

Auftragsverarbeitungsvereinbarung (AVV)

nach Art. 28 Abs. 3 DS-GVO · Kennung AVV-2026-01 · Fassung vom 26.09.2026 · Querschnittsanlage (Ebene 3)

Zwischen dem im Rahmenvertrag IT-Services benannten Auftraggeber (nachfolgend „Auftraggeber“ oder „Verantwortlicher“) und der im Rahmenvertrag benannten implec-Gesellschaft (nachfolgend „Auftragnehmer“ oder „Auftragsverarbeiter“) wird folgende Vereinbarung über die Auftragsverarbeitung von personenbezogenen Daten im Sinne des Art. 28 Abs. 3 DS-GVO geschlossen:

Präambel

Zwischen den Parteien besteht ein Rahmenvertrag IT-Services, unter dem der Auftragnehmer über Bestellscheine eine oder mehrere der folgenden Leistungen erbringt: die Pflege von IT-Software und Wartung von IT-Infrastrukturen (Managed Workplace und Einzelleistungen), die Bereitstellung von Rechenkapazitäten (IaaS, virtuelle Server) im Rechenzentrum (implec Cloud), die Datensicherung und Archivierung im Rechenzentrum (Managed Backup), die Bereitstellung von Telefonie-Diensten über einen Vorleistungsanbieter (implec Phone), die Vermietung von IT-Geräten (Gerätemiete) sowie weitere im Leistungsscheine-Katalog beschriebene Leistungen. Diese Vereinbarung gilt für alle unter dem Rahmenvertrag bestellten Leistungen, ohne dass sie je Bestellschein erneut geschlossen werden muss.

Diese Vereinbarung wird als ergänzende Regelung zur Einhaltung der datenschutzrechtlichen Bestimmungen des Art. 28 DS-GVO getroffen. Der Auftraggeber hat den Auftragnehmer im Rahmen der Sorgfaltspflichten des Art. 28 DS-GVO ausgewählt. Die nachfolgende Vereinbarung konkretisiert die Verpflichtungen der Vertragsparteien zum Datenschutz, die bei der Verarbeitung personenbezogener Daten im Auftrag zu beachten sind. Sofern nicht anders definiert, sind datenschutzspezifische Begriffe im Sinne der DS-GVO zu verstehen.

1. Allgemeines

- (1) Der Auftragnehmer führt im Auftrag des Auftraggebers Pflege- und Wartungsarbeiten an IT-Systemen durch, stellt Kapazitäten im Rechenzentrum (IaaS, virtuelle Server, Datenspeicher für Backups und Archive) bereit, verwaltet Telefonie-Dienste und Endgeräte und/oder erbringt weitere Leistungen nach den bestellten Leistungsscheinen.
- (2) In diesem Zusammenhang ist nicht ausgeschlossen, dass der Auftragnehmer Sicht auf personenbezogene Daten erhält beziehungsweise theoretischen Zugriff darauf erhält, um die Leistungen erbringen zu können. Eine direkte Verarbeitung personenbezogener Daten erfolgt insbesondere, wenn der Auftragnehmer Daten zur Archivierung oder zur Erstellung eines Backups kopiert und verschiebt, Benutzerkonten anlegt und verwaltet oder Ressourcen bereitstellt, auf denen der Auftraggeber Daten verarbeitet.
- (3) Diese Vereinbarung findet auf alle Tätigkeiten Anwendung, bei denen Mitarbeiter des Auftragnehmers oder durch ihn beauftragte Unterauftragsverarbeiter personenbezogene Daten des Auftraggebers verarbeiten oder theoretisch Einblick in diese erhalten.
- (4) Soweit Erklärungen „schriftlich“ zu erfolgen haben, ist die Schriftform nach § 126 BGB gemeint. Im Übrigen können Erklärungen in Textform erfolgen, soweit eine angemessene Nachweisbarkeit gewährleistet ist.
- (5) Ist eine Partei verpflichtet, Dokumentationen oder Nachweise zu erstellen, sind diese der anderen Partei auf Anfrage zur Verfügung zu stellen.

