Vertrag über die Verarbeitung personenbezogener Daten im Auftrag

Auftragsverarbeitungsvertrag (AVV) gemäß Art. 28 DSGVO

zwischen

Firma des Auftraggebers

Straße und Hausnummer

PLZ und Ort

Vertreten durch: …

– nachstehend „Auftraggeber" oder „Verantwortlicher" genannt –

und

E-PROJECTA GmbH

In der Täschen 20/1

72336 Balingen

Vertreten durch den Geschäftsführer Marc Eberhart

– nachstehend „Auftragnehmer" oder „Auftragsverarbeiter" genannt –

– gemeinsam die „Parteien" –

Fassung **2.0** · Stand **01.09.2026**

Präambel

Der Auftragnehmer erbringt für den Auftraggeber auf Grundlage eines gesonderten Vertragsverhältnisses (nachfolgend „Hauptvertrag") Leistungen in den Bereichen IT, Software-Entwicklung und Consulting, insbesondere Managed Services, Betrieb, Wartung und Support von Hard- und Software, Individual- und Weiterentwicklung von Software sowie damit verbundene Beratungs- und Cloud-Leistungen.

Im Rahmen dieser Leistungserbringung verarbeitet der Auftragnehmer personenbezogene Daten im Auftrag und nach Weisung des Auftraggebers im Sinne des Art. 4 Nr. 8 und Art. 28 DSGVO. Dieser Vertrag konkretisiert die datenschutzrechtlichen Rechte und Pflichten der Parteien und erfüllt die Anforderungen des Art. 28 Abs. 3 DSGVO.

Soweit in diesem Vertrag Begriffe der Datenschutz-Grundverordnung (Verordnung (EU) 2016/679, nachfolgend „DSGVO") verwendet werden, gelten die Begriffsbestimmungen des Art. 4 DSGVO. Ergänzend gelten die Vorschriften des Bundesdatenschutzgesetzes (BDSG) sowie des Landesdatenschutzgesetzes Baden-Württemberg (LDSG BW), soweit anwendbar.

Ansprechpartner für den Datenschutz

	AUFTRAGGEBER	AUFTRAGNEHMER
Ansprechpartner Datenschutz	**Name**	**Daniel Lohmüller**
Funktion	**Funktion**	**Kaufm. Mitarbeiter**
Datenschutzbeauftragter (Art. 37 DSGVO)	**benannt / nicht benannt – Name, Kontakt**	**Reiner Braun**
E-Mail	info@e-projecta.com	datenschutz@e-projecta.com
Telefon	07433 99934-0	07433 99934-0
Meldeweg Sicherheitsvorfälle (24/7)	**Kontakt**	**Kontakt / Ticketsystem**

Änderungen der vorstehenden Angaben teilen sich die Parteien unverzüglich in Textform mit. Eine Änderung dieser Tabelle bedarf keiner Vertragsänderung.

§ 1 Gegenstand, Rangfolge und Geltungsbereich

(1) Gegenstand dieses Vertrages ist die Verarbeitung personenbezogener Daten durch den Auftragnehmer im Auftrag des Auftraggebers im Zusammenhang mit den im Hauptvertrag vereinbarten Leistungen.

(2) Dieser Vertrag gilt für sämtliche Leistungen, die der Auftragnehmer für den Auftraggeber erbringt und bei denen eine Verarbeitung personenbezogener Daten nicht ausgeschlossen werden kann. Er gilt auch

dann, wenn der Zugriff auf personenbezogene Daten nur gelegentlich, kurzfristig oder lediglich nicht ausgeschlossen erfolgt (Art. 4 Nr. 2 DSGVO).

(3) Bei Widersprüchen zwischen den Regelungen dieses Vertrages, dem Hauptvertrag und etwaigen Allgemeinen Geschäftsbedingungen gilt für datenschutzrechtliche Fragen die folgende Rangfolge: 1. dieser Vertrag einschließlich seiner Anlagen, 2. der Hauptvertrag, 3. Allgemeine Geschäftsbedingungen. Innerhalb dieses Vertrages geht der Vertragstext den Anlagen vor, soweit nicht ausdrücklich etwas anderes bestimmt ist.

(4) Die Anlagen 1 bis 3 sind Bestandteil dieses Vertrages. Soweit Anlagen zusätzlich in jeweils aktueller Fassung online bereitgestellt werden, ist für den Vertragsschluss die diesem Vertrag beigefügte Fassung maßgeblich; die Online-Fassung dient der Fortschreibung nach Maßgabe von § 7 Abs. 4 und § 10 Abs. 3.

§ 2 Art, Umfang und Zweck der Verarbeitung

(1) Art und Zweck der Verarbeitung

Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich zum Zweck der Erbringung der im Hauptvertrag vereinbarten Leistungen. Dies umfasst insbesondere:

- sämtliche Tätigkeiten zur Sicherstellung und Wiederherstellung der Betriebsbereitschaft der Hard- und Software des Auftraggebers;
- Installation, Einrichtung, Konfiguration, Migration, Wartung und Pflege von Hard- und Software-Produkten einschließlich Cloud-Diensten;
- Anwender-, System- und Applikationssupport (First-, Second- und Third-Level) einschließlich Fehleranalyse und Störungsbeseitigung;
- Betrieb, Überwachung und Administration von IT-Systemen, Netzwerken, Datensicherungen und Sicherheitslösungen (Managed Services, Monitoring, Backup, Security Operations);
- Bereitstellung und Administration von Cloud- und Hosting-Leistungen;
- Entwicklung, Anpassung, Test und Einführung von Individual- und Standardsoftware sowie Integrations- und Schnittstellenleistungen;
- Datenmigrationen, Auswertungen und Analysen auf Anforderung des Auftraggebers;
- Schulungen, Trainings und Anwenderbegleitung;
- Marketingaktionen, Messen und Veranstaltungen

Die Tätigkeiten werden vor Ort beim Auftraggeber, aus den Betriebsstätten des Auftragnehmers, im Wege des Fernzugriffs (§ 8) sowie – nach Maßgabe der internen Richtlinien des Auftragnehmers – aus dem mobilen Arbeiten bzw. Homeoffice erbracht.

Zur Aufrechterhaltung der Betriebsbereitschaft kann es erforderlich sein, Daten, Datenbanken oder Konfigurationen des Auftraggebers vorübergehend in die Systemumgebung des Auftragnehmers zu übernehmen (z. B. zur Fehleranalyse oder Testinstallation). Diese Verarbeitung erfolgt ausschließlich zweckgebunden, mandantengetrennt und nur für die erforderliche Dauer; anschließend werden die Daten datenschutzgerecht gelöscht.

(2) Kategorien personenbezogener Daten

Gegenstand der Verarbeitung können insbesondere folgende Datenkategorien sein:

- Stamm-, Adress- und Kontaktdaten;
- Vertragsstamm-, Abrechnungs- und Zahlungsdaten;
- Nutzungs-, Verkehrs- und Bestandsdaten, Protokoll- und Metadaten;
- Kommunikationsdaten (E-Mail, Telefonie, Messaging, Ticketinhalte);
- Kunden- und Vorgangshistorie;
- personenbezogene Daten von Beschäftigten des Auftraggebers, einschließlich Zugangs-, Berechtigungs- und Anwesenheitsdaten;
- personenbezogene Daten von Geschäftspartnern, Kunden, Interessenten und Lieferanten des Auftraggebers sowie dessen Erfüllungsgehilfen.

(3) Besondere Kategorien personenbezogener Daten (Art. 9 DSGVO), Daten über strafrechtliche Verurteilungen und Straftaten (Art. 10 DSGVO) sowie Daten, die einem Berufsgeheimnis nach § 203 StGB unterliegen, sind: nicht Gegenstand der Verarbeitung. Sofern derartige Daten Gegenstand der Verarbeitung sind, gelten die ergänzenden Regelungen in § 6 Abs. 4 und § 8 Abs. 5.

(4) Kategorien betroffener Personen

Von der Verarbeitung betroffen sind insbesondere:

- Beschäftigte, ehemalige Beschäftigte und Bewerber des Auftraggebers;
- Kunden, Interessenten und deren Ansprechpartner;
- Lieferanten, Dienstleister und deren Ansprechpartner;
- sonstige Geschäftspartner und Dritte, deren Daten der Auftraggeber verarbeitet.

§ 3 Weisungsrecht

(1) Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich auf dokumentierte Weisung des Auftraggebers, einschließlich hinsichtlich der Übermittlung in ein Drittland oder an eine internationale Organisation (Art. 28 Abs. 3 lit. a DSGVO). Dieser Vertrag einschließlich seiner Anlagen sowie der Hauptvertrag stellen die initiale und maßgebliche Weisung dar.

(2) Ergänzende Weisungen kann der Auftraggeber jederzeit erteilen. Weisungen sind in Textform (§ 126b BGB) zu erteilen; hierzu genügen E-Mail an die in der Ansprechpartnertabelle genannte Adresse sowie dokumentierte Vorgänge im Ticketsystem des Auftragnehmers. Mündlich erteilte Weisungen sind vom Auftraggeber unverzüglich in Textform zu bestätigen.

