projektinhalten, die der Verantwortliche im Rahmen der Anwendung einstellt oder durch Projektbeteiligte einstellen lässt. Für den Betrieb der Anwendung, Nutzerkonten, Registrierungsdaten, Zugriffsprotokolle, Korrespondenz und Abrechnung ist der Auftragsverarbeiter eigener Verantwortlicher; diese Verarbeitungen sind nicht Gegenstand dieses Vertrages, soweit sie nicht zugleich Projektinhalte betreffen.

(4) Dieser Vertrag wird bei Vertragsschluss oder in der Anwendung in Textform geschlossen (Art. 28 Abs. 9 DSGVO). Der Auftragsverarbeiter protokolliert Zeitpunkt, Kundenkonto, handelnde Person und Fassung dieses Vertrages und stellt dem Verantwortlichen die von ihm abgeschlossene Fassung einschließlich seiner Angaben nach Absatz 2 jederzeit als Dokument zum Abruf bereit.

§ 2 Gegenstand und Dauer

(1) Dieser Vertrag regelt die Verarbeitung personenbezogener Daten durch den Auftragsverarbeiter im Auftrag des Verantwortlichen bei der Nutzung der Anwendung „Bibertron Baubegleiter“ zur Baudokumentation und Projektkoordination, soweit diese Daten in den Projektinhalten enthalten sind.

(2) Der Vertrag beginnt mit der Registrierung des Verantwortlichen, sobald dieser personenbezogene Daten in die Anwendung einstellt. Er gilt auch während einer kostenlosen Testphase.

(3) Der Vertrag endet mit der vollständigen Löschung oder Rückgabe der im Auftrag verarbeiteten Daten nach § 11. Er besteht über das Ende des Nutzungsvertrages hinaus fort, solange der Auftragsverarbeiter Daten auf Weisung des Verantwortlichen aufbewahrt.

§ 3 Art und Zweck der Verarbeitung

(1) Zweck der Verarbeitung ist die Verwaltung von Bauprojekten, Terminen, Mängeln, Aufgaben und Dokumenten sowie die Kommunikation zwischen Projektbeteiligten.

(2) Art der Verarbeitung: Erheben, Speichern, Organisieren, Anzeigen, Verändern, Übermitteln an Projektbeteiligte, automatisierte Vorklassifizierung von Mängelfotos, Umwandlung von Sprachaufnahmen in Text, Erzeugen von Protokollen und Exportdateien, Versand von Benachrichtigungen, Löschen.

(3) Die Verarbeitung findet grundsätzlich ausschließlich in einem Mitgliedstaat der Europäischen Union oder in einem Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Verarbeitungen in Drittländern oder Zugriffe aus Drittländern, einschließlich durch weitere Auftragsverarbeiter, sind nur zulässig, wenn sie in § 9 und Anlage 2 konkret ausgewiesen sind und die Voraussetzungen der Art. 44 bis 49 DSGVO sowie des jeweils einschlägigen Transfermechanismus erfüllt sind. Bei Wegfall der Voraussetzungen gilt § 9.

(4) Die KI-Verarbeitungen werden getrennt und zweckgebunden durchgeführt: (a) Mängelfotos werden ausschließlich zur automatisierten Vorklassifizierung und Erzeugung von Klassifizierungsergebnissen verarbeitet; (b) Sprachaufnahmen werden ausschließlich zur Transkription für das Bautagebuch verarbeitet; die daraus entstehenden Transkripte werden ausschließlich zur Strukturierung und gegebenenfalls Übersetzung der jeweiligen Eingabe verarbeitet. Eingaben, Ausgaben, technische Metadaten, Zugriffs- und Verarbeitungsprotokolle sowie Sicherungskopien dürfen jeweils nur für diesen Zweck verarbeitet werden. Eingaben beim KI-Unterauftragsverarbeiter sind nach Abschluss der Klassifizierung oder Transkription unverzüglich, spätestens innerhalb von 24 Stunden, zu löschen; Ausgaben werden nur in der Anwendung nach Maßgabe des § 11 gespeichert; technische Protokolle werden nach 7 Tagen und Sicherungskopien spätestens 35 Tage nach der Löschung aus dem Produktivsystem gelöscht. Eine Nutzung zu Training, Modellverbesserung, Profilbildung oder eigenen Zwecken ist nicht Gegenstand dieses Auftrags und ist vor einer Aktivierung ausdrücklich auszuschließen oder gesondert datenschutzrechtlich zu prüfen und zu vereinbaren.

(5) Die KI-Ausgaben sind ausschließlich unterstützende Arbeitsergebnisse. Eine automatisierte Entscheidung mit rechtlicher Wirkung oder einer ähnlich erheblichen Wirkung gegenüber einer natürlichen Person wird nicht getroffen. Der Verantwortliche oder die von ihm berechtigten Projektbeteiligten prüfen die KI-Ausgaben vor ihrer Verwendung.

§ 4 Art der personenbezogenen Daten

- Namen und Kontaktdaten (E-Mail, Telefon) der Projektbeteiligten
- Firmenzugehörigkeit und Rolle im Projekt
- Anschriften von Bauvorhaben, soweit sie einer natürlichen Person zuzuordnen sind
- Unterschriften (digitale Abnahmeunterschriften als Bilddatei)
- Fotodokumentationen, insbesondere Mängelfotos, auf denen Personen erkennbar sein können
- Kommunikationsinhalte aus Projektnachrichten und Bautagebuch
- Audioaufnahmen zur Spracherfassung für das Bautagebuch
- Für die KI-Funktionen werden zusätzlich Eingabedaten (Fotos, Audioaufnahmen, Transkripte und gegebenenfalls begleitende Texte), Ausgabedaten (Klassifizierungsergebnisse und Transkripte), technische Metadaten, Zugriffs- und Verarbeitungsprotokolle sowie Sicherungskopien verarbeitet. Zweck, Speicher- und Löschfristen richten sich nach § 3 Abs. 4 und § 11. OFFENE PRÜFUNG: Vor jeder Aktivierung ist anhand der konkreten Datenflüsse zu klären und zu dokumentieren, ob Fotos, Sprachaufnahmen oder Transkripte besondere Kategorien personenbezogener Daten nach Art. 9 DSGVO enthalten können.
- Prüfspurdaten zu Änderungen an Projektinhalten (Zeitpunkt und handelnde Person)

§ 5 Kategorien betroffener Personen

- Mitarbeiter und Nachunternehmer des Verantwortlichen

- Bauherren und Auftraggeber des Verantwortlichen
- Externe Projektpartner und am Bau beteiligte Gewerke
- Dritte, die auf Fotos oder Sprachaufnahmen erfasst werden

§ 6 Weisungsrecht des Verantwortlichen

(1) Der Auftragsverarbeiter verarbeitet personenbezogene Daten ausschließlich auf dokumentierte Weisung des Verantwortlichen, es sei denn, er ist nach dem Recht der Union oder der Mitgliedstaaten zur Verarbeitung verpflichtet; in diesem Fall teilt er dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht dies nicht wegen eines wichtigen öffentlichen Interesses verbietet.