2. Gegenstand der Verarbeitung

Gegenstand sind die in Ziffer 1 genannten Leistungen. Die Einzelheiten zu den übernommenen Verarbeitungen, zur Art der Daten und zu den Kategorien betroffener Personen werden in Anlage 1 festgelegt; welche Leistungen konkret bestellt sind, ergibt sich aus den jeweiligen Bestellscheinen.

3. Dauer und Beendigung der Datenverarbeitung

(1) Diese Vereinbarung beginnt mit Abschluss des Rahmenvertrages und gilt für die Dauer des Rahmenvertrages und aller unter ihm geschlossenen Bestellscheine sowie darüber hinaus, solange der Auftragnehmer personenbezogene Daten des Auftraggebers verarbeitet oder speichert.

(2) Ein außerordentliches Kündigungsrecht jeder Partei bleibt unberührt.

(3) Nach Beendigung der jeweiligen Leistung hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, Daten und erstellten Verarbeitungs- oder Nutzungsergebnisse, die im Zusammenhang mit dieser Leistung stehen, dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Dies betrifft auch etwaige Datensicherungen beim Auftragnehmer. Die Löschung ist zu dokumentieren. Test- und Ausschussmaterial ist unverzüglich zu vernichten oder physisch zu löschen. Die Fristen für Datenherausgabe und Löschung bei Rechenzentrumsleistungen ergeben sich aus dem jeweiligen Leistungsschein.

(4) Der Auftraggeber hat das Recht, die vollständige und vertragsgemäße Rückgabe und Löschung der Daten beim Auftragnehmer zu kontrollieren, auch durch Inaugenscheinnahme der Datenverarbeitungsanlagen in der Betriebsstätte des Auftragnehmers. Die Vor-Ort-Kontrolle ist mit angemessener Frist anzukündigen.

(5) Dokumentationen, die dem Nachweis der ordnungsgemäßen Datenverarbeitung dienen, sind vom Auftragnehmer entsprechend den jeweiligen Aufbewahrungsfristen auch über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung dem Auftraggeber bei Vertragsende übergeben.

4. Weisungen

(1) Der Auftraggeber behält sich hinsichtlich der Auftragsverarbeitung ein umfassendes Weisungsrecht vor. Er hat insbesondere das Recht, jederzeit ergänzende Weisungen über Art, Umfang und Verfahren der Verarbeitung zu erteilen. Alle Aufträge, Teilaufträge oder Weisungen werden dokumentiert erteilt. In Eilfällen können Weisungen mündlich gegeben werden; der Auftraggeber bestätigt sie unverzüglich dokumentiert.

(2) Auftraggeber und Auftragnehmer benennen die zur Erteilung und Annahme von Weisungen befugten Personen in Anlage 2. Bei einem Wechsel oder einer längerfristigen Verhinderung sind der anderen Partei Nachfolger beziehungsweise Vertreter unverzüglich mitzuteilen.

(3) Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich entsprechend der vertraglichen Vereinbarung und nach diesen Weisungen, es sei denn, er ist gesetzlich zu einer bestimmten Verarbeitung verpflichtet. Sofern solche Verpflichtungen bestehen, teilt er sie dem Auftraggeber vor der Verarbeitung mit, es sei denn, die Mitteilung ist ihm gesetzlich verboten.

(4) Der Auftragnehmer macht den Auftraggeber unverzüglich darauf aufmerksam, wenn eine Weisung seiner Meinung nach gegen gesetzliche Vorschriften verstößt. Er ist berechtigt, die Durchführung der Weisung auszusetzen, bis sie durch den Verantwortlichen beim Auftraggeber bestätigt oder geändert wird.

(5) Der Auftragnehmer dokumentiert die ihm erteilten Weisungen und deren Umsetzung.

5. Allgemeine Pflichten des Auftragnehmers

(1) Der Auftragnehmer bestätigt, dass ihm die einschlägigen datenschutzrechtlichen Vorschriften bekannt sind. Er beachtet bei der Auftrags Erfüllung die Grundsätze ordnungsgemäßer Datenverarbeitung.

