

Rahmen-Auftragsverarbeitungsvertrag (AVV)

gemäß Art. 28 DSGVO

Auftragsverarbeiter:

EXT IT GmbH, Vahrenwalder Str. 271, 30179 Hannover • HRB 230379 (Amtsgericht Hannover) • USt-IdNr: DE461194895

Geschäftsführer: Kilian Schwarz, Maik Harald Döbler, Philipp-Alexander Meyer • Datenschutzkontakt: datenschutz@ext-it.tech

Veröffentlicht unter: ext-it.tech/avv

§1 Geltungsbereich und Einbeziehung

- (1) Dieser Rahmen-Auftragsverarbeitungsvertrag (nachfolgend „AVV“) regelt die datenschutzrechtlichen Pflichten zwischen der **EXT IT GmbH** (nachfolgend „Auftragnehmer“ oder „Auftragsverarbeiter“) und dem jeweiligen Kunden (nachfolgend „Auftraggeber“ oder „Verantwortlicher“) im Zusammenhang mit der Auftragsverarbeitung gemäß Art. 28 DSGVO.
- (2) **Einbeziehung:** Dieser AVV wird Vertragsbestandteil, sobald der Auftraggeber ein Angebot, einen Vertrag, eine Bestellung oder einen Einzelauftrag des Auftragnehmers annimmt, der auf diesen AVV verweist. Die Annahme kann durch Unterschrift, elektronische Bestätigung, konkludentes Handeln (z.B. Beauftragung) oder ausdrückliche Zustimmung erfolgen. Eine gesonderte Unterzeichnung dieses AVV ist nicht erforderlich.
- (3) Der AVV in seiner jeweils aktuellen Fassung ist jederzeit unter ext-it.tech/avv abrufbar. Wesentliche Änderungen dieses AVV teilt der Auftragnehmer dem Auftraggeber mindestens **sechs (6) Wochen** vor Inkrafttreten in Textform (§ 126b BGB) mit. Die Mitteilung enthält eine Gegenüberstellung der bisherigen und neuen Regelung sowie einen Hinweis auf das Widerspruchsrecht. Der Auftraggeber kann der Änderung innerhalb von **vier (4) Wochen** nach Zugang in Textform widersprechen. Widerspricht der Auftraggeber, gelten die bisherigen Bestimmungen fort. Können sich die Parteien nicht innerhalb von **30 Tagen** nach Widerspruch auf eine einvernehmliche Lösung einigen, hat der Auftraggeber das Recht zur außerordentlichen Kündigung der betroffenen Leistung zum Zeitpunkt des geplanten Inkrafttretens. Redaktionelle Änderungen, Klarstellungen und Änderungen zu Gunsten des Auftraggebers werden ohne Widerspruchsverfahren wirksam.
- (4) Dieser AVV besteht aus dem vorliegenden Rahmen-AVV, der Anlage 1 (Technische und Organisatorische Maßnahmen), den produktspezifischen Anlagen (je beauftragtem Service eine Anlage) sowie der Anlage 3 (Zentrale Unterauftragsverarbeiter-Liste). Alle Bestandteile sind unter ext-it.tech/avv abrufbar.
- (5) Welche produktspezifischen Anlagen im konkreten Vertragsverhältnis gelten, ergibt sich aus dem jeweiligen Angebot, Vertrag oder Einzelauftrag.

§2 Gegenstand und Dauer der Verarbeitung

- (1) Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag und nach dokumentierter Weisung des Auftraggebers im Rahmen der jeweils beauftragten IT-Dienstleistungen.
- (2) Die Laufzeit dieses AVV richtet sich nach der Laufzeit des zugrunde liegenden Vertragsverhältnisses. Er beginnt mit der Einbeziehung gemäß §1 Abs. 2 und endet automatisch mit Beendigung des letzten zwischen den Parteien bestehenden Vertragsverhältnisses, unbeschadet etwaiger Nachwirkungspflichten (insb. Löschung/Rückgabe gemäß §10).