(3) Weisungsberechtigte Personen des Auftraggebers und weisungsempfangsberechtigte Personen bzw. Organisationseinheiten des Auftragnehmers sind in Anlage 3 benannt. Änderungen sind der jeweils anderen Partei unverzüglich in Textform mitzuteilen.

(4) Der Auftragnehmer dokumentiert erteilte Weisungen und bewahrt die Dokumentation für die Dauer des Vertragsverhältnisses sowie für drei Jahre nach dessen Beendigung auf, soweit nicht längere gesetzliche Aufbewahrungspflichten bestehen.

(5) Ist der Auftragnehmer der Auffassung, dass eine Weisung gegen datenschutzrechtliche Vorschriften verstößt, informiert er den Auftraggeber unverzüglich (Art. 28 Abs. 3 Satz 3 DSGVO). Der Auftragnehmer ist berechtigt, die Ausführung der betreffenden Weisung auszusetzen, bis diese durch den Auftraggeber in Textform bestätigt oder geändert wird. Bei offensichtlichem Rechtsverstoß ist der Auftragnehmer zur Ausführung nicht verpflichtet.

(6) Eine Verarbeitung außerhalb des Weisungsrahmens ist nur zulässig, soweit der Auftragnehmer hierzu nach Unionsrecht oder dem Recht eines Mitgliedstaats verpflichtet ist. In diesem Fall teilt der Auftragnehmer dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

(7) Führt eine Weisung zu Mehraufwand beim Auftragnehmer, der über die im Hauptvertrag vereinbarten Leistungen hinausgeht, gilt § 18.

§ 4 Pflichten des Auftraggebers

(1) Der Auftraggeber ist für die Rechtmäßigkeit der Verarbeitung sowie für die Wahrung der Rechte betroffener Personen allein verantwortlich (Art. 4 Nr. 7, Art. 24 DSGVO). Er stellt insbesondere sicher, dass für die Verarbeitung eine Rechtsgrundlage besteht und dass die Informationspflichten nach Art. 13, 14 DSGVO erfüllt sind.

(2) Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten im Zusammenhang mit der Verarbeitung personenbezogener Daten durch den Auftragnehmer feststellt.

(3) Der Auftraggeber überzeugt sich vor Beginn der Verarbeitung und sodann regelmäßig von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen. Er dokumentiert das Ergebnis in geeigneter Weise. Für den Nachweis gilt § 15.

(4) Die Erfüllung der Melde- und Benachrichtigungspflichten nach Art. 33, 34 DSGVO gegenüber der Aufsichtsbehörde und den betroffenen Personen obliegt dem Auftraggeber. Der Auftragnehmer unterstützt ihn hierbei nach Maßgabe von § 13.

(5) Der Auftraggeber teilt dem Auftragnehmer besondere Geheimhaltungspflichten, berufsrechtliche Vorgaben oder branchenspezifische Anforderungen (z. B. § 203 StGB, KRITIS-, NIS2- oder aufsichtsrechtliche Pflichten) rechtzeitig vor Beginn der Verarbeitung mit, damit der Auftragnehmer diese berücksichtigen kann.

(6) Der Auftraggeber stellt sicher, dass ihm überlassene Zugangsdaten, Berechtigungen und Fernzugriffsfreigaben nur an berechtigte Personen weitergegeben und bei Wegfall der Erforderlichkeit unverzüglich entzogen werden.

§ 5 Allgemeine Pflichten des Auftragnehmers

(1) Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich im Rahmen dieses Vertrages und der erteilten Weisungen. Zweck, Art und Umfang der Verarbeitung richten sich ausschließlich nach diesem Vertrag und den Weisungen des Auftraggebers.

(2) Der Auftragnehmer gestaltet seine Betriebsabläufe so, dass die im Auftrag verarbeiteten Daten im erforderlichen Maß gesichert und vor unbefugter Kenntnisnahme Dritter geschützt sind. Wesentliche

Änderungen in der Organisation der Auftragsverarbeitung, die für die Sicherheit der Daten erheblich sind, stimmt er vorab mit dem Auftraggeber ab.

(3) Der Auftragnehmer führt ein Verzeichnis aller Kategorien von Verarbeitungstätigkeiten im Auftrag nach Art. 30 Abs. 2 DSGVO und stellt es dem Auftraggeber auf Anforderung zur Verfügung.

(4) Der Auftragnehmer unterstützt den Auftraggeber bei der Erstellung und Pflege des Verzeichnisses von Verarbeitungstätigkeiten nach Art. 30 Abs. 1 DSGVO, indem er die datenschutzrelevanten Informationen zu seinen Leistungen in standardisierter Form bereitstellt.

(5) Der Auftragnehmer benennt den Status seines betrieblichen Datenschutzbeauftragten in der Ansprechpartnertabelle. Sofern ein Datenschutzbeauftragter benannt ist, sind dessen aktuelle Kontaktdaten auf der Internetseite des Auftragnehmers leicht zugänglich hinterlegt.

(6) Der Auftragnehmer stellt sicher, dass die mit der Verarbeitung befassten Personen ausschließlich nach dem Grundsatz der Erforderlichkeit („need to know") Zugriff auf personenbezogene Daten des Auftraggebers erhalten.

(7) Der Auftragnehmer trennt die Daten des Auftraggebers logisch von Daten anderer Auftraggeber sowie von eigenen Daten (Mandantentrennung). Sofern Daten zu unterschiedlichen Zwecken verarbeitet werden, erfolgt eine getrennte Verarbeitung.

(8) Der Auftragnehmer teilt dem Auftraggeber unverzüglich mit, wenn eine Aufsichtsbehörde nach Art. 58 DSGVO ihm gegenüber tätig wird und dies auch die Verarbeitung im Auftrag des Auftraggebers betreffen kann.

(9) Der Auftragnehmer informiert den Auftraggeber unverzüglich, wenn Eigentum oder Daten des Auftraggebers beim Auftragnehmer durch Maßnahmen Dritter (etwa Pfändung, Beschlagnahme, behördliche Anordnung), durch ein Insolvenzverfahren oder durch sonstige Ereignisse gefährdet werden. Der Auftragnehmer weist Dritte unverzüglich darauf hin, dass es sich um im Auftrag verarbeitete Daten handelt.

(10) Der Auftragnehmer unterhält eine Betriebs- und Vermögensschadenhaftpflichtversicherung sowie eine Cyber-Versicherung mit einer Deckungssumme von mindestens 1 Mio. EUR je Schadensfall und weist dies dem Auftraggeber auf Anforderung nach.

§ 6 Vertraulichkeit und Verpflichtung der Beschäftigten

(1) Der Auftragnehmer wahrt über alle Daten, die er im Zusammenhang mit dem Auftrag erhält oder zur Kenntnis erlangt, Vertraulichkeit. Diese Verpflichtung besteht auch nach Beendigung des Vertrages zeitlich unbegrenzt fort.

(2) Der Auftragnehmer stellt sicher, dass sich alle zur Verarbeitung befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen (Art. 28 Abs. 3 lit. b DSGVO). Die Verpflichtung erfolgt in Textform, überdauert das Beschäftigungsverhältnis und ist dem Auftraggeber auf Anforderung nachzuweisen.

(3) Der Auftragnehmer macht die mit der Verarbeitung befassten Personen vor Aufnahme der Tätigkeit und danach in angemessenen Abständen, mindestens jedoch jährlich, mit den maßgeblichen datenschutz- und informationssicherheitsrechtlichen Anforderungen vertraut (Awareness-Schulung) und dokumentiert dies.

(4) Unterliegt der Auftraggeber einer Berufsgeheimnispflicht nach § 203 StGB, so ist dem Auftragnehmer bekannt, dass er als „sonstige mitwirkende Person" im Sinne des § 203 Abs. 3 StGB unmittelbar strafbewehrt zur Verschwiegenheit verpflichtet ist. Der Auftragnehmer verpflichtet in diesem Fall alle mitwirkenden Personen sowie eingeschaltete Unterauftragnehmer nach § 203 Abs. 4 StGB zur Geheimhaltung und weist dies dem Auftraggeber auf Anforderung nach. Der Auftraggeber informiert den Auftragnehmer über das Bestehen einer solchen Pflicht (§ 4 Abs. 5).

(5) Wirkt der Auftragnehmer im Zusammenhang mit Leistungen für den Auftraggeber an der Erbringung von Telekommunikations- oder digitalen Diensten mit, verpflichtet er die beteiligten Beschäftigten zusätzlich auf das Fernmeldegeheimnis nach § 3 TDDDG.

(6) Die Vertraulichkeitspflicht gilt nicht für Informationen, die nachweisbar öffentlich bekannt sind, die eine Partei von Dritten ohne Geheimhaltungsverpflichtung erhalten hat oder deren Offenlegung gesetzlich oder behördlich angeordnet ist; im letzteren Fall informiert die offenlegende Partei die andere Partei vorab, soweit rechtlich zulässig.