(2) Die Nutzung der Anwendung im vertraglich vorgesehenen Umfang, einschließlich der vom Verantwortlichen aktivierten Funktionen und der in seinem Kundenkonto vorgenommenen Einstellungen, kann die Weisung und ihren Umfang dokumentieren. Sie ersetzt jedoch nicht die für Drittlandübermittlungen oder Drittlandzugriffe erforderliche transparente Information und dokumentierte Festlegung nach § 9. Ergänzende Weisungen erteilt der Verantwortliche in Textform an hallo@bibertron.de.

(3) Weisungsberechtigt sind die im Kundenkonto als administrationsberechtigt hinterlegten Personen. Der Verantwortliche hält diese Angaben aktuell.

(4) Weisungen werden nur im vereinbarten Leistungsumfang und im Rahmen der für die Anwendung vorgesehenen Funktionen umgesetzt. Bei widersprüchlichen, unklaren oder nach Auffassung des Auftragsverarbeiters datenschutzrechtlich unzulässigen Weisungen informiert der Auftragsverarbeiter den Verantwortlichen unverzüglich, bittet erforderlichenfalls um Klärung und kann die Ausführung bis zur Bestätigung oder Klärung aussetzen (Art. 28 Abs. 3 Satz 3 DSGVO).

§ 7 Pflichten des Auftragsverarbeiters

Der Auftragsverarbeiter verpflichtet sich insbesondere:

- personenbezogene Daten nur auf dokumentierte Weisung des Verantwortlichen zu verarbeiten, einschließlich im Hinblick auf Übermittlungen personenbezogener Daten in ein Drittland oder an eine internationale Organisation, soweit hierzu keine gesetzliche Verpflichtung besteht;
- die Vertraulichkeit aller mit der Verarbeitung befassten Personen sicherzustellen und diese schriftlich auf Vertraulichkeit zu verpflichten, soweit sie nicht bereits einer gesetzlichen Verschwiegenheitspflicht unterliegen (Art. 28 Abs. 3 lit. b DSGVO);
- die technischen und organisatorischen Maßnahmen nach Art. 32 DSGVO umzusetzen und aufrechtzuerhalten; die derzeit umgesetzten Maßnahmen sind in der Anlage 1 beschrieben (Art. 28 Abs. 3 lit. c DSGVO);
- den Verantwortlichen bei der Erfüllung seiner Pflichten gegenüber betroffenen Personen zu unterstützen, insbesondere bei Auskunfts-, Berichtigungs-, Löschungs-, Einschränkungs- und Übertragbarkeitsanfragen (Art. 28 Abs. 3 lit. e DSGVO). Wenden sich betroffene Personen unmittelbar an den Auftragsverarbeiter, leitet dieser die Anfrage unverzüglich an den Verantwortlichen weiter und beantwortet sie nicht selbst;
- den Verantwortlichen bei der Einhaltung der Pflichten aus den Art. 32 bis 36 DSGVO zu unterstützen, insbesondere bei der Datenschutz-Folgenabschätzung und einer vorherigen Konsultation der Aufsichtsbehörde (Art. 28 Abs. 3 lit. f DSGVO);

- den Verantwortlichen über Verletzungen des Schutzes personenbezogener Daten ohne schuldhaftes Zögern nach Bekanntwerden zu informieren und ihm die für dessen Meldung nach Art. 33 DSGVO erforderlichen Angaben zur Verfügung zu stellen, damit dieser die ihm obliegende Frist von 72 Stunden einhalten kann (Art. 33 Abs. 2 DSGVO);
- dem Verantwortlichen alle erforderlichen Informationen zum Nachweis der Einhaltung der in Art. 28 DSGVO festgelegten Pflichten zur Verfügung zu stellen und Überprüfungen einschließlich Inspektionen nach Maßgabe des § 12 zu ermöglichen (Art. 28 Abs. 3 lit. h DSGVO);
- ein Verzeichnis aller Kategorien von Verarbeitungstätigkeiten im Auftrag nach Art. 30 Abs. 2 DSGVO zu führen;
- nach Wahl des Verantwortlichen alle personenbezogenen Daten nach Maßgabe des § 11 zu löschen oder zurückzugeben;
- den Verantwortlichen unverzüglich zu informieren, wenn der Auftragsverarbeiter der Auffassung ist, dass eine Weisung gegen Datenschutzrecht verstößt, und die Ausführung nach Maßgabe des § 6 bis zur Klärung oder Bestätigung auszusetzen.

die Transfermechanismen, Anbieterbedingungen und Unterauftragsverarbeiter mindestens jährlich sowie anlassbezogen, insbesondere bei Änderungen der Rechtslage, des Verarbeitungsortes, des Zugriffsmodells oder der KI-Nutzungsbedingungen, zu prüfen und die Prüfung zu dokumentieren

den Verantwortlichen unverzüglich über festgestellte oder drohende Transfer- und Sicherheitsrisiken, behördliche Zugriffsverlangen, rechtliche Hindernisse oder den Wegfall eines Transfermechanismus zu informieren, soweit eine Information rechtlich zulässig ist

für KI-Verarbeitungen Löschtests für Eingaben, Ausgaben, Protokolle und Sicherungskopien sowie regelmäßige Überprüfungen privilegierter Konten und Anbieterzugriffe durchzuführen und die Ergebnisse nachzuweisen

§ 8 Pflichten des Verantwortlichen

(1) Der Verantwortliche ist hinsichtlich der Projektinhalte für die Rechtmäßigkeit der von ihm veranlassten Verarbeitung und für die Erfüllung seiner Pflichten als Verantwortlicher nach der DSGVO verantwortlich. Er stellt insbesondere sicher, dass für die Erhebung, Verarbeitung und Übermittlung der von ihm oder durch Projektbeteiligte in die Anwendung eingestellten Projektinhalte eine Rechtsgrundlage besteht. Die gesetzlichen Pflichten des Auftragsverarbeiters aus diesem Vertrag und der DSGVO bleiben unberührt.