- (3) Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich auf Grundlage dokumentierter Weisungen des Auftraggebers (Weisungsgebundenheit), es sei denn, er ist durch das Recht der Union oder der Mitgliedstaaten zur Verarbeitung verpflichtet. In diesem Fall teilt der Auftragnehmer dem Auftraggeber diese rechtliche Anforderung vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

§3 Art und Zweck der Verarbeitung, Kategorien betroffener Personen und Daten

- (1) Art, Zweck und Umfang der Verarbeitung, die Kategorien der betroffenen Personen sowie die Kategorien der verarbeiteten personenbezogenen Daten ergeben sich aus der jeweils beauftragten Leistung und sind in den **produktspezifischen Anlagen zum AVV (je beauftragtem Service eine Anlage)** im Detail beschrieben.
- (2) Die Art der Verarbeitung kann insbesondere umfassen: Erheben, Erfassen, Organisation, Ordnen, Speicherung, Anpassung, Veränderung, Auslesen, Abfragen, Verwendung, Übermittlung, Abgleich, Verknüpfung, Einschränkung, Löschen und Vernichtung.
- (3) Die produktspezifischen Anlagen sind Bestandteil dieses AVV. Im jeweiligen Angebot oder Vertrag wird angegeben, welche produktspezifischen Anlagen für das Vertragsverhältnis gelten.

§4 Pflichten des Auftragsverarbeiters

- (1) Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich auf Grundlage der dokumentierten Weisungen des Auftraggebers (Art. 28 Abs. 3 lit. a DSGVO). Weisungen können schriftlich, in Textform oder in elektronischer Form erteilt werden. In Eilfällen können Weisungen mündlich erteilt werden; der Auftraggeber bestätigt diese unverzüglich in Textform. Die Beauftragung einer Leistung gemäß dem Hauptvertrag gilt als dokumentierte Weisung für die dort beschriebenen Verarbeitungen. Darüber hinausgehende Weisungen bedürfen der Textform.
- (2) Der Auftragnehmer gewährleistet, dass die mit der Verarbeitung befassten Personen:
 - a) zur Vertraulichkeit verpflichtet sind oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen (Art. 28 Abs. 3 lit. b DSGVO),
 - b) die personenbezogenen Daten nur auf Weisung des Auftraggebers verarbeiten,
 - c) regelmäßig im Datenschutz und in der Informationssicherheit geschult werden.
- (3) Der Auftragnehmer ergreift angemessene technische und organisatorische Maßnahmen gemäß Art. 32 DSGVO, wie in **Anlage 1 (TOMs)** dokumentiert.
- (4) Der Auftragnehmer unterstützt den Auftraggeber unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen bei:
 - a) der Erfüllung der Pflichten zur Beantwortung von Anträgen betroffener Personen auf Ausübung ihrer Rechte gemäß Kapitel III DSGVO (Art. 28 Abs. 3 lit. e DSGVO),
 - b) der Einhaltung der Pflichten gemäß Art. 32-36 DSGVO (Datensicherheit, Meldepflichten, Datenschutz-Folgenabschätzung, vorherige Konsultation).

Im Rahmen der Unterstützung bei Datenschutz-Folgenabschätzungen (DSFA) gemäß Art. 35 DSGVO stellt der Auftragnehmer dem Auftraggeber auf Anfrage insbesondere folgende Informationen zur Verfügung: Beschreibung der technischen und organisatorischen Maßnahmen, Informationen zu eingesetzten Unterauftragsverarbeitern und Drittlandtransfers, Art und Umfang der Datenverarbeitung sowie eine Einschätzung der Risiken aus Sicht des Auftragsverarbeiters. Die Kostentragung richtet sich nach §4 Abs. 6.

- (5) Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich, wenn er der Auffassung ist, dass eine Weisung gegen die DSGVO oder andere datenschutzrechtliche Bestimmungen verstößt (Art. 28 Abs. 3 Satz 3 DSGVO). Der Auftragnehmer ist berechtigt, die Durchführung der betreffenden Weisung bis zur Bestätigung oder Änderung durch den Auftraggeber auszusetzen.

- a) **Änderungsweisungen nach Leistungsbeginn:** Weisungen, die über den im Hauptvertrag und den produktspezifischen Anlagen definierten Verarbeitungsumfang hinausgehen, bedürfen der Textform und einer angemessenen Umsetzungsfrist. Der Auftragnehmer prüft die Umsetzbarkeit und informiert den Auftraggeber innerhalb von **10 Werktagen** über die technische und organisatorische Machbarkeit sowie etwaige Mehrkosten. Soweit die Änderungsweisung den bestehenden Verarbeitungsumfang wesentlich verändert, wird die betreffende produktspezifische Anlage entsprechend aktualisiert.
- (6) Soweit die Unterstützungsleistungen des Auftragnehmers nach §4 Abs. 4, §7, §8 und §9 über das im Rahmen der vereinbarten Vergütung abgedeckte Maß hinausgehen, kann der Auftragnehmer einen angemessenen Vergütungsanspruch geltend machen. Die Vergütung richtet sich nach der jeweils geltenden Preisliste des Auftragnehmers.
- (7) Sollten die Daten des Auftraggebers beim Auftragnehmer durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren gefährdet werden, hat der Auftragnehmer den Auftraggeber unverzüglich darüber zu informieren. Der Auftragnehmer wird alle Verantwortlichen darüber informieren, dass die Hoheit und das Eigentum an den Daten beim Auftraggeber als Verantwortlichem liegen.
- (8) Auskünfte an Dritte oder Betroffene darf der Auftragnehmer nur nach vorheriger Zustimmung des Auftraggebers erteilen, es sei denn, er ist gesetzlich dazu verpflichtet.