§ 7 Technische und organisatorische Maßnahmen

(1) Der Auftragnehmer trifft unter Berücksichtigung des Stands der Technik, der Implementierungskosten sowie der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung und der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen die erforderlichen technischen und organisatorischen Maßnahmen nach Art. 32 DSGVO.

(2) Der zum Zeitpunkt des Vertragsschlusses maßgebliche Stand der technischen und organisatorischen Maßnahmen ist in Anlage 2 dokumentiert. Die dort beschriebenen Maßnahmen sind verbindlich vereinbart.

(3) Die Maßnahmen unterliegen dem technischen Fortschritt. Der Auftragnehmer ist berechtigt, alternative, gleichwertige Maßnahmen umzusetzen. Das vereinbarte Schutzniveau darf dabei nicht unterschritten werden. Wesentliche Änderungen dokumentiert der Auftragnehmer und teilt sie dem Auftraggeber unaufgefordert in Textform mit.

(4) Der Auftragnehmer stellt die Dokumentation der Maßnahmen in jeweils aktueller, versionierter Fassung unter https://www.e-projecta.com/AV/TOM.pdf bereit. Für den Vertragsschluss maßgeblich ist die als Anlage 2 beigefügte Fassung; spätere Fassungen werden Vertragsbestandteil, wenn sie das vereinbarte Schutzniveau mindestens wahren und dem Auftraggeber mitgeteilt wurden.

(5) Der Auftragnehmer überprüft die Wirksamkeit der Maßnahmen regelmäßig, mindestens jährlich, sowie anlassbezogen (Art. 32 Abs. 1 lit. d DSGVO) und dokumentiert die Überprüfung. Besteht Optimierungs- oder Änderungsbedarf mit Auswirkung auf die Leistungen für den Auftraggeber, informiert er diesen.

(6) Der Auftragnehmer berücksichtigt bei der Ausgestaltung seiner Leistungen die Grundsätze des Datenschutzes durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen (Art. 25 DSGVO), soweit die Gestaltung in seinem Verantwortungsbereich liegt.

§ 8 Fernzugriff, Fernwartung und administrative Zugriffe

(1) Der Auftragnehmer erbringt Wartungs-, Pflege- und Supportleistungen auch im Wege des Fernzugriffs. Der Fernzugriff erfolgt ausschließlich über die vereinbarte, dem Stand der Technik

entsprechende Fernwartungslösung (**Teamviewer**) unter Verwendung verschlüsselter Verbindungen und Mehr-Faktor-Authentifizierung.

(2) Der Auftraggeber behält die Kontrolle über den Fernzugriff. Der Zugriff auf Arbeitsplatzsysteme mit Anwenderbezug erfolgt grundsätzlich erst nach aktiver Freigabe durch den Auftraggeber bzw. den betroffenen Anwender; dieser kann die Sitzung jederzeit beenden und den Bildschirminhalt mitverfolgen. Für unbeaufsichtigte Zugriffe auf Serversysteme und Infrastrukturkomponenten gilt Absatz 3.

(3) Unbeaufsichtigte administrative Zugriffe sind zulässig, soweit sie zur Erbringung der vereinbarten Leistungen erforderlich sind. Sie erfolgen über personalisierte, von Standardbenutzerkonten getrennte administrative Konten mit Mehr-Faktor-Authentifizierung. Der Auftragnehmer protokolliert Zeitpunkt, Dauer, handelnde Person, betroffenes System und Anlass (Ticketbezug) der Zugriffe manipulationsgeschützt und stellt die Protokolle dem Auftraggeber auf Anforderung zur Verfügung.

(4) Zugangsdaten des Auftraggebers werden ausschließlich in einem verschlüsselten Passwort-Management-System des Auftragnehmers gespeichert; ein Zugriff erfolgt nur nach dem Grundsatz der Erforderlichkeit und wird protokolliert.

(5) Unterliegt der Auftraggeber einer Berufsgeheimnispflicht nach § 203 StGB, setzt der Auftragnehmer ausschließlich Technologien ein, die dem Auftraggeber sowohl das Mitverfolgen der Tätigkeit als auch die jederzeitige Unterbrechung der Sitzung ermöglichen. Die Parteien treffen ergänzend organisatorische Maßnahmen, um eine unbefugte Offenbarung auszuschließen.

(6) Der Auftragnehmer dokumentiert die durchgeführten Arbeiten nachvollziehbar im Ticketsystem.

§ 9 Einsatz von KI-Systemen und automatisierten Analysewerkzeugen

(1) Der Auftragnehmer setzt im Rahmen der Leistungserbringung KI-Systeme im Sinne des Art. 3 Nr. 1 der Verordnung (EU) 2024/1689 (KI-Verordnung) sowie sonstige automatisierte Analyse- und Assistenzwerkzeuge nur ein, soweit dies nachfolgend geregelt oder vom Auftraggeber gesondert in Textform genehmigt ist.

(2) Ein Einsatz von KI-Systemen, bei dem personenbezogene Daten des Auftraggebers verarbeitet werden, ist: vereinbart für folgende Anwendungsfälle: Prüfung der Richtigkeit der Daten, Abgleich mit Bestandsdaten, Unternehmensportal (z.B: NorthData). Die eingesetzten Anbieter werden als Unterauftragnehmer in Anlage 1 geführt.

(3) Soweit ein Einsatz vereinbart ist, stellt der Auftragnehmer sicher, dass die eingesetzten Anbieter die überlassenen Daten nicht zum Training oder zur Verbesserung ihrer Modelle verwenden, dass die Verarbeitung nach Maßgabe von § 11 erfolgt und dass die Speicherdauer beim Anbieter auf das erforderliche Maß begrenzt ist.

(4) Ergebnisse von KI-Systemen werden vor ihrer Verwendung durch fachkundige Beschäftigte des Auftragnehmers geprüft. Eine ausschließlich auf einer automatisierten Verarbeitung beruhende Entscheidung mit rechtlicher Wirkung oder ähnlich erheblicher Beeinträchtigung betroffener Personen im Sinne des Art. 22 DSGVO findet nicht statt.

(5) Der Auftragnehmer stellt sicher, dass die mit dem Einsatz von KI-Systemen befassten Beschäftigten über ein ausreichendes Maß an KI-Kompetenz im Sinne des Art. 4 der KI-Verordnung verfügen.

§ 10 Unterauftragsverhältnisse

(1) Der Auftraggeber erteilt dem Auftragnehmer die allgemeine schriftliche Genehmigung im Sinne des Art. 28 Abs. 2 Satz 2 DSGVO, weitere Auftragsverarbeiter (Unterauftragnehmer) einzusetzen. Die zum Zeitpunkt des Vertragsschlusses eingesetzten Unterauftragnehmer sind in Anlage 1 aufgeführt und werden hiermit genehmigt.

(2) Der Auftragnehmer informiert den Auftraggeber über jede beabsichtigte Hinzuziehung oder Ersetzung eines Unterauftragnehmers mindestens **30** Kalendertage vor der beabsichtigten Änderung in Textform.

(3) Der Auftraggeber kann der Änderung innerhalb von **14** Kalendertagen nach Zugang der Information aus wichtigem, datenschutzrechtlich begründetem Anlass in Textform widersprechen. Im Falle eines Widerspruchs suchen die Parteien zunächst eine einvernehmliche Lösung. Kommt eine solche nicht binnen **30** Kalendertagen zustande und kann der Auftragnehmer die Leistung ohne den betreffenden Unterauftragnehmer nicht in zumutbarer Weise erbringen, steht beiden Parteien hinsichtlich der betroffenen Leistung ein Sonderkündigungsrecht mit einer Frist von **drei Monaten** zum Monatsende zu.

(4) Der Auftragnehmer wählt den Unterauftragnehmer sorgfältig aus und prüft vor der Beauftragung sowie danach regelmäßig, dass dieser die nach Art. 32 DSGVO erforderlichen technischen und organisatorischen Maßnahmen getroffen hat. Das Ergebnis der Prüfung dokumentiert er und übermittelt es dem Auftraggeber auf Anfrage.

(5) Der Auftragnehmer schließt mit dem Unterauftragnehmer einen Vertrag, der den Anforderungen des Art. 28 DSGVO entspricht und dem Unterauftragnehmer dieselben Datenschutzpflichten auferlegt, die zwischen Auftraggeber und Auftragnehmer vereinbart sind (Art. 28 Abs. 4 DSGVO). Der Vertrag ist dem Auftraggeber auf Anfrage in Kopie – erforderlichenfalls in geschwärzter Fassung hinsichtlich kommerzieller Angaben – zu übermitteln.

(6) Der Auftragnehmer stellt vertraglich sicher, dass die Kontrollbefugnisse nach § 15 sowie die Befugnisse der Aufsichtsbehörden auch gegenüber dem Unterauftragnehmer gelten und dass dieser Kontrollmaßnahmen einschließlich Vor-Ort-Kontrollen zu dulden hat.

(7) Kommt der Unterauftragnehmer seinen Datenschutzpflichten nicht nach, haftet der Auftragnehmer gegenüber dem Auftraggeber für die Einhaltung der Pflichten des Unterauftragnehmers (Art. 28 Abs. 4 Satz 2 DSGVO).