(2) Der Verantwortliche kommt seinen Informationspflichten nach den Art. 13 und 14 DSGVO gegenüber den betroffenen Personen selbst nach. Das gilt insbesondere gegenüber Mitarbeitern, Nachunternehmern und Bauherren, die er zu Projekten einlädt, sowie gegenüber Personen, die auf Fotos oder Sprachaufnahmen erfasst werden.

(3) Der Verantwortliche beurteilt selbst, ob für seine Verarbeitung eine Datenschutz-Folgenabschätzung nach Art. 35 DSGVO erforderlich ist, und führt sie gegebenenfalls durch. Das gilt insbesondere, soweit er die Prüfspur, das Bautagebuch oder Foto- und Sprachaufnahmen in einer Weise nutzt, die eine Verhaltens- oder Leistungskontrolle seiner Beschäftigten ermöglicht.

(4) Wählt der Verantwortliche die Aufbewahrung nach § 11 Absatz 1, prüft er eigenständig, ob dafür eine Rechtsgrundlage besteht, insbesondere im Hinblick auf Daten seiner Beschäftigten.

(5) Meldungen an die Aufsichtsbehörde nach Art. 33 DSGVO und Benachrichtigungen betroffener Personen nach Art. 34 DSGVO nimmt der Verantwortliche vor.

(6) Der Verantwortliche erteilt Weisungen nach § 6 und benennt dem Auftragsverarbeiter einen Ansprechpartner für Datenschutzfragen.

§ 9 Weitere Auftragsverarbeiter

(1) Der Verantwortliche erteilt dem Auftragsverarbeiter die allgemeine Genehmigung zur Hinzuziehung weiterer Auftragsverarbeiter (Art. 28 Abs. 2 Satz 2 DSGVO). Zum Zeitpunkt des Vertragsschlusses sind dies die in der nachstehenden Übersicht und in Anlage 2 bezeichneten Anbieter. Anthropic PBC, OpenAI Ireland Ltd. sowie die von OpenAI eingesetzten US-Unterauftragsverarbeiter werden ausdrücklich als weitere Auftragsverarbeiter im Sinne des Art. 28 DSGVO behandelt. Anlage 2 konkretisiert für jeden Anbieter, soweit anhand der vorliegenden Unterlagen feststellbar, Rechtseinheit, Funktion, Datenkategorien, Verarbeitungs- und Zugriffsort, Unterauftragsverarbeiter, Transfermechanismus, Schutzmaßnahmen, Löschfristen und offene Prüfungen.

DIENSTLEISTER	ZWECK	ORT DER VERARBEITUNG
Hetzner Online GmbH, Gunzenhausen	Hosting und Speicherung einschließlich Datensicherung (Produktivsystem Nürnberg, Storage Box)	Deutschland
Brevo SAS, Paris, Frankreich	Technischer Versand von Benachrichtigungs- und Systemmails	Europäische Union
Anthropic PBC, USA	Automatisierte Vorklassifizierung von Mängelfotos; Strukturierung und gegebenenfalls Übersetzung von Transkripten der Spracheingabe	USA, EU-Standardvertragsklauseln nach Art. 46 Abs. 2 lit. c DSGVO
OpenAI Ireland Ltd., Dublin	Umwandlung von Sprachaufnahmen in Text (Bautagebuch)	Irland; Weiterverarbeitung durch Unterauftragsverarbeiter in den USA auf Grundlage der EU-Standardvertragsklauseln nach Art. 46 Abs. 2 lit. c DSGVO

Für Anthropic PBC, USA, gilt: Funktion ist die automatisierte Vorklassifizierung von Mängelfotos sowie die Strukturierung und gegebenenfalls Übersetzung von Transkripten der Spracheingabe. Verarbeitet werden können Mängelfotos, gegebenenfalls erkennbare Personen, Transkripte, Klassifizierungsergebnisse, Metadaten, Protokolle und Sicherungskopien. Verarbeitungs-, Support-, Konzern- und Fernzugriffsstaaten, die konkrete empfangende Rechtseinheit, weitere Unterauftragsverarbeiter, Transfermechanismus, DPF-Status, SCC-Modul, Anhänge, Transferprüfung und Löschung sind anhand aktueller Anbieterunterlagen zu bestätigen. OFFENE PRÜFUNG: Diese Angaben sind aus dem vorliegenden AVV nicht vollständig verifizierbar.

Für OpenAI Ireland Ltd., Dublin, gilt: Die irische Rechtseinheit ist von jedem tatsächlich eingesetzten US-Unterauftragsverarbeiter sowie von möglichen US-Konzern-, Support- oder Fernzugriffen zu unterscheiden. Funktion ist die Umwandlung von Sprachaufnahmen in Text für das Bautagebuch. Verarbeitet werden können Audioaufnahmen, Transkripte, gegebenenfalls Sprecher- und Kommunikationsinhalte, Metadaten, Protokolle und Sicherungskopien. OFFENE PRÜFUNG: aktuelle Unterauftragsverarbeiterliste, konkrete US-Rechtseinheiten, Speicher-, Support- und Zugriffsstaaten, Anbieterbedingungen, Transfermechanismus und Löschtests.

Für Drittlandübermittlungen gilt: Eine Berufung auf Art. 45 DSGVO setzt voraus, dass die konkrete empfangende Rechtseinheit zum maßgeblichen Zeitpunkt in der aktuellen Data-Privacy-Framework-Liste geführt wird und der Zertifizierungsumfang die konkrete Verarbeitung, Datenkategorien und etwaige

Weiterübermittlung abdeckt. Soweit Art. 45 DSGVO nicht anwendbar ist, sind die aktuellen Standarddatenschutzklauseln nach dem Durchführungsbeschluss (EU) 2021/914, das passende Modul und die erforderlichen Anhänge zu verwenden. Vor der Übermittlung ist eine dokumentierte Transferprüfung nach Schrems II einschließlich der Prüfung des Rechts des Bestimmungslandes, möglicher behördlicher Zugriffe und der praktischen Fähigkeit des Empfängers zur Einhaltung der Klauseln durchzuführen. SCC allein genügen nicht ohne diese Prüfung und erforderliche zusätzliche Schutzmaßnahmen. OFFENE PRÜFUNG: DPF-Status, Zertifizierungsumfang, SCC-Modul, Anhänge und Ergebnis der Transferprüfung sind je Anbieter aktuell zu dokumentieren.