- (2) Der Auftragnehmer kontrolliert regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass die Verarbeitung in seinem Verantwortungsbereich im Einklang mit dem geltenden Datenschutzrecht erfolgt und der Schutz der Rechte der betroffenen Personen gewährleistet wird.
- (3) Der Auftragnehmer verpflichtet sich, die gleichen Geheimnisschutzregeln zu beachten, wie sie dem Auftraggeber obliegen. Der Auftraggeber teilt dem Auftragnehmer etwaige besondere Geheimnisschutzregeln mit.
- (4) Der Auftragnehmer gestaltet sein Unternehmen und seine Betriebsabläufe so, dass die im Auftrag verarbeiteten Daten vor der unbefugten Kenntnisnahme Dritter geschützt sind. Er verwendet die Daten nur zur Erfüllung der vertraglich vorgegebenen Zwecke sowie zur Erfüllung zwingender gesetzlicher Vorschriften.
- (5) Der Auftragnehmer sichert zu, dass die zur Verarbeitung eingesetzten Personen vor Beginn der Verarbeitung mit den relevanten Bestimmungen des Datenschutzes und dieser Vereinbarung vertraut gemacht wurden, regelmäßig geschult und laufend angemessen angeleitet und überwacht werden. Alle Mitarbeiter sind auf das Datengeheimnis verpflichtet.
- (6) Auskünfte an Dritte oder an Betroffene erteilt der Auftragnehmer nur nach vorheriger Zustimmung des Auftraggebers. Direkt an ihn gerichtete Anfragen leitet er unverzüglich an den Auftraggeber weiter.
- (7) Für berechtigte Kontrollen ermöglicht der Auftragnehmer den mit der Kontrolle betrauten Personen, soweit erforderlich, Zutritt und Einblick, erteilt erforderliche Auskünfte, demonstriert Abläufe und führt Nachweise.

6. Unterstützung des Auftraggebers

- (1) Der Auftragnehmer unterstützt den Auftraggeber bei Erstellung und Fortschreibung des Verzeichnisses der Verarbeitungstätigkeiten sowie bei der Durchführung von Datenschutz-Folgenabschätzungen und hält alle erforderlichen Angaben und Dokumentationen vor. Er kommt seinen Pflichten aus Art. 30 Abs. 2 DS-GVO nach.
- (2) Der Auftraggeber ist als Verantwortlicher für die Wahrung der Betroffenenrechte verantwortlich. Der Auftragnehmer unterstützt ihn mit geeigneten technischen und organisatorischen Maßnahmen bei der Beantwortung von Anträgen auf Wahrnehmung von Betroffenenrechten nach Art. 12 ff. DS-GVO, insbesondere auf Auskunft, Berichtigung, Einschränkung oder Löschung, und trifft die erforderlichen Maßnahmen nach Weisung des Auftraggebers.
- (3) Der Auftragnehmer unterstützt den Verantwortlichen bei Datenschutzüberprüfungen durch Aufsichtsbehörden oder Dritte, soweit diese die Verarbeitung nach dieser Vereinbarung betreffen, und setzt Auflagen der Aufsichtsbehörde in Absprache mit dem Auftraggeber um.
- (4) Der Auftragnehmer unterstützt den Auftraggeber bei dessen Meldepflichten nach Art. 33 und 34 DS-GVO im erforderlichen Umfang, einschließlich der Mitteilungspflichten nach Ziffer 7.

7. Mitteilungspflichten des Auftragnehmers

- (1) Der Auftragnehmer meldet dem Auftraggeber jede Verletzung des Schutzes personenbezogener Daten im Sinne von Art. 4 Nr. 12 DS-GVO – Vernichtung, Verlust, Veränderung, unbefugte Offenlegung oder unbefugter Zugang, gleich ob unbeabsichtigt oder unrechtmäßig – sowie jeden Verstoß gegen datenschutzrechtliche Vorschriften, diese Vereinbarung oder Weisungen unverzüglich, spätestens 24 Stunden nach Kenntnis, in Textform an die in Anlage 2 benannte Person, damit der Auftraggeber seine Frist nach Art. 33 DS-GVO einhalten kann. Die Meldung enthält, soweit bekannt, Art und Umfang der Verletzung, betroffene Datenkategorien und Personen, wahrscheinliche Folgen und ergriffene oder vorgeschlagene Maßnahmen; nicht sofort verfügbare Angaben werden nachgereicht.
- (2) Ergänzend gilt bei besonderer Schutzbedürftigkeit: Stellt der Auftragnehmer fest oder begründen Tatsachen die Annahme, dass von ihm für den Auftraggeber verarbeitete a) besondere Kategorien personenbezogener Daten im Sinne des Art. 9 DS-GVO, b) personenbezogene Daten, die einem Berufsgeheimnis unterliegen, c) personenbezogene