(8) Keine Unterauftragsverhältnisse im Sinne der Absätze 1 bis 7 sind Nebenleistungen Dritter, die der Auftragnehmer zur Ausübung seiner geschäftlichen Tätigkeit in Anspruch nimmt und die keinen Bezug zu den für den Auftraggeber erbrachten Leistungen aufweisen, insbesondere Reinigungsleistungen, reine Telekommunikationsleistungen, Post- und Kurierdienste, Transport- und Bewachungsdienste sowie Buchhaltungs- und Steuerberatungsleistungen des Auftragnehmers. Auch bei diesen Leistungen trifft der Auftragnehmer angemessene Vorkehrungen zum Schutz personenbezogener Daten. Wartungs-, Prüf- und Supportleistungen Dritter an IT-Systemen, die auch zur Leistungserbringung für den Auftraggeber genutzt werden, stellen demgegenüber genehmigungspflichtige Unterauftragsverhältnisse dar.

§ 11 Verarbeitungsorte und Datenübermittlung in Drittländer

(1) Die Verarbeitung personenbezogener Daten erfolgt grundsätzlich in Mitgliedstaaten der Europäischen Union oder in Vertragsstaaten des Abkommens über den Europäischen Wirtschaftsraum. Die Verarbeitungsorte sind in Anlage 1 angegeben.

(2) Eine Verarbeitung in einem Drittland ist nur zulässig, wenn die Voraussetzungen der Art. 44 bis 49 DSGVO erfüllt sind, insbesondere auf Grundlage

- eines Angemessenheitsbeschlusses der Europäischen Kommission nach Art. 45 DSGVO (einschließlich einer Zertifizierung nach dem EU-US Data Privacy Framework für Empfänger in den Vereinigten Staaten) oder
- geeigneter Garantien nach Art. 46 DSGVO, insbesondere der Standardvertragsklauseln der Europäischen Kommission (Durchführungsbeschluss (EU) 2021/914) in der jeweils maßgeblichen Modulvariante, ergänzt um erforderliche zusätzliche Maßnahmen.

(3) Der Auftragnehmer führt vor Aufnahme einer Drittlandverarbeitung eine Risikobewertung der Übermittlung (Transfer Impact Assessment) durch, dokumentiert diese und stellt sie dem Auftraggeber auf Anforderung zur Verfügung.

(4) Der Auftraggeber erteilt dem Auftragnehmer die Weisung, Drittlandübermittlungen nach Maßgabe der Absätze 2 und 3 vorzunehmen, soweit sie zur Erbringung der vereinbarten Leistungen erforderlich und in Anlage 1 ausgewiesen sind. Für Änderungen gilt § 10 Abs. 2 und 3 entsprechend.

(5) Fällt die Grundlage einer Drittlandübermittlung weg oder wird sie für unwirksam erklärt, informiert der Auftragnehmer den Auftraggeber unverzüglich und setzt die betroffene Übermittlung aus, bis eine tragfähige Grundlage geschaffen ist.

(6) Ein Zugriff auf personenbezogene Daten des Auftraggebers aus dem mobilen Arbeiten oder Homeoffice von Beschäftigten des Auftragnehmers ist nur aus dem Gebiet der EU/des EWR und nur nach Maßgabe der internen Richtlinie des Auftragnehmers zum mobilen Arbeiten zulässig.

§ 12 Rechte betroffener Personen

(1) Für die Wahrung der Rechte betroffener Personen ist der Auftraggeber verantwortlich.

(2) Wendet sich eine betroffene Person unmittelbar an den Auftragnehmer, leitet dieser das Anliegen unverzüglich, spätestens innerhalb von **drei Werktagen**, an den Auftraggeber weiter und beantwortet es nicht selbst.

(3) Der Auftragnehmer unterstützt den Auftraggeber mit geeigneten technischen und organisatorischen Maßnahmen nach Möglichkeit dabei, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung von Betroffenenrechten nachzukommen (Art. 28 Abs. 3 lit. e DSGVO), insbesondere bei Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung, Datenübertragbarkeit und Widerspruch.

(4) Berichtigungen, Löschungen und Einschränkungen der Verarbeitung nimmt der Auftragnehmer nur nach dokumentierter Weisung des Auftraggebers vor.

(5) Für Mehraufwände gilt § 18.

§ 13 Verletzungen des Schutzes personenbezogener Daten

(1) Der Auftragnehmer meldet dem Auftraggeber jede Verletzung des Schutzes personenbezogener Daten im Sinne des Art. 4 Nr. 12 DSGVO, die im Verantwortungsbereich des Auftragnehmers oder eines seiner Unterauftragnehmer eingetreten ist, unverzüglich nach Bekanntwerden, spätestens jedoch innerhalb von **24** Stunden. Die Meldung erfolgt über den in der Ansprechpartnertabelle benannten Meldeweg.

(2) Der Auftragnehmer meldet ferner jeden Verstoß gegen datenschutzrechtliche Vorschriften, gegen die Regelungen dieses Vertrages oder gegen erteilte Weisungen unverzüglich.

(3) Die Meldung enthält, soweit verfügbar, mindestens:

- eine Beschreibung der Art der Verletzung, soweit möglich mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen und Datensätze;
- Zeitpunkt bzw. Zeitraum des Vorfalls und Zeitpunkt der Kenntniserlangung;
- eine Beschreibung der wahrscheinlichen Folgen;
- eine Beschreibung der ergriffenen und vorgeschlagenen Maßnahmen zur Behebung und zur Abmilderung möglicher nachteiliger Folgen;
- Kontaktdaten einer Auskunftsstelle beim Auftragnehmer.

(4) Sind zum Zeitpunkt der Erstmeldung nicht alle Informationen verfügbar, meldet der Auftragnehmer zunächst den bekannten Sachverhalt und ergänzt die Angaben unverzüglich nach deren Verfügbarkeit.

(5) Der Auftragnehmer unterstützt den Auftraggeber bei der Erfüllung seiner Melde- und Benachrichtigungspflichten nach Art. 33, 34 DSGVO in dem Umfang und in der Geschwindigkeit, die dem Auftraggeber die Einhaltung der 72-Stunden-Frist des Art. 33 Abs. 1 DSGVO ermöglichen. Dem Auftragnehmer ist bekannt, dass diese Frist mit Kenntniserlangung des Auftraggebers beginnt.

(6) Der Auftragnehmer ergreift unverzüglich die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen, sichert Beweismittel und dokumentiert den Vorfall sowie die getroffenen Maßnahmen. Meldungen an die Aufsichtsbehörde oder an betroffene Personen im Namen des Auftraggebers nimmt der Auftragnehmer nur nach dessen Weisung vor.

(7) Soweit der Auftraggeber Pflichten nach der Richtlinie (EU) 2022/2555 (NIS2) bzw. deren nationaler Umsetzung unterliegt, unterstützt ihn der Auftragnehmer bei der Erfüllung der ihn betreffenden Melde- und Nachweispflichten in der Lieferkette. Der Auftraggeber informiert den Auftragnehmer über eine entsprechende Betroffenheit.

§ 14 Unterstützung bei Datenschutz-Folgenabschätzung und Konsultation

(1) Der Auftragnehmer unterstützt den Auftraggeber unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen bei der Einhaltung der in den Art. 32 bis 36 DSGVO genannten Pflichten (Art. 28 Abs. 3 lit. f DSGVO).

(2) Dies umfasst insbesondere die Bereitstellung von Informationen zur Beschreibung der Verarbeitungsvorgänge, zu den getroffenen technischen und organisatorischen Maßnahmen sowie zu eingesetzten Unterauftragnehmern für Zwecke einer Datenschutz-Folgenabschätzung nach Art. 35 DSGVO und einer vorherigen Konsultation der Aufsichtsbehörde nach Art. 36 DSGVO.

(3) Für Mehraufwände gilt § 18.

§ 15 Nachweise und Kontrollrechte

(1) 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 (Art. 28 Abs. 3 lit. h DSGVO).

(2) Der Nachweis erfolgt vorrangig durch geeignete Unterlagen, insbesondere:

- aktuelle Dokumentation der technischen und organisatorischen Maßnahmen (Anlage 2);
- gültige Zertifikate, Testate oder Prüfberichte anerkannter Stellen (z. B. ISO/IEC 27001, BSI C5, TISAX, IDW PS 951) – soweit vorhanden;
- Ergebnisse eigener oder externer Audits, Penetrationstests oder Schwachstellenanalysen in zusammengefasster Form;
- ausgefüllte Standard-Fragebögen zur Informationssicherheit;
- Bestätigungen des Datenschutzbeauftragten oder eines unabhängigen Prüfers.