Für KI-Übermittlungen sind mindestens folgende zusätzlichen Schutzmaßnahmen vertraglich und technisch sicherzustellen: Verschlüsselung während der Übertragung und Speicherung, Entfernung der EXIF-Metadaten, insbesondere der Standortangaben, bei Fotos vor der Übermittlung (eine inhaltliche Schwärzung oder Pseudonymisierung von Fotos, Audioaufnahmen und Transkripten findet nicht statt), strikte rollen- und zweckbezogene Zugriffsbeschränkung, getrennte Schlüsselverwaltung, Datenminimierung, keine Echtdaten in Test- oder Trainingsumgebungen, Löschung von Eingaben und Ausgaben nach den festgelegten Fristen, Ausschluss der Nutzung zu Training, Produktverbesserung, Profilbildung oder eigenen Zwecken sowie keine Weiterübermittlung ohne Genehmigung und dokumentierte Absicherung.

Der weitere Auftragsverarbeiter verpflichtet sich, den Auftragsverarbeiter unverzüglich über behördliche Zugriffsverlangen, rechtliche Hindernisse für die Vertragserfüllung, Änderungen des Drittlandrechts, eine drohende oder eingetretene Unmöglichkeit der Einhaltung der Standarddatenschutzklauseln und den Verlust oder die Einschränkung des DPF-Status zu informieren. Soweit eine Mitteilung rechtlich verboten ist, informiert er zumindest über die Unmöglichkeit der Vertragseinhaltung, soweit dies zulässig ist, und dokumentiert seine rechtlichen und technischen Gegenmaßnahmen.

Entfällt ein angemessenes Schutzniveau oder kann ein Transfermechanismus nicht mehr eingehalten werden, setzt der Auftragsverarbeiter die betroffene Übermittlung und erforderlichenfalls die betroffene KI-Funktion unverzüglich aus, beschränkt Zugriffe, veranlasst Rückgabe oder Löschung und informiert den Verantwortlichen. Die Verarbeitung wird erst nach dokumentierter Wiederherstellung einer geeigneten Garantie fortgesetzt. Ist dies nicht möglich, kann der Verantwortliche die betroffene Funktion außerordentlich kündigen; zwingende gesetzliche Rechte bleiben unberührt.

(2) Der Auftragsverarbeiter schließt mit jedem weiteren Auftragsverarbeiter einen Vertrag, der diesem im Wesentlichen dieselben Pflichten auferlegt, die in diesem Vertrag festgelegt sind (Art. 28 Abs. 4 DSGVO). Er bleibt dem Verantwortlichen gegenüber für die Einhaltung dieser Pflichten verantwortlich.

(3) Der Auftragsverarbeiter informiert den Verantwortlichen mindestens vier Wochen im Voraus in Textform über die Hinzuziehung oder den Austausch eines weiteren Auftragsverarbeiters sowie über Änderungen des Verarbeitungsorts, eines Fern-, Konzern- oder Supportzugriffs, des Transfermechanismus, des DPF-Zertifizierungsstatus, der eingesetzten Unterauftragsverarbeiter oder der KI-Nutzungsbedingungen. Der Verantwortliche kann der Änderung innerhalb von zwei Wochen ab Zugang der Mitteilung aus einem datenschutzrechtlichen Grund einschließlich einer wesentlichen Risikoerhöhung widersprechen. Bei begründetem Widerspruch oder einer wesentlichen Verschlechterung des Schutzniveaus kann der Verantwortliche die betroffene KI-Funktion bis zur Klärung vorläufig deaktivieren und die Verarbeitung aussetzen. Im Fall des Widerspruchs steht ihm ein Sonderkündigungsrecht zum Wirksamwerden der Änderung zu; Ziffer 5 Absatz 9 der Allgemeinen Geschäftsbedingungen gilt entsprechend. Gesetzliche Rechte des Verantwortlichen nach Art. 28 DSGVO bleiben unberührt.

(3a) Die Aussetzung, Abschaltung, Rückgabe und Löschung gilt auch bei einem behördlichen Zugriffsverlangen, einem begründeten Verdacht einer unzulässigen Weiterübermittlung oder einer nicht

bestandenen Transfer- oder Löschprüfung. Die jeweils betroffenen Eingaben, Ausgaben, Audio- und Fotodateien, Protokolle und Sicherungskopien sind nach § 11 zu behandeln.

(4) Nicht als weitere Auftragsverarbeiter gelten Nebenleistungen wie Telekommunikationsdienste, Post- und Transportdienste sowie Wartungs- und Prüfleistungen, die nicht auf die Verarbeitung personenbezogener Daten gerichtet sind. Dazu zählen auch reine Übertragungsdienste, bei denen der Inhalt für den Übertragenden nicht lesbar ist, insbesondere die Push-Dienste der Browserhersteller bei Ende-zu-Ende-verschlüsselten Nachrichteninhalten.

Für die Wetterdokumentation im Bautagebuch ruft der Anbieter allgemeine, nicht kundenbezogene Vorhersagedaten des Deutschen Wetterdienstes (DWD, Bundesbehörde, Offenbach am Main) über dessen Open-Data-Server ab und gleicht sie ausschließlich auf eigenen Servern mit der Koordinate des jeweiligen Bauvorhabens ab. An den Deutschen Wetterdienst werden keine Bauvorhaben-Koordinaten oder sonstigen personenbezogenen Daten übermittelt; der Abruf und der Abgleich mit der Koordinate finden vollständig innerhalb der eigenen Infrastruktur des Anbieters statt. Der Deutsche Wetterdienst ist deshalb kein weiterer Auftragsverarbeiter im Sinne dieses Vertrages.

(5) Cloudflare, Google Workspace und Mollie sind in dieser Liste nicht als weitere Auftragsverarbeiter dieses Vertrages aufgeführt, soweit die in der Datenschutzerklärung beschriebenen Verarbeitungen außerhalb des Gegenstands dieses Vertrages liegen oder als eigenverantwortliche Verarbeitungen von Bibertron beziehungsweise des Zahlungsdienstleisters beschrieben sind. Dieser Vertrag regelt diese Verarbeitungen nicht.