Daten, die sich auf strafbare Handlungen oder Ordnungswidrigkeiten oder deren Verdacht beziehen, oder d) personenbezogene Daten zu Bank- oder Kreditkartenkonten unrechtmäßig übermittelt oder auf sonstige Weise Dritten unrechtmäßig zur Kenntnis gelangt sind, informiert er den Auftraggeber unverzüglich und vollständig über Zeitpunkt, Art und Umfang des Vorfalls in Textform. Die Information enthält eine Darlegung der Art der unrechtmäßigen Kenntniserlangung, der möglichen nachteiligen Folgen und der getroffenen Maßnahmen zur künftigen Verhinderung.

(3) Soweit die getroffenen Sicherheitsmaßnahmen den Anforderungen des Auftraggebers nicht oder nicht mehr genügen, benachrichtigt der Auftragnehmer den Auftraggeber unverzüglich.

(4) Der Auftragnehmer informiert den Auftraggeber unverzüglich über Kontrollen oder Maßnahmen von Aufsichtsbehörden oder anderen Dritten, soweit diese Bezug zur Auftragsverarbeitung aufweisen, auch bei Ermittlungen im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens.

(5) Wendet sich eine betroffene Person unmittelbar an den Auftragnehmer, leitet dieser das Ersuchen unverzüglich an den Auftraggeber weiter.

8. Fernwartung

(1) Sofern der Auftragnehmer Leistungen im Wege der Fernwartung erbringt (Anlage FW), ermöglicht er dem Auftraggeber eine wirksame Kontrolle der Fernwartungsarbeiten, zum Beispiel durch Einsatz einer Technologie, die dem Auftraggeber ermöglicht, die durchgeführten Arbeiten auf einem Monitor zu verfolgen.

(2) Unterliegt der Auftraggeber einer Berufsgeheimnispflicht im Sinne des § 203 StGB, trägt er Sorge dafür, dass eine unbefugte Offenbarung durch die Fernwartung nicht erfolgt. Der Auftragnehmer setzt insoweit Technologien ein, die dem Auftraggeber nicht nur ein Verfolgen der Tätigkeit auf dem Bildschirm ermöglichen, sondern auch die Möglichkeit geben, die Fernwartungsarbeiten jederzeit zu unterbinden.

(3) Wünscht der Auftraggeber nicht, die Fernwartungsarbeiten an einem Monitor zu beobachten, dokumentiert der Auftragnehmer die durchgeführten Arbeiten in geeigneter Weise; die Protokollierung nach Anlage FW genügt hierfür.

9. Datenschutzbeauftragter des Auftragnehmers

(1) Soweit gesetzlich verpflichtet, benennt der Auftragnehmer eine fachkundige und zuverlässige Person als Datenschutzbeauftragten. Der Auftragnehmer teilt dem Auftraggeber die Kontaktdaten in Anlage 2 mit oder begründet, weshalb kein Beauftragter benannt wurde. Änderungen teilt der Auftragnehmer unverzüglich mit.

10. Rechte und Pflichten des Auftraggebers

(1) Für die Beurteilung der Zulässigkeit der beauftragten Verarbeitung sowie für die Wahrung der Rechte der Betroffenen ist allein der Auftraggeber verantwortlich.

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

(3) Der Auftraggeber ist berechtigt, die Einhaltung der Vorschriften über den Datenschutz und dieser Vereinbarung beim Auftragnehmer in angemessenem Umfang selbst oder durch Dritte zu kontrollieren, insbesondere durch die Einholung von Auskünften, die Einsichtnahme in die gespeicherten Daten und die Datenverarbeitungsprogramme sowie sonstige Kontrollen vor Ort.