(3) Reichen die Nachweise nach Absatz 2 nicht aus, kann der Auftraggeber Kontrollen in den Betriebsstätten des Auftragnehmers während der üblichen Geschäftszeiten durchführen. Vor-Ort-Kontrollen sind mit angemessener Frist, in der Regel **vier Wochen**, in Textform anzukündigen und finden ohne besonderen Anlass höchstens einmal je Kalenderjahr statt. Bei konkretem Anlass, insbesondere nach einer Verletzung des Schutzes personenbezogener Daten oder auf Anordnung einer Aufsichtsbehörde, entfallen die Beschränkungen nach Häufigkeit und Frist.

(4) Der Auftraggeber führt Kontrollen nur in dem erforderlichen Umfang durch und trägt dafür Sorge, dass die Betriebsabläufe des Auftragnehmers nicht unverhältnismäßig gestört werden. Der Auftraggeber kann sich eines externen Prüfers bedienen; dieser darf kein Wettbewerber des Auftragnehmers sein und ist zur Verschwiegenheit zu verpflichten. Der Auftragnehmer kann die Zulassung eines Prüfers aus wichtigem Grund ablehnen.

(5) Kontrollen dürfen nicht dazu führen, dass der Auftraggeber Einsicht in Daten anderer Auftraggeber des Auftragnehmers oder in dessen Betriebs- und Geschäftsgeheimnisse erhält.

(6) Der Auftragnehmer erteilt der zuständigen Aufsichtsbehörde die erforderlichen Auskünfte und ermöglicht Vor-Ort-Kontrollen, soweit Maßnahmen nach Art. 58 DSGVO die Verarbeitung im Auftrag betreffen. Er informiert den Auftraggeber hierüber, soweit rechtlich zulässig.

(7) Ohne besonderen Anlass durchgeführte Vor-Ort-Kontrollen sowie die Bearbeitung von Fragebögen sind ab der zweiten Inanspruchnahme je Kalenderjahr nach § 18 zu vergüten.

§ 16 Löschung und Rückgabe nach Beendigung

(1) Nach Abschluss der Erbringung der Verarbeitungsleistungen löscht der Auftragnehmer nach Wahl des Auftraggebers alle personenbezogenen Daten oder gibt sie an den Auftraggeber zurück und löscht sodann vorhandene Kopien, sofern nicht nach Unionsrecht oder dem Recht eines Mitgliedstaats eine Verpflichtung zur Speicherung besteht (Art. 28 Abs. 3 lit. g DSGVO).

(2) Der Auftraggeber teilt seine Wahl spätestens **30** Kalendertage vor Vertragsende in Textform mit. Trifft er keine Wahl, erfolgt die Rückgabe in einem gängigen, maschinenlesbaren Format und anschließend die Löschung. Für Aufwände der Datenrückgabe und -migration gilt § 18.

(3) Die Löschung erfolgt nach dem Stand der Technik. Physische Datenträger werden nach DIN 66399 in der jeweils angemessenen Schutzklasse und Sicherheitsstufe vernichtet. Die Löschung bzw. Vernichtung wird dokumentiert; der Nachweis wird dem Auftraggeber auf Anforderung übermittelt.

(4) Daten in Datensicherungen werden nicht einzeln gelöscht, sondern mit Ablauf des jeweiligen Aufbewahrungszyklus der Datensicherung. Bis zu ihrer Löschung bleiben sie durch die vereinbarten technischen und organisatorischen Maßnahmen geschützt und werden nicht zu anderen Zwecken verarbeitet. Der Auftragnehmer gibt den maximalen Aufbewahrungszyklus in Anlage 2 an.

(5) Unterlagen mit personenbezogenen Daten, die zur Leistungserbringung nicht mehr erforderlich sind, vernichtet der Auftragnehmer nach Maßgabe seines Löschkonzepts datenschutzgerecht, ohne dass es einer gesonderten Zustimmung des Auftraggebers bedarf. Der Auftraggeber kann abweichende Weisungen erteilen.

(6) Der Auftraggeber ist berechtigt, die vollständige und vertragsgemäße Rückgabe und Löschung nach Maßgabe von § 15 zu überprüfen.

(7) Die Parteien sind sich einig, dass ein Zurückbehaltungsrecht des Auftragnehmers nach § 273 BGB hinsichtlich der verarbeiteten personenbezogenen Daten und der zugehörigen Datenträger ausgeschlossen ist.

§ 17 Haftung

(1) Für die Haftung der Parteien untereinander gelten die Regelungen des Hauptvertrages, soweit nachfolgend nichts Abweichendes bestimmt ist.

(2) Im Außenverhältnis gegenüber betroffenen Personen gilt Art. 82 DSGVO. Im Innenverhältnis tragen die Parteien den Schaden nach dem Anteil, der ihnen an der Verantwortung für den Schaden zukommt (Art. 82 Abs. 5 DSGVO).

(3) Der Auftragnehmer haftet für Schäden, die durch eine unter Verstoß gegen diesen Vertrag oder gegen rechtmäßige Weisungen des Auftraggebers erfolgte Verarbeitung entstehen.

(4) Der Auftraggeber stellt den Auftragnehmer von Ansprüchen Dritter frei, die darauf beruhen, dass der Auftraggeber die Verarbeitung ohne ausreichende Rechtsgrundlage veranlasst oder eine rechtswidrige Weisung erteilt hat, es sei denn, der Auftragnehmer hat den Verstoß erkannt oder hätte ihn offensichtlich erkennen müssen.

§ 18 Vergütung

(1) Die Vergütung für die vertragsgegenständlichen Verarbeitungsleistungen ist im Hauptvertrag geregelt.

(2) Leistungen des Auftragnehmers, die über die im Hauptvertrag vereinbarten Leistungen hinausgehen – insbesondere Mehraufwände aufgrund ergänzender Weisungen (§ 3 Abs. 7), Unterstützung bei Betroffenenrechten (§ 12 Abs. 5), Unterstützung bei einer Datenschutz-Folgenabschätzung (§ 14 Abs. 3), Kontrollen und Fragebögen ab der zweiten Inanspruchnahme je Kalenderjahr (§ 15 Abs. 7) sowie

Datenrückgabe und -migration (§ 16 Abs. 2) –, werden nach Aufwand auf Grundlage der jeweils gültigen Preisliste des Auftragnehmers vergütet, derzeit **Stundensatz** 150 EUR zzgl. USt. je angefangene **15** Minuten.

(3) Der Auftragnehmer weist den Auftraggeber auf eine zu erwartende Vergütungspflicht vor Beginn der Leistung hin.

(4) Nicht vergütungspflichtig sind Aufwände, die der Auftragnehmer zu vertreten hat, insbesondere im Zusammenhang mit einer von ihm verursachten Verletzung des Schutzes personenbezogener Daten.

§ 19 Laufzeit und Kündigung

(1) Dieser Vertrag tritt am **01.09.2026** in Kraft. Er wird auf unbestimmte Zeit geschlossen und ist an die Laufzeit des Hauptvertrages gekoppelt. Er endet automatisch mit der Beendigung des Hauptvertrages, ohne dass es einer gesonderten Kündigung bedarf.

(2) Eine isolierte ordentliche Kündigung dieses Vertrages ist ausgeschlossen, solange und soweit der Auftragnehmer aufgrund des Hauptvertrages personenbezogene Daten im Auftrag verarbeitet.

(3) Das Recht zur Kündigung aus wichtigem Grund bleibt unberührt. Ein wichtiger Grund für den Auftraggeber liegt insbesondere vor, wenn

- ein schwerwiegender Verstoß des Auftragnehmers gegen datenschutzrechtliche Vorschriften oder gegen Pflichten aus diesem Vertrag vorliegt;
- der Auftragnehmer eine rechtmäßige Weisung des Auftraggebers nicht ausführen kann oder will;
- der Auftragnehmer Kontrollrechte des Auftraggebers oder der zuständigen Aufsichtsbehörde vertragswidrig verweigert.

(4) Vor einer Kündigung wegen eines behebbaren Verstoßes setzt der Auftraggeber dem Auftragnehmer eine angemessene Frist zur Abhilfe, es sei denn, dies ist im Einzelfall unzumutbar.

(5) Die Verpflichtungen nach § 6 (Vertraulichkeit) und § 16 (Löschung und Rückgabe) bestehen über das Vertragsende hinaus fort.

§ 20 Schlussbestimmungen

(1) Änderungen und Ergänzungen dieses Vertrages sowie Nebenabreden bedürfen der Textform. Dies gilt auch für die Aufhebung dieses Textformerfordernisses.

(2) Sollten einzelne Bestimmungen dieses Vertrages unwirksam oder undurchführbar sein oder werden, bleibt die Wirksamkeit der übrigen Bestimmungen unberührt. Die Parteien verpflichten sich, die unwirksame Bestimmung durch eine wirksame zu ersetzen, die dem wirtschaftlichen Zweck der unwirksamen Bestimmung möglichst nahekommt. Entsprechendes gilt für Regelungslücken.

(3) Ändern sich die datenschutzrechtlichen Rahmenbedingungen wesentlich, passen die Parteien diesen Vertrag einvernehmlich an die geänderte Rechtslage an.

(4) Es gilt das Recht der Bundesrepublik Deutschland unter Ausschluss des UN-Kaufrechts.

