1 Präambel

Diese Vereinbarung konkretisiert die Verpflichtungen der Vertragsparteien zum Datenschutz in Bezug auf Auftragsverarbeitung, die sich aus der Vertragsbeziehung zwischen dem Auftraggeber und dem Auftragnehmer und allen dieser Vertragsbeziehung zugrundeliegenden Verträge inklusive aller Anlagen (im Folgenden „Vertrag" genannt) ergibt. Sie findet Anwendung auf alle Tätigkeiten, die mit dem Vertrag in Zusammenhang stehen und bei denen Beschäftigte des Auftragnehmers oder durch den Auftragnehmer beauftragte Dritte personenbezogene Daten („Daten") des Auftraggebers verarbeiten („Auftragsverarbeitung").

(§1) Gegenstand, Dauer und Spezifizierung der Auftragsverarbeitung

(1) Aus dem Vertrag ergeben sich Gegenstand, Dauer, Umfang sowie Art und Zweck der Auftragsverarbeitung. Dies gilt auch, sofern die jeweiligen vertraglichen Vereinbarungen nicht ausdrücklich Bezug nehmen auf diese Vereinbarung zur Auftragsverarbeitung. Soweit sich die Art der Daten und die Kategorie der betroffenen Personen nicht aus dem Vertrag ergeben, ist der Auftragnehmer berechtigt, diese dem Auftraggeber in elektronischer Form zugänglich zu machen. Die Verarbeitung kann dabei grundsätzlich folgende Arten der Verarbeitung umfassen: das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, die Verbreitung oder eine andere Form der Bereitstellung, der Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung von Daten. Die Verarbeitung kann im Rahmen eines Rechenzentrumsbetriebs des Auftragnehmers, über Fernwartung oder durch sonstige Leistungen des Auftragnehmers beim Auftraggeber wie z.B. Installationen vor Ort stattfinden.

Die Laufzeit dieser Vereinbarung richtet sich grundsätzlich nach der Laufzeit des zugrundeliegenden Vertrages und gilt solange eine Vertragsbeziehung zwischen dem Auftraggeber und dem Auftragnehmer besteht. Eine Kündigung dieser Vereinbarung kann nur aus einem wichtigen datenschutzrechtlichen Grund erfolgen. Keiner Kündigung dieser Vereinbarung bedarf es im Falle der Beendigung der Vertragsbeziehung zwischen Auftraggeber und Auftragnehmer.

(2) Die dieser Vereinbarung zugrundeliegenden Leistungen werden ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum erbracht. Jede Verlagerung der Leistungen oder von Teilarbeiten dazu in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind.

(§2) Rechte und Pflichten des Auftragnehmers

(1) Der Auftragnehmer verarbeitet Daten von betroffenen Personen ausschließlich im Rahmen der getroffenen Vereinbarungen und der dokumentierten Weisungen des Auftraggebers sowie entsprechend den datenschutzrechtlichen Regelungen, sofern er nicht zu einer anderen Verarbeitung durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragnehmer unterliegt, verpflichtet ist. In einem solchen 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 (Art. 28 Abs. 3 Satz 2 lit. a DSGVO). Die Weisungen werden anfänglich durch den Vertrag festgelegt und können vom Auftraggeber danach in schriftlicher Form oder in einem elektronischen Format (Textform) an die vom Auftragnehmer bezeichnete Stelle durch einzelne Weisungen geändert, ergänzt oder ersetzt werden. Weisungen, die im Vertrag nicht vorgesehen sind, werden als Antrag auf Leistungsänderung behandelt.

(2) Der Auftragnehmer informiert den Auftraggeber unverzüglich, wenn er der Auffassung ist, dass eine Weisung gegen anwendbare Gesetze verstößt. Der Auftragnehmer darf die Umsetzung der Weisung solange aussetzen, bis die Parteien eine einvernehmliche Lösung gefunden haben. Der Auftragnehmer darf die Durchführung einer offensichtlich rechtswidrigen Weisung ablehnen.