§ 10 Technisch-organisatorische Maßnahmen

(1) Der Auftragsverarbeiter trifft die in Anlage 1 beschriebenen technischen und organisatorischen Maßnahmen nach Art. 32 DSGVO.

(2) Die Maßnahmen unterliegen dem technischen Fortschritt. Der Auftragsverarbeiter darf sie anpassen, solange das Schutzniveau nicht unterschritten wird. Wesentliche Änderungen dokumentiert er und teilt sie dem Verantwortlichen auf Anfrage mit.

(3) Der Auftragsverarbeiter überprüft die Wirksamkeit der Maßnahmen mindestens jährlich und dokumentiert das Ergebnis.

(4) Für KI-Verarbeitungen und privilegierte Konten führt der Auftragsverarbeiter zusätzlich mindestens jährlich sowie anlassbezogen Prüfungen des Transfermechanismus, der Anbieterbedingungen, der Unterauftragsverarbeiter, der Zugriffskontrollen, der Löschung und der Wirksamkeit der zusätzlichen Schutzmaßnahmen durch. Anlassbezogene Prüfungen erfolgen insbesondere bei Sicherheitsvorfällen, Änderungen des Drittlandrechts, behördlichen Zugriffsverlangen, Anbieteränderungen oder begründeten Zweifeln an der Einhaltung. Die Ergebnisse werden dokumentiert und dem Verantwortlichen auf Anfrage zur Verfügung gestellt.

§ 11 Aufbewahrung, Löschung und Rückgabe

(1) Der Verantwortliche entscheidet bei Vertragsschluss und jederzeit danach in Textform, ob der Auftragsverarbeiter die im Auftrag verarbeiteten Projektdaten nach Ende des Nutzungsvertrages für zehn Jahre aufbewahren und für ihn lesend abrufbar halten soll. Diese Weisung setzt ein eigenes rechtliches oder wirtschaftliches Interesse des Verantwortlichen voraus, das der Verantwortliche mit der Weisung bestätigt. Ohne eine solche Weisung löscht der Auftragsverarbeiter die Projektdaten drei Monate nach Ende des Nutzungsvertrages, soweit keine gesetzliche Aufbewahrungspflicht entgegensteht.

(1a) Die Auswahl und Dauer der Aufbewahrung ist nach Datenkategorien und, soweit technisch möglich, nach einzelnen Projekten zu differenzieren. Eine zehnjährige Aufbewahrung rechtfertigt nicht automatisch die Aufbewahrung sämtlicher Datenkategorien. Der Verantwortliche prüft vor Erteilung und bei jeder Änderung der Weisung eigenständig die Erforderlichkeit und Rechtsgrundlage der Aufbewahrung, insbesondere bei Beschäftigtendaten, Audioaufnahmen, Fotos, Kommunikationsinhalten und Transkripten.

(2) Der Verantwortliche kann eine erteilte Weisung nach Absatz 1 jederzeit in Textform widerrufen und die vorzeitige Löschung oder Rückgabe verlangen. Er kann die Aufbewahrung auch auf einzelne Projekte beschränken. Der Auftragsverarbeiter setzt den Widerruf innerhalb von 30 Tagen um, soweit keine gesetzlichen Aufbewahrungspflichten entgegenstehen.

(3) Der Auftragsverarbeiter kann die verlängerte Aufbewahrung nach Absatz 1 mit einer Frist von acht Wochen in Textform beenden, indem er dem Verantwortlichen den vollständigen Datenbestand in einem strukturierten, gängigen und maschinenlesbaren Format bereitstellt. Drei Monate nach der Bereitstellung löscht der Auftragsverarbeiter die Daten, soweit keine gesetzliche Aufbewahrungspflicht entgegensteht. Die Regelung entspricht Ziffer 10 Absatz 5 der Allgemeinen Geschäftsbedingungen.

(4) Unabhängig von Absatz 1 gelten folgende Fristen:

- Daten aus einer nicht in ein Abonnement übergegangenen Testphase: Löschung mit Ablauf des lesenden Zugriffs nach Ziffer 3 Absatz 2 der Allgemeinen Geschäftsbedingungen, also 60 Tage nach Registrierung
- Zugriffs- und Serverprotokolldaten: Löschung nach 7 Tagen
- Versandprotokolle der Benachrichtigungsmails beim eingesetzten Versanddienstleister: Löschung nach Maßgabe der dort eingerichteten Aufbewahrungsregel; der Auftragsverarbeiter erteilt hierüber auf Anfrage Auskunft
- Rechnungen und Buchungsbelege des Auftragsverarbeiters: acht Jahre, beginnend mit dem Schluss des Kalenderjahres, in dem der Beleg entstanden ist (§ 147 Abs. 3 Satz 1 AO, § 257 Abs. 4 HGB, § 14b Abs. 1 Satz 1 UStG). Insoweit ist der Auftragsverarbeiter eigener Verantwortlicher; diese Daten unterliegen nicht der Weisung des Verantwortlichen

(5) Der Auftragsverarbeiter löscht personenbezogene Daten auch aus seinen Sicherungskopien. Da Sicherungskopien turnusmäßig überschrieben werden, erfolgt die Löschung aus den Sicherungskopien im Rahmen des bestehenden Sicherungszyklus, spätestens jedoch 35 Tage nach der Löschung aus dem Produktivsystem. Bis dahin sind die Daten gesperrt und werden ausschließlich zur Wiederherstellung im Störungsfall verwendet.

(5a) KI-Eingaben, insbesondere Audioaufnahmen und Fotos, sowie beim KI-Unterauftragsverarbeiter erzeugte Zwischen- und Ausgabedaten werden nach Abschluss der jeweiligen Verarbeitung unverzüglich, spätestens innerhalb von 24 Stunden, gelöscht, soweit sie nicht als Projektdaten in der Anwendung nach Weisung des Verantwortlichen benötigt werden. KI-Ausgaben und Transkripte in der Anwendung unterliegen den Weisungen nach Absatz 1; technische Protokolle werden nach 7 Tagen und Sicherungskopien spätestens 35 Tage nach der Löschung aus dem Produktivsystem gelöscht.

(5b) Ist die Löschung wegen eines zwingenden Drittlandrechts vorübergehend nicht möglich, werden die betroffenen Daten gesperrt, der Zugriff auf das rechtlich zwingend erforderliche Maß beschränkt und der Verantwortliche unverzüglich informiert, soweit dies rechtlich zulässig ist. Der Auftragsverarbeiter dokumentiert das Hindernis sowie die Rückgabe oder Löschung unverzüglich nach Wegfall des Hindernisses und weist sie nach.