(5) Ausschließlicher Gerichtsstand für alle Streitigkeiten aus und im Zusammenhang mit diesem Vertrag ist Balingen, sofern beide Parteien Kaufleute sind,, soweit gesetzlich zulässig. Abweichende Regelungen des Hauptvertrages gehen vor.

Unterschriften

Ort, den **TT.MM.JJJJ**

Balingen, den **01.09.2026**

Firma des Auftraggebers

Name, Funktion

Unterschrift / Ort, Datum

E-PROJECTA GmbH

Marc Eberhart, Geschäftsführer

Unterschrift / Ort, Datum

Anlage 1 – Unterauftragnehmer und Verarbeitungsorte

Stand: 01.09.2026 | Version: **1.0**. Die jeweils aktuelle Fassung ist abrufbar unter https://www.e-projecta.com/AV/subunternehmer.pdf.

Der Auftragnehmer nimmt für die Verarbeitung personenbezogener Daten im Auftrag des Auftraggebers Leistungen der nachfolgend aufgeführten Unterauftragnehmer in Anspruch. Diese sind nach § 10 Abs. 1 dieses Vertrages genehmigt.

A. Unterauftragnehmer mit Zugriff auf Systeme und Daten des Auftraggebers

NR.	UNTERAUFTRAGNEHMER (FIRMA, SITZ)	LEISTUNG / ZWECK	VERARBEITUNGSORT	GRUNDLAGE BEI DRITTLAND
1	Rechenzentrums- bzw. Hosting-Dienstleister	Bereitstellung Server- und Cloud-Infrastruktur	Standort	–
2	Anbieter Cloud-Produktivitätsdienste	Kollaborations- und Mailinfrastruktur	EU / ggf. Drittland	Art. 45 bzw. 46 DSGVO – konkretisieren
3	Anbieter E-Mail-Security und Archivierung	Spam- und Malwarefilterung, Archivierung	EU	–
4	Backup- bzw. Disaster-Recovery-Dienstleister	Auslagerung von Datensicherungen	EU	–
5	Anbieter Fernwartungs- bzw. RMM-Lösung	Fernzugriff, Monitoring, Patchmanagement	EU / ggf. Drittland	konkretisieren
6	Anbieter Ticket- bzw. Servicemanagementsystem	Vorgangsbearbeitung, Dokumentation	EU	–
7	Anbieter Security Operations / EDR	Bedrohungserkennung und -abwehr	EU / ggf. Drittland	konkretisieren
8	Freiberufliche Consultants / Entwickler	Consulting, Schulung, Installation, Support	Deutschland	–
9	Anbieter KI-/Analysedienste, sofern § 9 Abs. 2 aktiviert	…	…	…

Verarbeitete Datenkategorien: siehe § 2 Abs. 2 dieses Vertrages. Die Unterauftragnehmer erhalten Zugriff nur im jeweils erforderlichen Umfang.

B. Verarbeitungsorte des Auftragnehmers

STANDORT / ART	ANSCHRIFT BZW. BESCHREIBUNG	VERARBEITETE DATEN
Hauptsitz / Büro	E-PROJECTA GmbH, In der Täschen 20/1, 72336 Balingen	sämtliche Kategorien nach § 2 Abs. 2
Serverraum / Rechenzentrum	Hetzner – Nürnberg LEW – Augsburg	sämtliche Kategorien nach § 2 Abs. 2
Mobiles Arbeiten / Homeoffice	Beschäftigte des Auftragnehmers, ausschließlich innerhalb der EU/des EWR, nach interner Richtlinie	sämtliche Kategorien nach § 2 Abs. 2
Vor-Ort-Einsatz	Standorte des Auftraggebers	sämtliche Kategorien nach § 2 Abs. 2

Anlage 2 – Technische und organisatorische Maßnahmen gemäß Art. 32 DSGVO

Stand: **01.09.2026** | Version: **1.0** | Freigegeben durch: **Eberhart, Marc , Geschäftsführer**. Die jeweils aktuelle Fassung ist abrufbar unter https://www.e-projecta.com/AV/TOM.pdf.

Der Auftragnehmer hat unter Berücksichtigung des Stands der Technik, der Implementierungskosten sowie der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung und der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen die nachfolgenden technischen und organisatorischen Maßnahmen umgesetzt.

Hinweis zur Bearbeitung: Es dürfen ausschließlich Maßnahmen aufgeführt werden, die tatsächlich umgesetzt sind. Nicht umgesetzte Maßnahmen sind zu streichen oder als geplant mit Zieltermin zu kennzeichnen.

1. Pseudonymisierung und Verschlüsselung (Art. 32 Abs. 1 lit. a DSGVO)

Ziel: Personenbezogene Daten sollen für Unbefugte auch bei Kenntniserlangung nicht nutzbar sein.

BEREICH	UMGESETZTE MAßNAHMEN
Verschlüsselung ruhender Daten	– Vollverschlüsselung aller Notebooks und mobilen Endgeräte **BitLocker** mit zentraler Schlüsselverwaltung – Verschlüsselung von Server-Volumes bzw. Speichersystemen **soweit möglich** – Verschlüsselung aller Datensicherungen einschließlich ausgelagerter Kopien – Verschlüsselung mobiler Datenträger; Verbot nicht verschlüsselter privater Datenträger
Verschlüsselung der Übertragung	– Ausschließliche Nutzung transportverschlüsselter Verbindungen (TLS 1.2/1.3); Abschaltung veralteter Protokolle und Cipher Suites – VPN-Technologie mit aktuellen Verfahren für Standort- und Client-Verbindungen – Verschlüsselter Fernzugriff über die vereinbarte Fernwartungslösung – E-Mail-Transportverschlüsselung (TLS, DANE/MTA-STS **soweit umgesetzt**); Ende-zu-Ende-Verschlüsselung bzw. verschlüsselter Dateiaustausch für vertrauliche Inhalte – Bereitstellung eines gesicherten Datenaustauschverfahrens anstelle unverschlüsselter E-Mail-Anhänge
Schlüssel- und Geheimnisverwaltung	– Zentrales, verschlüsseltes Passwort-Management-System mit rollenbasiertem Zugriff und Protokollierung – Trennung von Schlüsselmaterial und verschlüsselten Daten; definierter Wiederherstellungsprozess – Keine Speicherung von Zugangsdaten in Klartextdateien, Skripten oder E-Mails
Pseudonymisierung	– Pseudonymisierung bzw. Anonymisierung von Datenbeständen, soweit der Verarbeitungszweck dies zulässt – insbesondere bei Test-, Entwicklungs- und Schulungsumgebungen – Bei Support- und Wartungstätigkeiten am Produktivsystem ist eine Pseudonymisierung technisch nicht möglich; kompensierend wirken Zugriffsbeschränkung, Protokollierung und Vertraulichkeitsverpflichtung

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

2.1 Zutrittskontrolle – physischer Zutritt zu Räumlichkeiten

BEREICH	UMGESETZTE MAßNAHMEN
Technisch	– Chipkarten-/Transponder-Schließsystem mit protokollierter Berechtigungsvergabe – Videoüberwachung Räumlichkeiten und Eingangsbereich – Bewegungsmelder in sicherheitsrelevanten Bereichen – Separat gesicherter Serverraum mit eigener Zutrittsberechtigung (Rechenzentrum) – **Videoüberwachung sicherheitsrelevanter Zugänge**
Organisatorisch	– Schlüssel- und Transponderverwaltung mit dokumentierter Ausgabe und Rückgabe – Festlegung zutrittsberechtigter Personen; Sicherheitszonen mit abgestuften Berechtigungen – Regelmäßige Überprüfung und Revision der Zutrittsberechtigungen (jährlich) – Besucherregelung: Anmeldung, Registrierung und Begleitung betriebsfremder Personen – Regelungen für Handwerker, Reinigungs- und Wartungspersonal – Clean-Desk- und Clear-Screen-Richtlinie; verschließbare Schränke für Unterlagen und Datenträger

2.2 Zugangskontrolle – Nutzung der Datenverarbeitungssysteme

BEREICH	UMGESETZTE MAßNAHMEN
Authentifizierung	– Individuelle, personalisierte Benutzerkonten; keine Gruppen- oder Sammelkonten – Mehr-Faktor-Authentifizierung für alle Fernzugriffe, VPN-Verbindungen, Cloud-Dienste und administrativen Zugriffe – Trennung von Standardbenutzer- und administrativen Konten; Administrationsebenen-Modell – Passwortrichtlinie nach aktuellem Stand (BSI): Mindestlänge **12** Zeichen, Prüfung gegen Listen kompromittierter Passwörter, Sperre nach Fehlversuchen, Wechsel nur anlassbezogen statt turnusmäßig – Automatische Bildschirmsperre nach **15** Minuten Inaktivität – Deaktivierung bzw. Sperrung inaktiver Konten nach **90** Tagen
Systemschutz	– Zentral verwaltete Endpoint-Detection-and-Response-Lösung (EDR/XDR) auf allen Clients und Servern (ESET/microsoft Defender) – Firewall-Systeme mit Regelwerksdokumentation und regelmäßiger Regelwerksprüfung – Netzsegmentierung; getrennte Netze für Server, Clients, Management und Gäste

BEREICH	UMGESETZTE MAßNAHMEN
	– Zentrales Patch- und Schwachstellenmanagement mit Fristen nach Kritikalität (kritisch: 72 h, hoch: 14 Tage, generell: 30 Tage) – Systemhärtung nach definierter Baseline; Deaktivierung nicht benötigter Dienste – Mobile-Device-Management für mobile Endgeräte (Securepoint MDM); Regelung zu privaten Endgeräten – Bedingter Zugriff (Conditional Access) auf Cloud-Dienste nach Gerät, Standort und Risiko
Organisatorisch	– Dokumentierter Onboarding-, Änderungs- und Offboarding-Prozess mit unverzüglichem Berechtigungsentzug – Verwaltung von Benutzerprofilen und Rollen; Vier-Augen-Prinzip bei der Vergabe administrativer Rechte – Verpflichtung der Beschäftigten auf Vertraulichkeit und IT-Nutzungsrichtlinie

2.3 Zugriffskontrolle – Zugriff auf Daten

Berechtigte dürfen ausschließlich auf diejenigen Daten zugreifen, die ihrer Zugriffsberechtigung unterliegen; personenbezogene Daten dürfen bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden.