(3) Der Auftragnehmer wird in seinem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Er wird insbesondere technische und organisatorische Maßnahmen zum angemessenen Schutz der Daten des Auftraggebers treffen, die den Anforderungen des Art. 32 DSGVO genügen. Diese technischen und organisatorischen Maßnahmen sind in der beigefügten Anlage TOM beschrieben. Der Auftragnehmer wird diese technischen und organisatorischen Maßnahmen so treffen, dass die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sichergestellt sind. Eine Änderung der getroffenen Sicherheitsmaßnahmen bleibt dem Auftragnehmer vorbehalten, wobei jedoch sichergestellt sein muss, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird. Der Auftragnehmer verwendet die zur Verarbeitung überlassenen Daten für keine anderen und insbesondere nicht für eigene Zwecke. Duplikate der Daten werden, ohne dass sie im Auftrag oder in diesem Vertrag geregelt sind, nicht erstellt.

(4) Der Auftragnehmer unterstützt den Auftraggeber nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen in angemessener Weise bei der Erfüllung von Anfragen und Ansprüchen betroffener Personen gem. Kapitel III der DSGVO (Art. 28 Abs. 3 lit. e DSGVO) und unterstützt den Auftraggeber bei der Einhaltung der in den Art. 32 bis 36 DSGVO genannten Pflichten, wie etwa bei erforderlichen Datenschutz-Folgenabschätzungen (Art. 28 Abs. 3 Satz 2 lit. f DSGVO).

(5) Der Auftragnehmer gewährleistet, dass es den mit der Verarbeitung der Daten des Auftraggebers befassten Mitarbeitern und anderen für den Auftragnehmer tätigen Personen untersagt ist, die Daten außerhalb der Weisung zu verarbeiten. Ferner gewährleistet der Auftragnehmer, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheit unterliegen. Die Vertraulichkeits- /Verschwiegenheitspflicht besteht auch nach Beendigung dieser Vereinbarung fort.

(6) Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich, wenn ihm im Rahmen des Auftragsverhältnisses Verletzungen des Schutzes personenbezogener Daten des Auftraggebers bekannt werden. Der Auftragnehmer trifft die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen der betroffenen Personen.

(7) Der Auftragnehmer nennt dem Auftraggeber Ansprechpartner für im Rahmen dieser Vereinbarung anfallende Weisungen sowie einen etwaigen Beauftragten für den Datenschutz. Ein Wechsel oder eine längerfristige Verhinderung der Ansprechpartner ist dem Auftragnehmer unverzüglich anzuzeigen.

Weisungsempfänger des Auftragnehmers

Datenschutzbeauftragter des Auftragnehmers

Christoph Klein, ISB & DSB, datenschutz@technogroup.com

(8) Der Auftragnehmer berichtigt, löscht oder sperrt die vertragsgegenständlichen Daten, wenn der Auftraggeber dies anweist und dies vom Weisungsrahmen umfasst ist, es sei denn, die Weisung widerspricht etwaigen gesetzlichen oder vertraglichen Aufbewahrungspflichten.

(9) Im Fall von durch den Auftragnehmer ausgetauschten Datenträgern, übernimmt der Auftragnehmer die datenschutzkonforme Vernichtung, sofern nichts anderes vereinbart wurde. Dem Auftraggeber ist bekannt, dass der Transport von ausgetauschten Datenträgern durch den Auftragnehmer ungesichert erfolgt. Der Auftragnehmer bietet einen gesicherten Transport gegen gesonderte Vergütung an.

(10) Nach Auftragsende sind Daten, Datenträger sowie sonstige Materialien auf Verlangen des Auftraggebers entweder zurückzugeben oder zu löschen, sofern nicht nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung besteht. Entstehen zusätzliche Kosten durch abweichende Vorgaben bei der Rückgabe oder Löschung der Daten, so trägt diese der Auftraggeber.