(4) Kontrollen beim Auftragnehmer erfolgen ohne vermeidbare Störungen seines Geschäftsbetriebs. Soweit nicht aus vom Auftraggeber zu dokumentierenden, dringlichen Gründen anders angezeigt, finden Kontrollen nach angemessener Vorankündigung, zu Geschäftszeiten des Auftragnehmers und nicht häufiger als alle zwölf Monate

statt. Soweit der Auftragnehmer den Nachweis der korrekten Umsetzung der vereinbarten Datenschutzpflichten erbringt, beschränkt sich eine Kontrolle auf Stichproben. Kosten und Anwesenheitspflichten regelt Ziffer 16 der AB.

11. Berichtigung, Löschung und Einschränkung

Im Rahmen des Auftrags verarbeitete Daten berichtigt, löscht oder schränkt der Auftragnehmer nur entsprechend der vertraglichen Vereinbarung oder nach Weisung des Auftraggebers ein. Den entsprechenden Weisungen leistet er jederzeit und auch über die Beendigung dieser Vereinbarung hinaus Folge.

12. Technische und organisatorische Maßnahmen

(1) Der Auftragnehmer verpflichtet sich zur Einhaltung der nach Art. 32 DS-GVO erforderlichen technischen und organisatorischen Maßnahmen. Die bei Vertragsschluss getroffenen Maßnahmen sind in Anlage 3 beschrieben.

(2) Die Maßnahmen dienen der Datensicherheit und der Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme. Dabei sind der Stand der Technik, die Implementierungskosten sowie Art, Umfang und Zwecke der Verarbeitung und die Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen zu berücksichtigen.

(3) Die Maßnahmen können der technischen und organisatorischen Weiterentwicklung entsprechend angepasst werden, solange das vereinbarte Niveau nicht unterschritten wird. Wesentliche Änderungen teilt der Auftragnehmer dem Auftraggeber in Textform mit; Anlage 3 wird fortgeschrieben.

(4) Der Auftragnehmer trennt die im Auftrag verarbeiteten Daten strikt von sonstigen Datenbeständen. Kopien oder Duplikate werden ohne Wissen des Auftraggebers nicht erstellt; ausgenommen sind technisch notwendige, temporäre Vervielfältigungen sowie die vertraglich geschuldete Datensicherung. Dedizierte Datenträger, die vom Auftraggeber stammen oder für ihn genutzt werden, werden gekennzeichnet, laufend verwaltet und angemessen aufbewahrt.

13. Unterauftragsverarbeiter

(1) Unterauftragsverhältnisse im Sinne dieser Vereinbarung sind nur solche Leistungen, die einen direkten Zusammenhang mit der Erbringung der Hauptleistung aufweisen. Nebenleistungen wie Post, Transport, Reinigung oder Bewachung sind keine Unterauftragsverhältnisse, soweit der Dienstleister keinen Zugriff auf personenbezogene Daten des Auftraggebers erhält; der Auftragnehmer stellt insoweit durch angemessene Vereinbarungen und Kontrollen den Schutz der Daten sicher. Wartungs-, Support- und Telekommunikationsdienstleister mit Zugriff auf Daten des Auftraggebers sind Unterauftragsverarbeiter nach Anlage 4. Soweit ein Dienstleister Daten in eigener Verantwortung verarbeitet (zum Beispiel ein Telekommunikationsanbieter für die nach TKG geschuldeten Verkehrsdaten), weist Anlage 4 dies aus.

(2) Der Auftraggeber erteilt dem Auftragnehmer die allgemeine Genehmigung, die in Anlage 4 aufgeführten Unterauftragsverarbeiter einzusetzen. Die Liste ordnet jeden Unterauftragsverarbeiter den Leistungsscheinen zu, für die er eingesetzt wird; für den Auftraggeber sind nur die Unterauftragsverarbeiter der von ihm bestellten Leistungen relevant.