§5 Technische und Organisatorische Maßnahmen

- (1) Der Auftragnehmer hat die in **Anlage 1 (TOMs)** dokumentierten technischen und organisatorischen Maßnahmen umgesetzt. Diese gewährleisten ein dem Risiko angemessenes Schutzniveau unter Berücksichtigung von:
 - a) dem Stand der Technik,
 - b) den Implementierungskosten,
 - c) der Art, dem Umfang, den Umständen und den Zwecken der Verarbeitung,
 - d) der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen.
- (2) Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Der Auftragnehmer ist berechtigt, alternative adäquate Maßnahmen umzusetzen, sofern das Sicherheitsniveau nicht unterschritten wird. Wesentliche Änderungen werden in Anlage 1 dokumentiert und sind unter der in §1 Abs. 4 genannten URL einsehbar.
- (3) Der Auftragnehmer überprüft die Wirksamkeit der technischen und organisatorischen Maßnahmen **regelmäßig, mindestens anlassbezogen** (Art. 32 Abs. 1 lit. d DSGVO), und dokumentiert die Ergebnisse.

§6 Unterauftragsverarbeitung

- (1) Der Auftraggeber erteilt dem Auftragnehmer eine allgemeine schriftliche Genehmigung zur Hinzuziehung weiterer Auftragsverarbeiter (Unterauftragsverarbeiter) im Sinne des Art. 28 Abs. 2 DSGVO.
- (2) Die zum Zeitpunkt des Vertragsschlusses genehmigten produktspezifischen Unterauftragsverarbeiter sind in **Abschnitt 9 der jeweiligen produktspezifischen Anlage** aufgeführt. Die jeweils aktuelle Fassung der Anlagen ist unter ext-it.tech/avv einsehbar.
- (3) **Produktübergreifende Unterauftragsverarbeiter:** Der Auftragnehmer setzt bei Bedarf Subunternehmer und Freelancer für die technische Leistungserbringung im Kundenauftrag ein. Diese erhalten Zugriff auf Kundensysteme und -daten im Rahmen der beauftragten IT-Dienstleistungen. Es werden nur Subunternehmer eingesetzt, die vertraglich zur Einhaltung der Datenschutzpflichten (inkl. Vertraulichkeit und Weisungsgebundenheit) verpflichtet sind. Der

Auftraggeber wird gemäß Abs. 4 über den konkreten Einsatz (Name, Firma, Einsatzzweck) informiert.