(11) Im Falle einer Inanspruchnahme des Auftraggebers durch eine Person hinsichtlich etwaiger Schadensersatzansprüche nach Art. 82 DSGVO verpflichtet sich der Auftragnehmer, den Auftraggeber bei der Abwehr der Ansprüche im Rahmen seiner Möglichkeiten zu unterstützen.

(12) Für Unterstützungsleistungen, die nicht in der Leistungsbeschreibung des Hauptvertrages enthalten oder die auf ein Fehlverhalten des Auftraggebers zurückzuführen sind, kann der Auftragnehmer eine Vergütung beanspruchen.

(§3) Rechte und Pflichten des Auftraggebers

(1) Der Auftraggeber ist im Rahmen dieser Vereinbarung für die Einhaltung der gesetzlichen Bestimmungen der Datenschutzgesetze, insbesondere für die Beurteilung der Rechtmäßigkeit der Verarbeitung gemäß Art. 6 Abs. 1 DSGVO, für die Datenweitergabe an den Auftragnehmer sowie für die Wahrung der Rechte der betroffenen Personen nach den Art. 12 bis 22 DSGVO allein verantwortlich („Verantwortlicher" im Sinne des Art. 4 Nr. 7 DSGVO).

(2) Der Auftraggeber hat den Auftragnehmer unverzüglich zu informieren, wenn er in den Auftragsergebnissen Fehler oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt.

(3) Im Falle einer Inanspruchnahme des Auftragnehmers durch eine Person hinsichtlich etwaiger Schadensersatzansprüche nach Art. 82 DSGVO verpflichtet sich der Auftraggeber, den Auftragnehmer bei der Abwehr der Ansprüche im Rahmen seiner Möglichkeiten zu unterstützen.

(4) Beim Auftraggeber ist als Beauftragte(r) für den Datenschutz bestellt:

(5) Der Auftraggeber ist verpflichtet, alle im Rahmen der Vertragsbeziehung erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen des Auftragnehmers vertraulich zu behandeln. Diese Verpflichtung bleibt auch nach Beendigung dieser Vereinbarung bestehen.

(§4) Anfragen betroffener Personen

(1) Wendet sich eine betroffene Person mit Forderungen zur Beantwortung einer Auskunft, zur Berichtigung oder Löschung gemäß Art. 15 ff. DSGVO an den Auftragnehmer, wird der Auftragnehmer die betroffene Person an den Auftraggeber verweisen, sofern eine Zuordnung an den Auftraggeber auf Basis der Angaben der betroffenen Person möglich ist. Gemäß Ziffer 2.4 dieser Vereinbarung unterstützt der Auftragnehmer den Auftraggeber nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen. Der Auftragnehmer haftet nicht, wenn das Ersuchen der betroffenen Person vom Auftraggeber nicht, nicht richtig oder nicht fristgerecht beantwortet wird.

(§5) Kontrollrechte des Auftraggebers und Nachweismöglichkeiten des Auftragnehmers

(1) Der Auftragnehmer bietet hinreichende Garantien dafür, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen der DSGVO erfolgt und den Schutz der Rechte der betroffenen Person gewährleistet. Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der Auftraggeber und der Auftragnehmer geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.

(2) Der Auftragnehmer kann dem Auftraggeber die Einhaltung der in dieser Vereinbarung niedergelegten Pflichten mit geeigneten Mitteln nachweisen. Diese Nachweise können Ergebnisse eines Selbstaudits, Zertifikate zu Datenschutz und/oder Informationssicherheit (z.B. ISO 27001), Zertifikate gemäß Art. 42 DSGVO oder aktuelle Testate und/oder Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren), genehmigte Verhaltensregeln (Art. 40 DSGVO) oder verbindliche interne Datenschutzvorschriften (Art. 47 DSGVO) sein.