(6) Über eine Löschung auf Verlangen des Verantwortlichen stellt der Auftragsverarbeiter ein Löschprotokoll zur Verfügung.

(7) Entfällt der Verantwortliche ersatzlos, insbesondere durch Löschung der Gesellschaft nach Abschluss der Liquidation, löscht der Auftragsverarbeiter die im Auftrag verarbeiteten Daten nach Ablauf von sechs Monaten ab Kenntnis, soweit keine gesetzliche Aufbewahrungspflicht entgegensteht.

§ 12 Nachweise und Kontrollen

(1) Der Auftragsverarbeiter weist die Einhaltung seiner Pflichten vorrangig durch aktuelle Selbstauskünfte, Prüfberichte, geeignete Zertifizierungen oder Auszüge daraus, die Dokumentation der Maßnahmen nach Anlage 1 sowie durch Nachweise seiner weiteren Auftragsverarbeiter nach. Diese Nachweise stellt er unentgeltlich zur Verfügung, soweit sie gesetzlich geschuldet oder zur angemessenen Prüfung dieses Vertrages erforderlich sind.

(2) Genügen diese Nachweise im Einzelfall nicht, kann der Verantwortliche eine Überprüfung einschließlich einer Inspektion durchführen oder durch einen beauftragten Prüfer durchführen lassen. Gesetzliche Prüf- und Nachweisrechte des Verantwortlichen bleiben unberührt. Die Überprüfung wird mit einem Vorlauf von mindestens vier Wochen in Textform angekündigt, findet während der üblichen Geschäftszeiten statt und darf den Betrieb nicht unangemessen beeinträchtigen.

Die Nachweis- und Kontrollrechte erstrecken sich auch auf die bei weiteren Auftragsverarbeitern eingesetzten technischen und organisatorischen Maßnahmen, Drittlandtransfers, Transferprüfungen, DPF-Zertifizierungen, Standarddatenschutzklauseln, Unterauftragsverarbeiterlisten, Anbieterzugriffe und Löschtests. Die Vier-Wochen-Ankündigungsfrist gilt nicht, soweit eine Prüfung wegen eines Sicherheitsvorfalls, einer behördlichen Prüfung, eines begründeten Verdachts, eines drohenden Wegfalls des Schutzniveaus oder zur Prüfung einer Löschung erforderlich ist.

(3) Ein beauftragter Prüfer darf kein Wettbewerber des Auftragsverarbeiters sein und ist zur Verschwiegenheit zu verpflichten.

(4) Für Überprüfungen nach Absatz 2 sowie für Unterstützungsleistungen nach § 7, die über den gesetzlich geschuldeten Umfang und über angemessene, zur Prüfung der Einhaltung dieses Vertrages erforderliche Nachweise und Kontrollen hinausgehen, kann der Auftragsverarbeiter eine Vergütung nach Aufwand verlangen. Der Stundensatz beträgt 120 Euro zuzüglich Umsatzsteuer. Gesetzlich geschuldete Nachweise sowie angemessene Kontrollen der weiteren Auftragsverarbeiter und Drittlandtransfers sind nicht kostenpflichtig. Dies gilt auch dann nicht, wenn die Überprüfung oder Unterstützungsleistung durch einen vom Auftragsverarbeiter zu vertretenden Umstand veranlasst ist.

§ 13 Haftung

(1) Für die Haftung der Parteien untereinander gilt Ziffer 13 der Allgemeinen Geschäftsbedingungen entsprechend, soweit diese Regelung mit den zwingenden Anforderungen der DSGVO und diesem Vertrag vereinbar ist.

(2) Art. 82 DSGVO sowie sonstige zwingende gesetzliche Ansprüche und die Haftung gegenüber betroffenen Personen und Aufsichtsbehörden bleiben unberührt. Die Beschränkungen nach Absatz 1 gelten nicht, soweit sie nach Art. 82 DSGVO oder nach sonstigem zwingendem Recht unwirksam wären.

(3) Der Auftragsverarbeiter bleibt dem Verantwortlichen nach Art. 28 Abs. 4 DSGVO für die Erfüllung der Pflichten seiner weiteren Auftragsverarbeiter verantwortlich. Ein Innenregress und die Verteilung weitergehender Schäden richten sich im Übrigen nach Ziffer 13 der Allgemeinen Geschäftsbedingungen,

soweit dies mit den zwingenden gesetzlichen Ansprüchen und der vollständigen, vor Verwendung zu prüfenden AGB-Fassung vereinbar ist.

§ 14 Schlussbestimmungen

(1) Änderungen dieses Vertrages bedürfen der Textform. Ziffer 14 der Allgemeinen Geschäftsbedingungen gilt entsprechend.

(2) Sollte eine Bestimmung dieses Vertrages unwirksam sein oder werden, bleibt die Wirksamkeit der übrigen Bestimmungen unberührt. Die Parteien ersetzen die unwirksame Bestimmung durch eine wirksame, die dem angestrebten Zweck am nächsten kommt.

(3) Bei Widersprüchen zwischen diesem Vertrag und den Allgemeinen Geschäftsbedingungen geht dieser Vertrag vor, soweit die Verarbeitung personenbezogener Daten im Auftrag betroffen ist. Ziffer 13 der Allgemeinen Geschäftsbedingungen bleibt nach Maßgabe des § 13 unberührt.

(4) Anfragen zum Datenschutz und Meldungen über Verletzungen des Schutzes personenbezogener Daten sind zu richten an: Bibertron UG (haftungsbeschränkt), Am Haag 8, 82166 Gräfelfing, E-Mail hallo@bibertron.de.