(3) Den geplanten Einsatz eines neuen Unterauftragsverarbeiters oder den Wechsel eines bestehenden teilt der Auftragnehmer dem Auftraggeber in Textform mit. Der Auftraggeber kann innerhalb von zwei Wochen nach Zugang der Information Einspruch einlegen, wenn ein wichtiger datenschutzrechtlicher Grund gegen den Einsatz spricht. Im Fall des Einspruchs kann der Auftragnehmer nach eigener Wahl die Leistung ohne die beabsichtigte Änderung erbringen oder, sofern ihm dies nicht zumutbar ist, die betroffene Leistung innerhalb einer angemessenen Frist nach Zugang des Einspruchs einstellen; der betroffene Bestellschein endet dann zu diesem Zeitpunkt.

(4) Der Auftragnehmer wählt Unterauftragsverarbeiter sorgfältig aus und prüft vor der Beauftragung und regelmäßig während der Vertragsdauer, dass diese die nach Art. 32 DS-GVO erforderlichen technischen und organisatorischen Maßnahmen getroffen haben. Das Ergebnis dokumentiert er und übermittelt es dem Auftraggeber auf Anfrage.

(5) Die Beauftragung von Unterauftragsverarbeitern, die Verarbeitungen nicht ausschließlich aus dem Gebiet der EU oder des EWR erbringen, ist nur zulässig, soweit und solange der Unterauftragsverarbeiter angemessene Datenschutzgarantien bietet und Art. 44 bis 50 DS-GVO eingehalten werden.

(6) Der Auftragnehmer stellt sicher, dass die in dieser Vereinbarung getroffenen Regelungen und etwaige ergänzende Weisungen auch gegenüber dem Unterauftragsverarbeiter gelten und dass die Verpflichtung des Unterauftragsverarbeiters den Anforderungen des Art. 28 Abs. 4 DS-GVO entspricht, einschließlich der Kontrollbefugnisse des Auftraggebers und der Aufsichtsbehörden.

14. Vergütung

Eine gesonderte Vergütung oder Kostenerstattung im Rahmen dieser Vereinbarung erfolgt nicht. Unterstützungsleistungen nach Ziffer 6, die über das gesetzlich geschuldete Maß hinausgehen, können nach der Preisliste abgerechnet werden.

15. Haftung

(1) Auftraggeber und Auftragnehmer haften für den Schaden, der durch eine nicht der DS-GVO entsprechende Verarbeitung verursacht wird, im Außenverhältnis gegenüber der betroffenen Person nach Art. 82 DS-GVO. Im Innenverhältnis haftet der Auftragnehmer nur für Schäden, die auf einer von ihm durchgeführten Verarbeitung beruhen und wenn er a) seinen ihm speziell durch die DS-GVO oder diese Vereinbarung auferlegten Pflichten nicht nachgekommen ist oder b) unter Nichtbeachtung der rechtmäßig erteilten Weisungen des Auftraggebers oder gegen diese gehandelt hat.

(2) Soweit der Auftraggeber zum Schadensersatz gegenüber dem Betroffenen verpflichtet ist, bleibt ihm der Rückgriff auf den Auftragnehmer vorbehalten. Im Übrigen gilt Ziffer 15 der AB (Haftung).

16. Sonstiges

(1) Beide Parteien behandeln alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen der jeweils anderen Partei auch über die Beendigung hinaus vertraulich. Bestehen Zweifel, ob eine Information der Geheimhaltungspflicht unterliegt, ist sie bis zur Freigabe in Textform durch die andere Partei als vertraulich zu behandeln.

(2) Sollte Eigentum des Auftraggebers beim Auftragnehmer durch Maßnahmen Dritter (etwa Pfändung oder Beschlagnahme), durch ein Insolvenzverfahren oder durch sonstige Ereignisse gefährdet werden, verständigt der Auftragnehmer den Auftraggeber unverzüglich.

(3) Änderungen und Ergänzungen dieser Vereinbarung bedürfen der Textform. Änderungen der Anlagen 3 und 4 erfolgen nach Ziffer 12 Abs. 3 und Ziffer 13 Abs. 3.

(4) Die Einrede des Zurückbehaltungsrechts im Sinne von § 273 BGB wird hinsichtlich der im Auftrag verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen.

(5) Es gilt das Recht der Bundesrepublik Deutschland. Bei Widersprüchen zwischen dieser Vereinbarung und anderen Vertragsbestandteilen geht diese Vereinbarung für die Verarbeitung personenbezogener Daten vor (Ziffer 2 Abs. 1 des Rahmenvertrages).