(3) Sofern einschlägig verpflichtet sich der Auftragnehmer, den Auftraggeber über den Ausschluss von genehmigten Verhaltensregeln nach Art. 41 Abs. 4 DSGVO und den Widerruf einer Zertifizierung nach Art. 42 Abs. 7 DSGVO unverzüglich zu informieren.

(4) Der Auftraggeber ist berechtigt, sich vor Beginn der Verarbeitung und sodann regelmäßig in angemessener Weise von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen sowie der in dieser Vereinbarung festgelegten Verpflichtungen zu überzeugen.

(5) Sollten im Einzelfall Inspektionen durch den Auftraggeber oder einen von ihm beauftragten Prüfer erforderlich sein, werden diese nach vorheriger Anmeldung unter Berücksichtigung einer angemessenen Vorlauffrist zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs durchgeführt. Der Auftragnehmer hat die Inspektion von der Unterzeichnung einer Verschwiegenheitserklärung abhängig zu machen.

(§6) Subunternehmer (weitere Auftragsverarbeiter)

(1) Ein Subunternehmerverhältnis liegt vor, wenn der Auftragnehmer weitere Auftragnehmer mit der ganzen oder einer Teilleistung der im Vertrag vereinbarten Leistung beauftragt.
Der Auftraggeber erteilt dem Auftragnehmer die allgemeine Genehmigung, weitere Subunternehmer im Sinne des Art. 28 DSGVO einzusetzen.
Der Auftragnehmer trägt Sorge dafür, dass er die Subunternehmer unter besonderer Berücksichtigung der Eignung der von diesen getroffenen technischen und organisatorischen Maßnahmen im Sinne von Art. 32 DSGVO sorgfältig auswählt.

(2) Der Auftragnehmer haftet gegenüber dem Auftraggeber dafür, dass die von ihm eingesetzten Subunternehmer den Datenschutzpflichten nachkommen, die ihm durch den Auftragnehmer vertraglich auferlegt wurden.

(3) Eine Beauftragung von Subunternehmern in Drittstaaten darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind.

(4) Nicht als Subunternehmerverhältnis im Sinne dieser Regelung sind solche Leistungen zu verstehen, die der Auftragnehmer bei Dritten als Nebenleistung zur Unterstützung bei der Auftragsdurchführung in Anspruch nimmt. Hierzu zählen z.B. Telekommunikationsleistungen, Wartung und Benutzerservice (wenn kein Zugriff auf personenbezogene Daten des Auftraggebers erfolgt), Reinigungskräfte, Prüfer oder die Entsorgung von Datenträgern. Die Einbindung von Entsorgungsunternehmen ist jedoch anzeigepflichtig, wenn der Kern der Beauftragung die Entsorgung von Dokumenten/Datenträgern, welche Daten des Auftraggebers enthalten, beinhaltet. Der Auftragnehmer wird auch bei fremd vergebenen Nebenleistungen angemessene und

gesetzeskonforme vertragliche Vereinbarungen treffen und sich Kontrollmaßnahmen vorbehalten, um den Schutz und die Sicherheit der Daten des Auftraggebers zu gewährleisten.

(§7) Haftung und Schadensersatz

Die Vertragsparteien haften entsprechend den einschlägigen gesetzlichen Bestimmungen bzw. gegenüber betroffenen Personen gemäß Art. 82 DSGVO.

(§8) Schlussbestimmungen

(1) Sollten die Daten des Auftraggebers beim Auftragnehmer durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich darüber zu informieren. Der Auftragnehmer wird alle in diesem Zusammenhang Verantwortlichen und Beteiligten unverzüglich darüber informieren, dass die Hoheit und das Eigentum an den Daten ausschließlich beim Auftraggeber als „Verantwortlichem" im Sinne der Datenschutz-Grundverordnung liegen.

(2) Die Parteien sind sich darüber einig, dass die Einrede des Zurückbehaltungsrechts durch den Auftragnehmer i.S.d. § 273 BGB hinsichtlich der zu verarbeitenden Daten und der zugehörigen Datenträger ausgeschlossen ist.