BEREICH	UMGESETZTE MAßNAHMEN
Technisch	– Rollenbasiertes Berechtigungskonzept nach dem Grundsatz der minimalen Rechtevergabe („least privilege") – Maschinelle Prüfung der Berechtigungen; Zugriffsbeschränkung auf Verzeichnis-, Datenbank- und Applikationsebene – Privileged-Access-Management: administrative Rechte nur bedarfsbezogen und zeitlich begrenzt („just in time") – Protokollierung von Zugriffen auf Anwendungen, insbesondere bei Eingabe, Änderung und Löschung von Daten – Verwaltung und Kennzeichnung mobiler Datenträger – Data-Loss-Prevention-Maßnahmen bzw. Beschränkung von Wechseldatenträgern (mittels ESET)
Organisatorisch	– Dokumentiertes Berechtigungskonzept je System mit benanntem fachlichem Verantwortlichen – Beschränkung der Zahl administrativer Konten auf das notwendige Maß – Regelmäßige Rezertifizierung der Berechtigungen (jährlich) – Sichere Aufbewahrung und Bestandsführung von Datenträgern – Vernichtung von Unterlagen und Datenträgern nach DIN 66399 (Schutzklasse 2, Sicherheitsstufe P-4 / H-4)

2.4 Trennungskontrolle

BEREICH	UMGESETZTE MAßNAHMEN
Technisch	– Mandantentrennung: logische Trennung der Daten unterschiedlicher Auftraggeber auf System-, Datenbank- und Verzeichnisebene – Getrennte Produktiv-, Test- und Entwicklungsumgebungen – Virtualisierung mit getrennten Instanzen bzw. getrennte Tenants bei Cloud-Diensten – Getrennte Ordner- und Ablagestrukturen je Auftraggeber
Organisatorisch	– Zweckbindung der Verarbeitung; Festlegung von Datenbank- und Applikationsrechten je Mandant – Kennzeichnung von Datenbeständen nach Auftraggeber und Zweck, soweit technisch möglich – Sicherstellung, dass behördliche Zugriffe auf Daten anderer Auftraggeber die Daten des Auftraggebers unberührt lassen

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

3.1 Weitergabekontrolle

BEREICH	UMGESETZTE MAßNAHMEN
Technisch	– Verschlüsselte Übertragung sämtlicher Daten (siehe Ziffer 1) – VPN-Tunnel für standortübergreifende Verbindungen – Gesicherter Dateiaustausch über Nextcloud / Sharepoint M365 statt E-Mail-Anhang bei vertraulichen Inhalten – E-Mail-Sicherheitsgateway mit Malware- und Phishing-Schutz; SPF, DKIM und DMARC – Protokollierung von Datenübertragungen und Exporten – Prüfung von Daten und Datenträgern auf Schadsoftware
Organisatorisch	– Festlegung der zur Übermittlung berechtigten Personen – Dokumentation der Empfänger von Daten sowie vereinbarter Überlassungszeiträume und Löschfristen – Regelungen zu Versandart und Transportweg; Transport von Datenträgern nur verschlüsselt – Regelung zum Umgang mit Daten bei Vor-Ort-Einsätzen und im mobilen Arbeiten

3.2 Eingabekontrolle

BEREICH	UMGESETZTE MAßNAHMEN
Technisch	– Protokollierung der Eingabe, Änderung und Löschung von Daten mit Benutzerkennung und Zeitstempel – Zentrale Sammlung von Protokolldaten (Log-Management/SIEM) – Definierte Aufbewahrungsfristen für Protokolldaten (90 Tage)

BEREICH	UMGESETZTE MAßNAHMEN
	– Automatisierte Auswertung und Alarmierung bei sicherheitsrelevanten Ereignissen – Protokollierung administrativer Tätigkeiten und Fernwartungssitzungen
Organisatorisch	– Nachvollziehbarkeit von Eingabe, Änderung und Löschung durch individuelle Benutzerkennungen – Vergabe von Eingabe-, Änderungs- und Löschrechten nach Rollenkonzept – Regelung zur Auswertung von Protokolldaten unter Beachtung der Mitbestimmung – Änderungs- und Freigabeverfahren (Change Management) für sicherheitsrelevante Änderungen

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

BEREICH	UMGESETZTE MAßNAHMEN
Physische Absicherung	– Feuer- und Rauchmeldeanlage; Brandschutzmaßnahmen – Überwachung von Temperatur und Luftfeuchtigkeit im Serverraum; Klimatisierung – Unterbrechungsfreie Stromversorgung (USV) mit regelmäßiger Prüfung; Überspannungsschutz – Schutzsteckdosenleisten; Diebstahlschutz – **Netzersatzanlage / Notstromversorgung**
Belastbarkeit / Resilienz	– Redundante Auslegung zentraler Komponenten (RAID, redundante Netzteile, redundante Netzanbindung) – Hochverfügbarkeits- bzw. Cluster-Konzepte für kritische Systeme – Kapazitäts- und Lastüberwachung mit Alarmierung (Monitoring 24/7) – Schutz vor Überlastungsangriffen (DDoS-Schutz)
Datensicherung	– Dokumentiertes Backup- und Recovery-Konzept nach der Regel 3-2-1-1-0 – Mindestens eine unveränderliche bzw. netzwerkgetrennte Sicherungskopie (immutable / air-gapped) zum Schutz vor Ransomware – Auslagerung von Sicherungen an einen räumlich getrennten, gesicherten Ort – Verschlüsselung sämtlicher Sicherungen – Sicherungsintervall: täglich; Aufbewahrungszyklus: 3 Monate – Automatisierte Erfolgskontrolle der Sicherungsläufe mit Alarmierung bei Fehlern
Wiederherstellbarkeit	– Definierte Wiederherstellungsziele: RTO 48 Std. / RPO 24 Std. – Regelmäßige, dokumentierte Wiederherstellungstests (**jährlich**) – Notfallhandbuch mit Wiederanlaufplänen und Eskalationsmatrix – Ransomware-spezifisches Wiederanlaufkonzept einschließlich Isolationsmaßnahmen – Business-Continuity-Management mit benannten Verantwortlichkeiten

5. Auftrags- und Lieferantenkontrolle

BEREICH	UMGESETZTE MAßNAHMEN
Auftragskontrolle	– Verarbeitung ausschließlich nach dokumentierter Weisung; Dokumentation erteilter Weisungen – Benennung weisungsempfangsberechtigter Organisationseinheiten – Klare Abgrenzung der Verantwortlichkeiten zwischen Auftraggeber und Auftragnehmer – Verpflichtung aller Beschäftigten auf Vertraulichkeit; jährliche Awareness-Schulungen mit Nachweis
Lieferantenmanagement	– Auswahl von Unterauftragnehmern nach dokumentierten Sorgfaltskriterien, insbesondere Datensicherheit – Abschluss von Auftragsverarbeitungsverträgen nach Art. 28 DSGVO mit allen Unterauftragnehmern – Laufende, mindestens jährliche Überprüfung der Unterauftragnehmer und Dokumentation der Ergebnisse – Führung eines aktuellen Verzeichnisses der Unterauftragnehmer einschließlich Verarbeitungsorten – Sicherstellung der Löschung bzw. Rückgabe der Daten nach Beendigung von Unteraufträgen

6. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO)