(6) Diese Vereinbarung wird durch Unterzeichnung des Rahmenvertrages IT-Services geschlossen, in dessen Anlagenverzeichnis sie mit Kennung und Fassung bezeichnet ist; eine gesonderte Unterzeichnung ist nicht erforderlich. Änderungen dieser Vereinbarung erfolgen nach Ziffer 18 der AB.

Anlage 1 – Details zur Verarbeitung personenbezogener Daten

Leistungen (Zutreffendes ergibt sich aus den Bestellscheinen)

- ☐ Wartung und Pflege von Software, IT-Systemen und Netzwerken mit Zugriff vor Ort und per Fernwartung (LS-MW, LS-ST, LS-MP, LS-DL)
- ☐ Verwaltung von Benutzerkonten, Postfächern und Cloud-Diensten (Microsoft 365) (LS-MW, LS-M365, LS-LIC)
- ☐ Austausch von Hardware und Monitoring der Komponenten (LS-MW, LS-ST, LS-GM)
- ☐ Bereitstellung von Kapazitäten für Infrastrukturen (IaaS) und virtuelle Server im Rechenzentrum (LS-MC)
- ☐ Bereitstellung von Kapazitäten für Backups und Archive im Rechenzentrum (LS-OB, LS-MC)
- ☐ Bereitstellung und Verwaltung von Telefonie-Diensten, Rufnummern und Endgeräten über einen Vorleistungsanbieter (LS-PH)
- ☐ Webhosting, Domains und Zertifikate (LS-WH, LS-CERT)
- ☐ Sonstige: _____

Art der Daten

Der Auftrag kann die Verarbeitung folgender Arten personenbezogener Daten beinhalten beziehungsweise der Zugriff oder Einblick kann aus technischen Gründen nicht ausgeschlossen werden:

- ☐ Name und Kontaktdaten von Nutzern der IT-Systeme (Benutzerkonten, E-Mail-Adressen, Telefonnummern, Rufnummern)
- ☐ Kommunikationsdaten: E-Mails, Kalender, Dateien in OneDrive/SharePoint/Teams, Verbindungsdaten der Telefonie (Rufnummern, Zeitpunkt, Dauer)
- ☐ Personaldaten: Name, Adresse, Geburtsdatum, Eintritt, Regelarbeitszeit, Urlaub, Fehlzeiten, steuer- und sozialversicherungsrelevante Daten, Mitarbeiterausstattung, Bankverbindung
- ☐ Weitere Daten von Betroffenen, die in den IT-Systemen des Auftraggebers gespeichert sind
- ☐ Sonstige: _____

Kategorien der betroffenen Personen

- ☐ Beschäftigte des Auftraggebers ☐ Kunden des Auftraggebers ☐ Lieferanten und Geschäftspartner ☐ Dritte ☐ Sonstige: _____

Anlage 2 – Ansprechpartner und weisungsberechtigte Personen

Rolle	Name	E-Mail	Telefon
Weisungsberechtigte Person des Auftraggebers	_____	_____	_____
Datenschutzbeauftragter des Auftraggebers	_____	_____	_____
Weisungsempfänger des Auftragnehmers	_____	technik@implec.de	_____
Datenschutzbeauftragter des Auftragnehmers	[2021: Peter Heutz – Stand 2026 prüfen]	[2021: heutz@datenschutz-mg.de]	[2021: 0178 7908080]