Anlage 1 Technische und organisatorische Maßnahmen nach Art. 32 DSGVO

VERTRAULICHKEIT

- **Zutrittskontrolle:** Das Produktivsystem wird im Rechenzentrum der Hetzner Online GmbH in Nürnberg betrieben, die Datensicherung auf einer Storage Box desselben Anbieters in Deutschland. Zutrittsschutz, Videoüberwachung und Besucherprotokollierung werden durch den Rechenzentrumsbetreiber sichergestellt.
- **Zugangskontrolle:** Authentifizierung über Passwort mit Mindestanforderungen an die Komplexität oder über einen zeitlich befristeten Anmeldelink per E-Mail. Passwörter werden ausschließlich als Hash gespeichert. Fail2Ban und Rate-Limiting gegen automatisierte Anmeldeversuche.
- **Verwaltung von Zugangsdaten:** Zugangsdaten zu Fremdsystemen, insbesondere für den Mailversand, Signaturschlüssel für Push-Benachrichtigungen und Schlüssel für Programmierschnittstellen, werden außerhalb des Quellcodes in der Serverumgebung hinterlegt und nicht in der Versionsverwaltung gespeichert.
- **Zugriffskontrolle:** Rollen- und projektbezogene Berechtigungen. Kein Zugriff zwischen Kundenmandanten. Administrativer Zugriff nur für benannte Personen des Auftragsverarbeiters und nur im erforderlichen Umfang.
- **Trennungskontrolle:** Logische Mandantentrennung der Kundendaten. Getrennte Umgebungen für Entwicklung, Test und Produktion. In Test- und Entwicklungsumgebungen werden keine Echtdaten verwendet.
- **Verpflichtung auf Vertraulichkeit:** Alle mit der Verarbeitung befassten Personen sind schriftlich auf das Datengeheimnis verpflichtet und werden mindestens jährlich zum Datenschutz unterwiesen.

INTEGRITÄT

- **Übertragungskontrolle:** Verschlüsselte Datenübertragung über HTTPS mit TLS 1.2 oder höher. Weiterleitung unverschlüsselter Verbindungen auf verschlüsselte.
- **Schutz gespeicherter Daten:** Der Betrieb erfolgt auf virtuellen Servern des Hosting-Dienstleisters in nach ISO/IEC 27001:2022 zertifizierten und nach BSI C5 Typ 2 testierten Rechenzentren. Ausgetauschte

Datenträger werden durch den Rechenzentrumsbetreiber vor Ort physisch zerstört und verlassen dessen Standorte nicht in einer Form, die eine Rekonstruktion der Daten ermöglicht.

- **Verschlüsselung der Sicherungskopien:** Sicherungskopien werden vor der Übertragung mit AES-256 verschlüsselt. Der Sicherungsspeicher erhält zu keinem Zeitpunkt unverschlüsselte Daten.
- **Eingabekontrolle:** Protokollierung von Anlage, Änderung und Löschung von Projektinhalten mit Zeitpunkt und handelnder Person (Prüfspur).

VERFÜGBARKEIT UND BELASTBARKEIT

- Tägliche automatisierte Datensicherung um 2:30 Uhr auf eine Storage Box der Hetzner Online GmbH mit Standort in Deutschland. Aufbewahrung der Sicherungen für 30 Tage.
- **Wiederherstellbarkeit:** Die Wiederherstellung des Produktivsystems aus der Sicherung ist innerhalb von 24 Stunden vorgesehen; der maximale Datenverlust beträgt 24 Stunden. Die Wiederherstellbarkeit der Sicherungen wird nächtlich automatisiert geprüft und das Ergebnis dokumentiert.
- **Schutz vor Angriffen:** Firewall, Rate-Limiting, regelmäßige Einspielung von Sicherheitsaktualisierungen.

VERFAHREN ZUR ÜBERPRÜFUNG UND BEWERTUNG

- Jährliche Überprüfung der Wirksamkeit der Maßnahmen mit Dokumentation des Ergebnisses.
- Verfahren zur Meldung und Bearbeitung von Verletzungen des Schutzes personenbezogener Daten mit benannten Zuständigkeiten.
- **Auftragskontrolle:** Schriftliche Vereinbarungen mit allen weiteren Auftragsverarbeitern nach Art. 28 DSGVO, regelmäßige Prüfung von deren Nachweisen.
- Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen nach Art. 25 DSGVO, insbesondere durch die Beschränkung der Sichtbarkeit von Projektinhalten auf die jeweilige Rolle im Projekt.
- **Zusätzliche Maßnahmen für KI-Verarbeitungen:** Verschlüsselung während der Übertragung und Speicherung, Entfernung der EXIF-Metadaten, insbesondere der Standortangaben, bei Fotos vor der Übermittlung (eine inhaltliche Schwärzung oder Pseudonymisierung von Fotos, Audioaufnahmen und Transkripten findet nicht statt), getrennte Schlüsselverwaltung, strikte Rollen- und Projektberechtigungen, keine Echtdaten in Test- oder Trainingsumgebungen, protokollierte Anbieterzugriffe, dokumentierte Löschtests für Eingaben, Ausgaben und Sicherungskopien sowie Schwachstellenmanagement.
- Privilegierte Konten sind durch Mehrfaktor-Authentifizierung oder Passkeys zu schützen, nach dem Prinzip der minimalen Rechtevergabe zu berechtigen und mindestens vierteljährlich auf ihre Berechtigung zu überprüfen. Anbieterzugriffe sind auf das erforderliche Maß zu beschränken, zu protokollieren und regelmäßig auszuwerten. Festgestellte Transfer- oder Sicherheitsrisiken sind unverzüglich zu bewerten, zu behandeln und dem Verantwortlichen mitzuteilen.
- **Incident-Response:** Sicherheitsvorfälle und Verletzungen des Schutzes personenbezogener Daten werden über einen dokumentierten Melde- und Bearbeitungsprozess erkannt, bewertet, eingedämmt, nachbereitet und auf gesetzliche Meldepflichten geprüft. Zuständigkeiten und Eskalationswege sind benannt; der Verantwortliche wird nach § 7 unverzüglich informiert.
- **Sichere Softwareentwicklung und Schwachstellenmanagement:** Änderungen werden in geschützten Entwicklungszweigen geprüft, in einer von der Produktivumgebung getrennten Testumgebung getestet und vor der Produktivsetzung freigegeben. Sicherheits-, Abhängigkeits- und Schwachstellenscans werden regelmäßig durchgeführt; festgestellte Schwachstellen werden nach Schweregrad priorisiert und zeitnah behoben.

Anlage 2 Drittlandübermittlungen und KI-Unterauftragsverarbeiter

Anbieter-/Datenflussmatrix. Die nachstehenden Angaben sind Mindestangaben und anhand aktueller Anbieterunterlagen, tatsächlicher Datenflüsse, Unterauftragsverarbeiterlisten und Transferprüfungen fortlaufend zu aktualisieren. Ein Sitz in der EU oder im EWR schließt einen Drittlandzugriff, Konzernzugriff oder Supportzugriff nicht aus.