- (4) Der Auftragnehmer informiert über beabsichtigte Änderungen an der Unterauftragsverarbeiter-Liste mindestens **30 Tage** vor deren Inkrafttreten durch Veröffentlichung der aktualisierten Liste unter ext-it.tech/avv. Der Auftraggeber kann beim Onboarding eine E-Mail-Adresse zur aktiven Benachrichtigung hinterlegen; ohne Hinterlegung gilt die Pflicht zur rechtzeitigen Kenntnisnahme der unter vorgenannter URL veröffentlichten Liste. Der Auftraggeber kann gegen beabsichtigte Änderungen innerhalb dieser 30-Tage-Frist begründeten Einspruch in Textform erheben.
- (5) Erhebt der Auftraggeber berechtigten Einspruch, bemühen sich die Parteien um eine einvernehmliche Lösung. Kann keine Einigung erzielt werden, steht dem Auftraggeber ein Sonderkündigungsrecht bezüglich der betroffenen Leistungen zu.
- (6) Der Auftragnehmer legt dem Unterauftragsverarbeiter im Wege eines Vertrages dieselben Datenschutzpflichten auf, die in diesem AVV festgelegt sind (Art. 28 Abs. 4 DSGVO).
- (7) Der Auftragnehmer haftet dem Auftraggeber gegenüber für die Einhaltung der Datenschutzpflichten durch den Unterauftragsverarbeiter wie für eigenes Handeln. Die Haftung des Auftragnehmers für Unterauftragsverarbeiter richtet sich nach §12 dieser AVV; eine darüber hinausgehende verschärfte Haftung besteht nicht.
- (8) Die Verarbeitung personenbezogener Daten außerhalb der EU/des EWR darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind. Als Rechtsgrundlage kommen insbesondere Angemessenheitsbeschlüsse nach Art. 45 DSGVO, die von der EU-Kommission veröffentlichten Standardvertragsklauseln (SCCs) nach Durchführungsbeschluss (EU) 2021/914 vom 04.06.2021 oder vergleichbare Garantien im Sinne des Art. 46 DSGVO in Betracht. Details zu Drittlandtransfers und den jeweils verwendeten Garantien ergeben sich aus den produktspezifischen Anlagen und Anlage 3.
- (9) Nicht als Unterauftragsverarbeitung im Sinne dieses AVV gelten Nebenleistungen wie Telekommunikation, Post-/Transportdienstleistungen, Reinigung, Gebäudesicherheit und allgemeine IT-Infrastrukturdienste (z.B. Internet Service Provider), bei denen keine gezielte Verarbeitung personenbezogener Daten im Auftrag erfolgt.
- (10) **Hosting-Anbieter mit physischem Zugang:** Hosting-Dienstleister, die physischen Zugang zur Server-Hardware des Auftragnehmers haben und auf deren Infrastruktur personenbezogene Daten im Auftrag gespeichert werden, gelten als Unterauftragsverarbeiter im Sinne dieses AVV und sind in Anlage 3 aufgeführt. Die Klarstellung dient der Abgrenzung zu reinen Konnektivitätsdienstleistern gemäß Abs. 9: Sobald die Möglichkeit der Kenntnisnahme personenbezogener Daten durch den Hosting-Anbieter besteht (z.B. durch Wartungszugriff auf laufende Systeme, Datenträgerhandling bei Hardware-Austausch), ist der Anbieter als Auftragsverarbeiter einzustufen (vgl. EDPB-Leitlinien zu Hosting-Anbietern). Der Auftragnehmer setzt in diesem Fall risikobasierte technische und organisatorische Maßnahmen ein (insbesondere physische Zugangskontrolle, logische Zugriffskontrolle und kontinuierliches Monitoring), um die tatsächliche Kenntnisnahmemöglichkeit zu minimieren. Satz 1 gilt entsprechend, wenn der Hosting-Dienstleister physischen Zugang zu Hardware des Auftraggebers hat, die in seinen Räumlichkeiten betrieben wird (Colocation/Housing).

§7 Informationspflichten bei Datenschutzverletzungen

- (1) Der Auftragnehmer unterrichtet den Auftraggeber **unverzüglich**, in der Regel innerhalb von **48 Stunden** nach Kenntniserlangung einer Verletzung des Schutzes personenbezogener Daten (Art. 33 Abs. 2 DSGVO). Die Meldung erfolgt an den benannten Ansprechpartner des Auftraggebers oder, falls kein Ansprechpartner benannt ist, an die im Vertrag hinterlegte E-Mail-Adresse. Die Erstmeldung ist ggf. vorläufig und wird durch eine vollständige Detailmeldung gemäß Abs. 5 ergänzt.

Verhältnis zu parallelen Meldepflichten: Ist ein Vorfall zugleich ein erheblicher Sicherheitsvorfall i.S.d. § 32 BSIG n.F. (NIS2), gelten die Fristen und Inhalte des §14 Abs. 6 lit. b ergänzend. Ist ein Vorfall ausschließlich ein allgemeiner Sicherheitsvorfall ohne Betroffenheit personenbezogener Daten, gilt §8a AGB (Erstmeldung in der Regel innerhalb von 48 Stunden). Die Fristen laufen parallel; maßgeblich ist die jeweils strengere gesetzliche Anforderung. Eigene Meldepflichten der Parteien gegenüber Aufsichtsbehörden (LfD, BSI) bleiben unberührt.