(3) Änderungen und Ergänzungen dieser Vereinbarung und aller seiner Bestandteile – einschließlich etwaiger Zusicherungen des Auftragnehmers – bedürfen einer schriftlichen Vereinbarung, die auch in einem elektronischen Format (Textform) erfolgen kann, und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Vereinbarung handelt. Dies gilt auch für den Verzicht auf dieses Formerfordernis.

(4) Sollten einzelne Bestimmungen dieser Vereinbarung ganz oder teilweise unwirksam oder undurchführbar sein oder werden, so ist die Wirksamkeit der übrigen Regelungen hiervon nicht betroffen. In diesem Falle werden die Parteien einvernehmlich eine neue Regelung oder Ergänzung der bestehenden Regelung vereinbaren, die die unwirksame oder undurchführbare Regelung in einer Art und Weise ersetzt bzw. ergänzt, die der ursprünglich von den Parteien bei Abfassung dieser Anlage beabsichtigten Regelung am nächsten kommt, hätten sie denn die Unwirksamkeit oder Undurchführbarkeit bedacht. Dies gilt auch für Regelungslücken.

(5) Diese Vereinbarung unterliegt deutschem Recht. Ausschließlicher Gerichtsstand ist der im Hauptvertrag festgelegte Gerichtsstand.

Ort, Datum	Ort, Datum
Unterschrift Auftragnehmer	Unterschrift Auftraggeber

Anlage AV1 - Hauptverträge

Liste der Hauptverträge

Bezeichnung des Vertrages	Kennzeichen des Auftragnehmers	Kennzeichen des Auftraggebers	Vertragsdatum

Anlage TOM

Technische und organisatorische Maßnahmen (TOM)
gemäß Art. 32 DSGVO
der Technogroup IT-Service GmbH

Die Grundsätze zum Umgang mit der beim Auftragnehmer eingesetzten informationstechnischen Infrastruktur sind in einem für alle Mitarbeiter verbindlichen Regelwerk festgelegt. Die darin getroffenen organisatorischen, personellen, infrastrukturellen und technischen Festlegungen gewährleisten ein hohes Maß an Sicherheit und Ordnungsmäßigkeit im gesamten Bereich des IT-Umfelds. Durch die Festlegung konkreter Zuständigkeiten und Verantwortlichkeiten wird die Erarbeitung bzw. Aktualisierung der fachlichen Vorgaben sowie deren Einhaltung sichergestellt.

1 Vertraulichkeit gem. Art. 32 Abs. 1 lit. DSGVO

1.1 Zutrittskontrolle

Anforderung:
Die Zutrittskontrolle verlangt, Unbefugten den körperlichen Zutritt zur Datenverarbeitungsanlage, mit der personenbezogene Daten verarbeitet werden, zu verwehren. Es soll verhindert werden, dass Personen, die dazu nicht befugt sind, unkontrolliert in die Nähe von Datenverarbeitungsanlagen kommen.
Ziel:
Durch die Zutrittskontrolle soll von vornherein die Möglichkeit unbefugter Kenntnis- und Einflussnahme, aber auch eine Zerstörung der Anlage(n) ausgeschlossen werden.

Technische Maßnahmen	Organisatorische Maßnahmen
☒ Mehrstufiger Zutrittsschutz	☒ Schlüsselregelung / Liste
☒ Chipkarten / Transpondersysteme	☒ Empfang / Rezeption / Pförtner
☒ Sicherheitsschlösser	☒ Besucherbuch / Protokoll der Besucher
☒ Türen mit Knauf Außenseite	☒ Mitarbeiter- / Besucherausweise
☒ Schließsystem mit Codesperre	☒ Besucher in Begleitung durch Mitarbeiter
☒ Außenhautsicherung der Rechenzentren	☒ Sorgfalt bei Auswahl des Wachpersonals
☒ Außenhautsicherung der Rechenzentren kombiniert mit Einbruchmeldeanlage mit Alarmweiterleitung zur Polizei	☒ Sorgfalt bei Auswahl Reinigungsdienste
☒ Videoüberwachung der Gebäudeeingänge und Räume der Rechenzentren	