Anlage 3 – Technische und organisatorische Maßnahmen

M.1 Vertraulichkeit

- Zutrittskontrolle: Alarmanlage mit Aufschaltung auf Sicherheitsdienst; Besucherkontrolle am Empfang; Schließsystem mit RFID-Transpondern; Schlüsselverwaltung mit Dokumentation; vom Arbeitsbereich separierter Serverraum; Videoüberwachung mit Aufzeichnung; externer Wachdienst.
- Zugangskontrolle: Firewall mit Intrusion Prevention; On-/Offboarding-Prozess für Benutzerberechtigungen; verschlüsselter Passwort-Speicher; persönlicher, individueller Log-in; sorgfältige Auswahl von Reinigungs- und Sicherheitspersonal; Deaktivierung ungenutzter Netzwerkdosen.
- Zugriffskontrolle: Aktenvernichter; Einzelschließung von Schränken mit sensiblen Daten; Passwortrichtlinie (Länge, Komplexität, Wechsel); Datentresor; Verschlüsselung von Datenträgern nach Stand der Technik.
- Weitergabekontrolle: Clean Desk an sensiblen Arbeitsplätzen; SSL/TLS bei Datenübertragung; VPN-Tunnel für Zugriff von außen.
- Trennungsgebot: Gäste-WLAN in eigenem VLAN; logische Trennung öffentlich/intern; MAC-Filter; Trennung von Produktiv- und Testsystem; Mandantentrennung im Ticketsystem und auf der Cloud-Plattform.
- Pseudonymisierung: Funktions-E-Mail-Adressen; Kundenkürzel statt Namen; TK-Anlage mit Metadaten-Logbuch.
- Verschlüsselung: abgesicherte Fernwartungsverbindungen; TLS auf Mail-Servern; WPA2/AES im produktiven WLAN.

M.2 Integrität

- Eingabekontrolle: personenbezogene Zugriffsrechte mit Protokollierung; Protokollierung jedes Fernzugriffs (Anlage FW).

M.3 Verfügbarkeit und Belastbarkeit

- Antivirensoftware; ausgelagerte Datensicherung im Rechenzentrum; Sicherung der Backupmedien gegen Diebstahl; IT-Monitoring; Spamfilter auf Mail-Server, Servern und Desktops; USV mit automatischem Shutdown; regelmäßige, dokumentierte Datenwiederherstellungen.

M.4 Verfahren zur regelmäßigen Überprüfung

- Auftragskontrolle: AV-Verträge mit Unterauftragsverarbeitern; Datenschutzbeauftragter; EDV-Nutzungsvereinbarung; Schulungen und Nachschulungen; Verpflichtung auf Vertraulichkeit.
- Datenschutz-Managementsystem: regelmäßige Datenschutz-Audits; Incident-Response-System; Löschkonzept; Richtlinien Home-Office/BYOD; softwaregestützte Datenschutz-Tools; Ticketsystem für IT-Servicefälle.

Anlage 4 – Unterauftragsverarbeiter

Unterauftragsverarbeiter	Leistung	Betroffene Leistungsscheine	Sitz / Verarbeitungsort
Microsoft Ireland Operations Ltd., Dublin	Microsoft 365 (Exchange Online, SharePoint, OneDrive, Teams), Lizenzen	LS-MW, LS-M365, LS-LIC	Irland; Verarbeitung innerhalb der EU (EU Data Boundary)

Unterauftragsverarbeiter	Leistung	Betroffene Leistungsscheine	Sitz / Verarbeitungsort
NinjaOne, LLC, Tampa (USA)	Management-Plattform: Fernwartung, Überwachung, Patchmanagement, Datensicherung	LS-MW, LS-ST, LS-OB, Anlage FW	USA; Instanz eu.ninjarmm.com, Rechenzentrum EU; EU- Standardvertragskla useln
Hornetsecurity GmbH, Hannover	E-Mail-Sicherheit, Archivierung, Microsoft-365-Backup	LS-MP	Deutschland
Enreach Communications GmbH	Cloud-Telefonie: Benutzerkonten, Rufnummern, Konfiguration (Unterauftragsverarbeiter); Verkehrsdaten nach TKG in eigener Verantwortung	LS-PH	Deutschland
TeamViewer Germany GmbH, Göppingen	Fernwartung (Zweitweg)	alle Leistungen mit Fernzugriff (Anlage FW)	Deutschland
Documenso, Inc.	Elektronische Signatur der Vertragsdokumente (Name, E-Mail, IP-Adresse des Unterzeichners)	Rahmenvertrag, Bestellscheine	Rechenzentrum EU (Frankfurt); EU- Standardvertragskla useln
Rechenzentrumsbetreiber implec Cloud	Colocation / Plattform für virtuelle Server und Backups	LS-MC, LS-OB	Deutschland (Ziffer 1 Abs. 5 LS-MC)