- (2) Die Meldung enthält mindestens folgende Informationen:
 - a) Beschreibung der Art der Verletzung, soweit möglich mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen und Datensätze,
 - b) den Namen und die Kontaktdaten der Anlaufstelle für weitere Informationen,
 - c) eine Beschreibung der wahrscheinlichen Folgen der Verletzung,
 - d) eine Beschreibung der ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung und Abmilderung.
- (3) Der Auftragnehmer unterstützt den Auftraggeber bei der Erfüllung seiner Meldepflichten gegenüber der Aufsichtsbehörde (Art. 33 DSGVO) und den betroffenen Personen (Art. 34 DSGVO).
- (4) Der Auftragnehmer dokumentiert alle Datenschutzverletzungen einschließlich aller damit zusammenhängenden Fakten, Auswirkungen und ergriffenen Abhilfemaßnahmen.
- (5) **Eskalationskette:** Die Meldung einer Datenschutzverletzung erfolgt nach folgendem Eskalationsverfahren:

Stufe	Zeitraum	Empfänger	Inhalt
1 – Erstmeldung	Unverzüglich, in der Regel innerhalb 48 Std. nach Kenntniserlangung	Benannter Ansprechpartner des Auftraggebers	Vorläufige Beschreibung des Vorfalls, Art der Verletzung, erste Sofortmaßnahmen
2 – Detailmeldung	Innerhalb 72 Std. nach Kenntniserlangung	Benannter Ansprechpartner + Datenschutzkontakt des Auftraggebers	Vollständige Meldung gemäß Abs. 2 lit. a–d
3 – Abschlussbericht	Auf Anfrage des Auftraggebers oder der Aufsichtsbehörde	Benannter Ansprechpartner bzw. anfragende Stelle	Ursachenanalyse, vollständige Auswirkungenanalyse, ergriffene und geplante Abhilfemaßnahmen

Die 72-Stunden-Frist der Detailmeldung ist an die aufsichtsbehördliche Meldefrist des Art. 33 Abs. 1 DSGVO angelehnt, damit der Auftraggeber seine eigene Meldepflicht gegenüber der Aufsichtsbehörde fristgerecht erfüllen kann.

Ist kein Ansprechpartner benannt, erfolgt die Meldung an die im Vertrag hinterlegte E-Mail-Adresse.

§8 Rechte der betroffenen Personen

- (1) Der Auftragnehmer unterstützt den Auftraggeber nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen bei der Erfüllung seiner Pflichten gemäß Art. 12-23 DSGVO, insbesondere bei Anträgen betroffener Personen auf:
 - a) Auskunft (Art. 15 DSGVO),
 - b) Berichtigung (Art. 16 DSGVO),
 - c) Löschung (Art. 17 DSGVO),
 - d) Einschränkung der Verarbeitung (Art. 18 DSGVO),
 - e) Datenübertragbarkeit (Art. 20 DSGVO),
 - f) Widerspruch (Art. 21 DSGVO).
- (2) Wendet sich eine betroffene Person direkt an den Auftragnehmer, leitet dieser den Antrag unverzüglich an den Auftraggeber weiter. Der Auftragnehmer wird den Antrag nicht selbständig bescheiden, es sei denn, der Auftraggeber weist ihn ausdrücklich dazu an.
- (3) Der Auftragnehmer stellt dem Auftraggeber die zur Beantwortung erforderlichen Informationen unverzüglich, spätestens innerhalb von vier (4) Wochen nach Anfrage, zur Verfügung.

§9 Kontrollrechte des Auftraggebers

- (1) Der Auftraggeber hat das Recht, die Einhaltung dieses AVV und der datenschutzrechtlichen Vorschriften beim Auftragnehmer zu überprüfen (Art. 28 Abs. 3 lit. h DSGVO). Dies umfasst:
 - a) Einholung von Auskünften,
 - b) Einsichtnahme in relevante Dokumentationen und Nachweise,
 - c) Vor-Ort-Inspektionen der Geschäftsräume und Datenverarbeitungsanlagen.
- (2) Vor-Ort-Inspektionen sind mit einer Vorlaufzeit von **4 Wochen** anzukündigen und während der üblichen Geschäftszeiten durchzuführen. Sie finden **höchstens einmal je Kalenderjahr** statt; weitergehende Inspektionen sind nur bei begründetem konkreten Anlass zulässig. Der Auftragnehmer kann verlangen, dass die Prüfer einer Vertraulichkeitsvereinbarung unterliegen.
- (3) Der Auftragnehmer stellt dem Auftraggeber alle erforderlichen Informationen zum Nachweis der Einhaltung der in Art. 28 DSGVO niedergelegten Pflichten zur Verfügung und ermöglicht Überprüfungen einschließlich Inspektionen.
- (4) Vor-Ort-Inspektionen gemäß Abs. 1 lit. c sind **ausgeschlossen**, soweit der Auftraggeber durch Vorlage geeigneter Zertifizierungen, Prüfberichte oder Testate unabhängiger Dritter oder durch schriftliche Fragebogen-Auskunft des Auftragnehmers den Nachweis der Einhaltung prüfen kann. Inspektionen vor Ort sind nur zulässig, wenn diese Nachweise im Einzelfall nicht ausreichen oder ein begründeter konkreter Verdacht auf Verstöße gegen diesen AVV besteht.
- (5) Die Kosten einer Vor-Ort-Inspektion trägt der Auftraggeber, es sei denn, die Inspektion ergibt wesentliche Verstöße gegen diesen AVV.