BEREICH	UMGESETZTE MAßNAHMEN
Datenschutz-Management	– Verzeichnis der Verarbeitungstätigkeiten nach Art. 30 Abs. 1 und Abs. 2 DSGVO – Dokumentiertes Löschkonzept mit definierten Fristen je Datenkategorie – Verfahren zur Durchführung von Datenschutz-Folgenabschätzungen nach Art. 35 DSGVO – Prozess zur Bearbeitung von Betroffenenanfragen – Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen (Art. 25 DSGVO) – Datenschutzbeauftragter Reiner Braun, datenschutz@e-projecta.com
Informationssicherheits-Management	– Informationssicherheits-Managementsystem nach ISO/IEC 27001 bzw. CISIS12/VdS 10000 – im Aufbau – Dokumentierte Richtlinien zu IT-Nutzung, Passwörtern, mobilem Arbeiten und Umgang mit Datenträgern – Risikoanalyse und -bewertung mit definierter Wiederholung (jährlich)
Vorfallmanagement	– Dokumentiertes Incident-Response-Verfahren mit Meldewegen und Eskalationsmatrix – Meldung von Datenschutzverletzungen an den Auftraggeber innerhalb von **24** Stunden nach Kenntnis – Nachbereitung von Vorfällen mit Ursachenanalyse und Maßnahmenableitung

BEREICH	UMGESETZTE MAßNAHMEN
Prüfungen und Nachweise	– Regelmäßige interne Überprüfung der technischen und organisatorischen Maßnahmen (jährlich) sowie anlassbezogen – Schwachstellenscans der extern erreichbaren Systeme (vierteljährlich) – Externe Penetrationstests (nach Bedarf, min. jährlich) – Auswertung der Ergebnisse und dokumentierte Maßnahmenverfolgung

Bestätigung des Auftragnehmers: Die vorstehend beschriebenen Maßnahmen sind zum angegebenen Stand umgesetzt. Änderungen mit wesentlicher Auswirkung auf das Schutzniveau werden dem Auftraggeber nach § 7 Abs. 3 dieses Vertrages mitgeteilt.

Anlage 3 – Weisungsberechtigte und weisungsempfangsberechtigte Personen

Stand: 01.09.2026. Änderungen sind der jeweils anderen Partei nach § 3 Abs. 3 dieses Vertrages unverzüglich in Textform mitzuteilen; sie bedürfen keiner Vertragsänderung.

A. Weisungsberechtigte Personen des Auftraggebers

NAME	FUNKTION / ABTEILUNG	E-MAIL	TELEFON	UMFANG DER WEISUNGSBEFUGNIS
Marc Eberhart	**CEO**	marc.eberhart@e-projecta.com	07433 99934-118	**Uneingeschränkt**
Daniel Lohmüller	**Kfm. Abteilung**	daniel.lohmueller@e-projecta.com	07433 99934-188	**Kaufmännische Befugnisse**
Michael Rieger	Abteilungsleiter SW/IT	michael.rieger@e-projecta.com	07433 99934-0	**Abt. personell / technisch bei IT + Software, ERP**

B. Weisungsempfangsberechtigte Organisationseinheiten des Auftragnehmers

ORGANISATIONSEINHEIT	ANSPRECHPARTNER	E-MAIL	TELEFON
Geschäftsleitung	Marc Eberhart	info@e-projecta.com	07433 99934-118
Abteilung IT-Technik / Managed Services	**Michael Rieger**	Michael.rieger@e-projecta.com	07433 99934-0
Abteilung Software-Entwicklung	**Michael Rieger**	Michael.Rieger@e-projecta.com	07433 99934-0
Abteilung ERP-Consulting	**Burak Yildirtan**	Burak.Yildirtan@e-projecta.com	07433 99934-0
Service Desk / Ticketsystem	**Daniel Lohmüller**	Daniel.Lohmueller@e-projecta.com	07433 99934-188

Bearbeitungshinweise – nicht Vertragsbestandteil

Diese Seite ist vor der Verwendung des Dokuments als Vertrag vollständig zu entfernen. Sie dient der internen Bearbeitung und der Vorbereitung der anwaltlichen Prüfung.

1. Vor der Verwendung zwingend zu erledigen

- Sämtliche gelb markierten Platzhalter befüllen oder streichen. Die Markierung anschließend entfernen.
- Anlage 1 vollständig um die tatsächlich eingesetzten Unterauftragnehmer ergänzen; bei natürlichen Personen (Freiberufler) statt der Privatanschrift die Geschäftsanschrift bzw. Firmierung angeben.
- Anlage 2 mit dem tatsächlichen Umsetzungsstand abgleichen. Nicht umgesetzte Maßnahmen streichen – die Anlage ist verbindlich vereinbart und wird bei Kundenaudits geprüft.
- Bestellstatus des betrieblichen Datenschutzbeauftragten nach § 38 BDSG prüfen und in der Ansprechpartnertabelle sowie in Anlage 2 Ziffer 6 korrekt abbilden.
- § 2 Abs. 3: Entscheiden, ob besondere Datenkategorien, Art.-10-Daten oder Berufsgeheimnisse Gegenstand der Verarbeitung sind.
- § 9 Abs. 2: Entscheiden, ob der Einsatz von KI-Systemen vereinbart wird; bei Aktivierung Anbieter in Anlage 1 aufnehmen.
- § 16 Abs. 4: Maximalen Aufbewahrungszyklus der Datensicherung eintragen und mit Anlage 2 Ziffer 4 abgleichen.
- Firmierung und Anschrift beider Parteien gegen das Handelsregister prüfen.

2. Punkte für die anwaltliche Prüfung

- § 10 Abs. 1 bis 3: Umstellung von der Einzelgenehmigung auf die allgemeine Genehmigung nach Art. 28 Abs. 2 Satz 2 DSGVO – Angemessenheit der Fristen und Ausgestaltung des Widerspruchs- und Sonderkündigungsrechts.
- § 11: Drittlandregelung, insbesondere Ausgestaltung der Weisung nach Absatz 4 und Reichweite der Aussetzungspflicht nach Absatz 5.
- § 13 Abs. 1: Angemessenheit der 24-Stunden-Meldefrist im Verhältnis zu den tatsächlichen Prozessen des Auftragnehmers; Prüfung, ob 48 Stunden realistischer sind.
- § 17: Abstimmung mit den Haftungsregelungen des Hauptvertrages; Prüfung einer gesonderten Haftungshöchstgrenze und der AGB-rechtlichen Wirksamkeit der Freistellung nach Absatz 4.
- § 15 Abs. 7 und § 18 Abs. 2: AGB-rechtliche Wirksamkeit der Vergütungsregelung für Mitwirkungsleistungen bei Verwendung gegenüber einer Vielzahl von Kunden.
- § 20 Abs. 1: Textform statt Schriftform für Nebenabreden – Vereinbarkeit mit dem Hauptvertrag.
- § 6 Abs. 4 und § 8 Abs. 5: Ausgestaltung der Regelungen zu § 203 StGB, insbesondere Nachweisführung der Verpflichtung nach § 203 Abs. 4 StGB.
- Prüfung, ob das Dokument als Allgemeine Geschäftsbedingung im Sinne der §§ 305 ff. BGB einzuordnen ist, wenn es gegenüber mehreren Kunden verwendet wird, und ob einzelne Klauseln der Inhaltskontrolle standhalten.

3. Gegenüber der Vorfassung geänderte Rechtsgrundlagen

VORFASSUNG	NEUFASSUNG
§ 11 BDSG a. F.	Art. 28 DSGVO
§ 9 BDSG a. F. nebst Anlage	Art. 32 DSGVO (Neustrukturierung der Anlage 2)
§ 5 BDSG a. F. (Datengeheimnis)	Art. 28 Abs. 3 lit. b, Art. 29, Art. 32 Abs. 4 DSGVO
§ 42a BDSG a. F.	Art. 33, 34 DSGVO
§ 15a TMG (TMG aufgehoben)	entfallen
§ 109a TKG a. F.	entfallen bzw. TKG in der Fassung seit 2021
§ 88 TKG (Fernmeldegeheimnis)	§ 3 TDDDG
Art. 25 DSGVO als Grundlage der Pseudonymisierung	Art. 32 Abs. 1 lit. a DSGVO
Übergangsformulierungen „ab dem 25.05.2018"	entfallen

4. Neu aufgenommene Regelungen

- Rangfolgeklausel gegenüber Hauptvertrag und AGB (§ 1 Abs. 3)
- Ansprechpartnertabelle Datenschutz einschließlich Meldeweg für Sicherheitsvorfälle
- Verarbeitungsorte und Drittlandtransfer nach Art. 44 ff. DSGVO einschließlich Transfer Impact Assessment (§ 11)
- Regelung zum Einsatz von KI-Systemen mit Bezug zur KI-Verordnung (§ 9)
- Konkrete Meldefrist bei Datenschutzverletzungen sowie NIS2-Unterstützungspflicht (§ 13)
- Nachweisführung über Zertifikate und Testate als vorrangige Alternative zur Vor-Ort-Kontrolle (§ 15)
- Haftung und Innenausgleich nach Art. 82 Abs. 5 DSGVO (§ 17)
- Vergütung von Mitwirkungsleistungen (§ 18)
- Kopplung der Laufzeit an den Hauptvertrag (§ 19)
- Anwendbares Recht und Gerichtsstand (§ 20)
- Nachweis einer Cyber- und Vermögensschadenhaftpflichtversicherung (§ 5 Abs. 10)
- Anlage 3 mit weisungsberechtigten Personen beider Parteien