Hetzner Online GmbH, Gunzenhausen – Funktion: Hosting, Speicherung und Datensicherung; Datenkategorien: Projektdaten, Nutzer- und Kontaktdaten, Fotos, Audio, Transkripte, Protokolle und Sicherungskopien; Verarbeitungsort: Deutschland; Fernzugriff: administrativer Zugriff nur im erforderlichen Umfang, tatsächliche Support- und Zugriffsstaaten nach Anbieterunterlagen zu prüfen; Unterauftragsverarbeiter: aus dem vorliegenden AVV nicht ersichtlich; Transfermechanismus: kein Drittlandtransfer ausgewiesen; Schutzmaßnahmen: Verschlüsselung, Mandantentrennung, Rollenrechte, Backups und Löschtests nach Anlage 1; Löschfristen: Produktivdaten nach § 11, Protokolle 7 Tage, Sicherungskopien spätestens 35 Tage nach Produktivlöschung; offene Prüfung: aktuelle Rechenzentrums-, Support- und Unterauftragsverarbeiterangaben prüfen.

Brevo SAS, Paris, Frankreich – Funktion: technischer Versand von Benachrichtigungs- und Systemmails; Datenkategorien: E-Mail-Adressen, Versand- und Zustellmetadaten sowie Benachrichtigungsinhalte im erforderlichen Umfang; Verarbeitungsort: Europäische Union; Fern- oder Supportzugriffe: nach Anbieterunterlagen zu prüfen; Unterauftragsverarbeiter: aus dem vorliegenden AVV nicht ersichtlich; Transfermechanismus: EU-/EWR-Verarbeitung, Art. 44 ff. DSGVO nur bei tatsächlicher Drittlandweiterleitung; Schutzmaßnahmen: Datenminimierung, Zugriffsbeschränkung und Löschung nach Anbieterregel; Löschfrist: nach Maßgabe der beim Versanddienstleister eingerichteten Aufbewahrungsregel; offene Prüfung: tatsächliche Speicher-, Support- und Weiterübermittlungsorte prüfen.

Anthropic PBC, USA – Funktion: automatisierte Vorklassifizierung von Mängelfotos sowie Strukturierung und gegebenenfalls Übersetzung von Transkripten der Spracheingabe; Datenkategorien: Mängelfotos, Transkripte, gegebenenfalls erkennbare Personen, Klassifizierungsergebnisse, Metadaten, Protokolle und Sicherungskopien; Verarbeitungs- und Zugriffsstaaten: USA und alle tatsächlichen Verarbeitungs-, Support- und Zugriffsstaaten; Fern-, Konzern- und Supportzugriffe: OFFENE PRÜFUNG; Unterauftragsverarbeiter: OFFENE PRÜFUNG; Transfermechanismus: Art. 45 DSGVO nur bei konkreter aktueller DPF-Zertifizierung, sonst Art. 46 DSGVO mit aktuellen SCC; DPF-Status, Zertifizierungsumfang, SCC-Modul, Anhänge, Transferprüfung und Löschtest: OFFENE PRÜFUNG; zusätzliche Schutzmaßnahmen: TLS, Verschlüsselung im Ruhezustand, Entfernung der EXIF-Metadaten bei Fotos (keine inhaltliche Schwärzung), getrennte Schlüssel, kein Training oder eigene Zwecke, keine Weiterübermittlung ohne Genehmigung.

OpenAI Ireland Ltd., Dublin, einschließlich sämtlicher tatsächlich eingesetzter US-Unterauftragsverarbeiter – Funktion: Transkription von Sprachaufnahmen für das Bautagebuch; Datenkategorien: Audioaufnahmen, Transkripte, gegebenenfalls Sprecher- und Kommunikationsinhalte, Metadaten, Protokolle und Sicherungskopien; Verarbeitungsorte: Irland sowie USA und alle tatsächlichen Verarbeitungs-, Support- und Zugriffsstaaten; konkrete Fern-, Support- und Konzernzugriffe sowie US-Unterauftragsverarbeiter: OFFENE PRÜFUNG; Transfermechanismus: Art. 45 DSGVO nur für die konkrete zertifizierte US-Rechtseinheit und den abgedeckten Umfang, sonst Art. 46 DSGVO mit aktuellen SCC; DPF-Status, SCC-Modul, Anhänge, Weiterübermittlungskette, Transferprüfung und Löschtest: OFFENE PRÜFUNG; zusätzliche Schutzmaßnahmen: TLS, Verschlüsselung, getrennte Schlüssel, kein Training oder eigene Zwecke, keine ungenehmigte Weiterübermittlung.

Für alle Anbieter gilt: Eine Änderung von Verarbeitungsort, Fern- oder Konzernzugriff, Unterauftragsverarbeiter, Transfermechanismus, DPF-Status, Speicher- oder Löschfristen sowie der KI-Nutzungsbedingungen ist nach §

9 Abs. 3 zu behandeln. Bei Wegfall einer Garantie werden der betroffene Transfer und erforderlichenfalls die betroffene KI-Funktion ausgesetzt, die Daten gesperrt oder gelöscht und der Verantwortliche informiert. Die konkrete Rechtmäßigkeit kann erst nach Prüfung der aktuellen Anbieterunterlagen, Datenflüsse, DPF-Zertifizierungen und dokumentierten Transferprüfungen abschließend beurteilt werden.

Dokumenthinweis – Rechtsgrundlagen und Prüfvorbehalt: Verordnung (EU) 2016/679, insbesondere Art. 28, 32, 44–49; EuGH, Urteil vom 16. Juli 2020, C-311/18, ECLI:EU:C:2020:559; Durchführungsbeschluss (EU) 2021/914 der Kommission vom 4. Juni 2021; Durchführungsbeschluss (EU) 2023/1795 der Kommission vom 10. Juli 2023. Diese Quellenangaben ersetzen keine anbieterbezogene Prüfung. Die konkrete Rechtmäßigkeit der Transfers ist vor Aktivierung und fortlaufend anhand aktueller Anbieterunterlagen, tatsächlicher Datenflüsse, Zertifizierungen, Unterauftragsverarbeiterlisten und dokumentierter Transferprüfungen zu prüfen.

Stand 05.11.2026 · Bibertron UG (haftungsbeschränkt), Am Haag 8, 82166 Gräfelfing · jeweils aktuelle Fassung: https://bau.bibertron.de/bau/avv