§10 Beendigung -- Löschung und Rückgabe

- (1) Nach Beendigung des Vertragsverhältnisses ist der Auftragnehmer verpflichtet, sämtliche im Auftrag verarbeiteten personenbezogenen Daten nach Wahl des Auftraggebers:
 - a) in einem gängigen, maschinenlesbaren Format an den Auftraggeber zurückzugeben, **oder**
 - b) datenschutzkonform zu löschen und die Löschung in Textform zu bestätigen.
- (2) Der Auftraggeber teilt seine Wahl innerhalb von **30 Tagen** nach Vertragsende mit. Erfolgt keine Mitteilung, löscht der Auftragnehmer die Daten.
- (3) Die Löschung bzw. Rückgabe hat innerhalb von **30 Tagen** nach Vertragsende bzw. nach Mitteilung des Auftraggebers zu erfolgen. Der Auftragnehmer bestätigt die vollständige Löschung in Textform.
- (4) Bestehende gesetzliche Aufbewahrungspflichten bleiben unberührt. In diesen Fällen werden die Daten gesperrt und nach Ablauf der Aufbewahrungsfrist gelöscht. Der Auftragnehmer informiert den Auftraggeber über Art und Umfang der aufzubewahrenden Daten.
- (5) Bestehende Datensicherungen (Backups) werden im Rahmen der regulären Backup-Rotation überschrieben, spätestens jedoch innerhalb von **180 Tagen** nach Vertragsende gelöscht. Die Frist trägt den bestehenden Rolling-Rotation-Zyklen der eingesetzten Backup-Systeme Rechnung; eine frühere Löschung einzelner Backup-Stände ist aus technischen Gründen nicht zuverlässig möglich. Soweit für einen Service eine **unveränderbare Vorhaltung** von Sicherungen (Objektsperre/Immutabilität) mit einer längeren Aufbewahrungsdauer vereinbart ist, tritt an die Stelle der Frist nach Satz 1 der Ablauf der jeweils vereinbarten Aufbewahrungsdauer. Solche Sicherungen sind technisch gegen vorzeitige Löschung geschützt; sie werden nach Fristablauf automatisiert gelöscht. Die jeweilige Aufbewahrungsdauer ergibt sich aus der produktspezifischen Anlage.
- (6) Die Einrede des Zurückbehaltungsrechts im Sinne des § 273 BGB wird im Hinblick auf die verarbeiteten Daten des Auftraggebers ausgeschlossen.
- (7) Dokumentationen, die dem Nachweis der ordnungsgemäßen Datenverarbeitung dienen (insb. Weisungsdokumentation, Löschartikel, Audit-Ergebnisse), werden nach den gesetzlichen

Verjährungs- und Aufbewahrungsfristen (insb. § 195 BGB, § 147 AO, § 257 HGB) aufbewahrt, soweit dies zur Abwehr von Ansprüchen oder zur Nachweisführung gegenüber Aufsichtsbehörden erforderlich ist. Anschließend werden sie datenschutzkonform gelöscht.

§11 Vertraulichkeit

- (1) Beide Parteien sind verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäfts- und Betriebsgeheimnissen sowie Datensicherheitsmaßnahmen der jeweils anderen Partei auch über die Beendigung des Vertrages vertraulich zu behandeln.
- (2) Diese Vertraulichkeitspflicht gilt nicht für Informationen, die öffentlich bekannt sind oder werden, ohne dass die empfangende Partei dies zu vertreten hat, oder die der empfangenden Partei nachweislich bereits vor der Offenlegung bekannt waren.

§12 Haftung

- (1) Die Haftung der Parteien richtet sich nach Art. 82 DSGVO. Jede an einer Verarbeitung beteiligte Partei haftet für den Schaden, der durch eine nicht DSGVO-konforme Verarbeitung verursacht wird.
- (2) Im Innenverhältnis haftet der Auftragnehmer nur für Schäden, die durch eine ihm zurechenbare, nicht den Weisungen des Auftraggebers entsprechende Verarbeitung verursacht wurden. Im Einzelnen gilt:
 - a) Der Auftragnehmer trägt die Verantwortung für Schäden, die durch Verstöße gegen seine Pflichten aus diesem AVV oder gegen spezifisch an Auftragsverarbeiter gerichtete Pflichten der DSGVO verursacht wurden.
 - b) Der Auftraggeber trägt die Verantwortung für Schäden, die durch rechtswidrige Weisungen oder durch Verstöße gegen seine Pflichten als Verantwortlicher verursacht wurden.
- (3) Die Haftung des Auftragnehmers für Schäden aus diesem AVV – mit Ausnahme von Vorsatz, grober Fahrlässigkeit sowie Schäden aus der Verletzung des Lebens, des Körpers oder der Gesundheit – ist auf die Obergrenzen des §7 Abs. 8 der AGB in ihrer jeweils einschlägigen Höhe (einschließlich der dortigen volumenabhängigen Staffel) begrenzt. Unmittelbare Ansprüche betroffener Personen nach Art. 82 DSGVO bleiben unberührt; im Innenverhältnis zwischen Auftraggeber und Auftragnehmer gelten die vorstehenden Obergrenzen entsprechend. Eine im Einzelauftrag abweichend vereinbarte Haftungsobergrenze gilt vorrangig.
- (4) **Freistellung im Innenverhältnis:** Bei Inanspruchnahme des Auftragnehmers durch Betroffene nach Art. 82 DSGVO stellt der Auftraggeber den Auftragnehmer frei, soweit der Schaden auf einem Verstoß des Auftraggebers als Verantwortlicher, auf nicht-DSGVO-konformen Weisungen oder auf Umständen beruht, die dem Verantwortungsbereich des Auftraggebers zuzuordnen sind. Die Freistellung umfasst auch zumutbare Rechtsverteidigungskosten.
- (5) Etwaige Haftungsbeschränkungen aus dem zugrunde liegenden Vertragsverhältnis (insb. §7 AGB) finden ergänzend Anwendung, soweit sie nicht im Widerspruch zu zwingenden Bestimmungen der DSGVO stehen.
- (6) Im Falle eines Anspruchs nach Art. 82 DSGVO trägt im Innenverhältnis jede Partei den Anteil des Schadens, der ihrem jeweiligen Verschuldensbeitrag entspricht. Die Parteien bemühen sich um eine einvernehmliche Regelung. Die Partei, die von einer betroffenen Person in Anspruch genommen wird, informiert die andere Partei unverzüglich.

§13 KI-Transparenzpflichten

- (1) Soweit der Auftragnehmer im Rahmen der beauftragten Leistungen KI-Systeme einsetzt, gelten ergänzend die Transparenzpflichten der Verordnung (EU) 2024/1689 (EU AI Act). Es wird zwischen folgenden KI-Kategorien unterschieden:
 - a) **Lokale KI-Systeme (Trainings- und Inference-KI):** KI-Modelle (z.B. Large Language Models), die auf der Infrastruktur des Auftragnehmers oder des Auftraggebers betrieben werden. Kundendaten werden ausschließlich lokal verarbeitet.
 - b) **Integrierte KI-Funktionen in Drittanbieter-Diensten:** KI-Funktionen, die Bestandteil eingesetzter Drittanbieter-Plattformen sind. Für diese gelten die Datenschutzbestimmungen des jeweiligen Dienstleisters gemäß Anlage 3.
 - c) **Keine Nutzung externer KI-Dienste mit Kundendaten:** Der Auftragnehmer übermittelt keine Kundendaten an eigenständige externe KI-Dienste (z.B. allgemeine Large-Language-Model-Dienste) zum Zweck der Verarbeitung.
- (2) Der Auftragnehmer gewährleistet:
 - a) Die Verarbeitung personenbezogener Daten durch lokale KI-Systeme (Abs. 1 lit. a) erfolgt ausschließlich auf der Infrastruktur des Auftragnehmers oder des Auftraggebers. Es findet keine Übermittlung von Kundendaten an externe KI-Anbieter statt.
 - b) Der Auftragnehmer informiert den Auftraggeber vor Erstnutzung transparent über den Einsatz von KI-Systemen, deren Art (lokal/integriert), Zweck, die verarbeiteten Datenkategorien und ob ein Training mit Kundendaten stattfindet.
 - c) Bei der Integration von KI-Systemen, die als hochriskant i.S.d. Verordnung (EU) 2024/1689 einzustufen sind, werden Risikobewertungen durchgeführt.
 - d) Entscheidungen, die ausschließlich auf automatisierter Verarbeitung beruhen und rechtliche Wirkung entfalten, unterliegen menschlicher Überprüfung (Art. 22 DSGVO).
 - e) Kundendaten werden nicht zum Training von KI-Modellen verwendet, es sei denn, der Auftraggeber hat dem ausdrücklich zugestimmt.
- (3) Der Auftragnehmer dokumentiert den Einsatz von KI-Systemen und stellt dem Auftraggeber auf Anfrage Informationen zur Funktionsweise und Datenverarbeitung zur Verfügung.

§14 Schlussbestimmungen

- (1) Änderungen und Ergänzungen dieses AVV bedürfen der Textform. Der Auftragnehmer kann Änderungen gemäß dem Verfahren in §1 Abs. 3 vornehmen.
- (2) Sollten einzelne Bestimmungen dieses AVV unwirksam sein oder werden, so wird hierdurch die Wirksamkeit des AVV im Übrigen nicht berührt. Die Parteien verpflichten sich, die unwirksame Bestimmung durch eine wirksame Regelung zu ersetzen, die dem wirtschaftlichen und rechtlichen Zweck der unwirksamen Bestimmung möglichst nahe kommt.
- (3) Es gilt das Recht der Bundesrepublik Deutschland. Gerichtsstand ist Hannover.
- (4) Dieser AVV geht im Konfliktfall den Regelungen des zugrunde liegenden Vertrages in Bezug auf den Datenschutz vor.
- (5) Der Auftraggeber bestätigt, dass er den AVV in seiner jeweils aktuellen Fassung unter [ext-it.tech/avv](https://www.ext-it.tech/avv) zur Kenntnis genommen hat.
- (6) **NIS2-Konformität:** Soweit der Auftraggeber oder der Auftragnehmer den Anforderungen des NIS2-Umsetzungsgesetzes (NIS2UmsuCG) unterliegt, gelten ergänzend folgende Verpflichtungen:
 - a) Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in § 30 BSIG n.F. genannten Risikomanagementmaßnahmen, soweit diese die vom Auftragnehmer erbrachten Leistungen betreffen.
 - b) Der Auftragnehmer meldet dem Auftraggeber erhebliche Sicherheitsvorfälle i.S.d. § 32 BSIG n.F. unverzüglich. Soweit der Auftraggeber selbst NIS2-verpflichtet ist und der Vorfall für dessen gesetzliche Meldepflicht relevant ist, erfolgt die Erstmeldung in der

Regel innerhalb von **24 Stunden**; in allen übrigen Fällen innerhalb von **48 Stunden**. Die Detailmeldung erfolgt in der Regel innerhalb von **72 Stunden**.

- c) Der Auftragnehmer gewährleistet die Sicherheit der Lieferkette gemäß § 30 Abs. 2 Nr. 4 BStG n.F. durch vertragliche Verpflichtung seiner Unterauftragsverarbeiter.
- d) Die konkreten technischen und organisatorischen Maßnahmen zur NIS2-Konformität sind in Anlage 1 (TOMs), Abschnitt 7, dokumentiert.

Anlagen

Alle Anlagen zu diesem AVV sind unter ext-it.tech/avv abrufbar:

- **Anlage 1** – Technische und Organisatorische Maßnahmen (TOMs)
- **Produktspezifische Anlagen** – Je beauftragtem Service eine eigenständige Anlage, die Gegenstand, Datenkategorien, Unterauftragsverarbeiter und servicespezifische Regelungen enthält
- **Anlage 3** – Zentrale Unterauftragsverarbeiter-Liste – Konsolidierte Übersicht aller Unterauftragsverarbeiter gemäß Art. 28 Abs. 4 DSGVO

Änderungshistorie

Version	Datum	Änderung	Verantwortlich
1.2	2026-08-12	Interne Dokumentenprüfung vom 12.08.2026 eingearbeitet: § 10 Abs. 5 um eine Ausnahme für unveränderbar vorgehaltene Sicherungen ergänzt – die 180-Tage-Frist war bei SaaS Backup und Managed Backup technisch nicht einhaltbar.	Geschäftsführung
1.1	2026-08-01	§6 Abs. 10 auf Colocation/Housing (Hardware des Auftraggebers in Räumlichkeiten des Hosting-Dienstleisters) erstreckt; §12 Abs. 3 dynamisch an die Haftungsobergrenzen des §7 Abs. 8 AGB gekoppelt (beseitigt die Diskrepanz zur volumenabhängigen Staffel)	Geschäftsführung
1.0	2026-04-21	Erstveröffentlichung	Geschäftsführung

Stand: 2026-08-12