1.2 Zugangskontrolle

Anforderung:
Im Gegensatz zur Zutrittskontrolle ist hiermit der Schutz vor einem Eindringen unbefugter Personen in das EDV System selbst, also dessen Benutzung, beabsichtigt. Es müssen daher Maßnahmen getroffen werden, die das unberechtigte Eindringen in die EDV-Systeme verhindern.
Ziel:
Die Zugangskontrolle soll die unbefugte Nutzung von Datenverarbeitungssystemen verhindern.

Technische Maßnahmen	Organisatorische Maßnahmen
☒ Authentifizierung gegen einen zentralen Verzeichnisdienst	☒ Verwalten von Benutzerberechtigungen
☒ Erzwungene Passwortkomplexität	☒ Erstellen von Benutzerprofilen
☒ Sperrung der Benutzerkennung nach mehrmaliger Fehleingabe	☒ Zentrale Passwortvergabe
☒ Firewall	☒ Allg. Richtlinie Sicherheitskonzept
☒ Intrusion Detection Systeme	☒ Richtlinie „Umgang mit Kennwörtern"
☒ Mobile Device Management	☒ Richtlinie „Löschen / Vernichten"

☒ Einsatz VPN bei Remote-Zugriffen	☒ Richtlinie „Clean Desk"
☒ Verschlüsselung von Datenträgern (Notebooks)	☒ Richtlinie zur Nutzung von mobilen Geräten (Mobile Device Policy)
☒ Anti-Viren-Software Server	☒ Richtlinie zur Nutzung von privaten Geräten
☒ Anti-Virus-Software Clients	☒ Durchführung von Penetrationstests
☒ BIOS Schutz (separates Passwort)	
☐ Sperre externer Schnittstellen (USB)	
☒ Automatische Desktopsperre	

1.3 Zugriffskontrolle

Anforderung:
Maßnahmen der Zugriffskontrolle müssen geeignet sein, zu gewährleisten, dass ausschließlich die zur Benutzung des Systems berechtigten Personen auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können.
Ziel:
Personenbezogene Daten sollen bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

Technische Maßnahmen	Organisatorische Maßnahmen
☒ Akten Schredder (mind. Stufe 3, Cross Cut)	☒ Einsatz Berechtigungskonzepte
☒ Datenschutztonnen	☒ Minimale Anzahl an Administratoren
☒ Datenträgertonnen	☒ Datenschutztresor
☒ Remotezugriffe sind verschlüsselt und passwortgeschützt (OWA, VPN)	☒ Verwaltung Benutzerrechte durch Administratoren
☒ Protokollierung von Zugriffen auf Anwendungen, konkret bei der Eingabe, Änderung und Löschung von Daten	☒ Beachtung von Aufbewahrungsfristen
☒ Protokollierung von Datenabflüssen personenbezogener Daten	☒ Richtlinie zum Gebrauch von kryptographischen Maßnahmen
	☒ Schlüssel- und Kennwortverwaltung

1.4 Trennungskontrolle

Anforderung:
Maßnahmen der Trennungskontrolle müssen gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt voneinander verarbeitet werden können. Eine Trennung darf nicht nur auf einem System oder nur auf dem Hauptsystem realisiert sein, sondern muss für die davon betroffenen Verfahren insgesamt durchgängig umgesetzt sein.
Ziel:
Die Trennungskontrolle dient der technischen Umsetzung des Prinzips der Zweckbindung und der Datensparsamkeit. Es soll verhindert werden, dass Personen Daten verarbeiten, welche für die Zweckerreichung nicht erforderlich sind.

Technische Maßnahmen	Organisatorische Maßnahmen
☒ Trennung von Produktiv- und Testumgebung	☒ Steuerung über Berechtigungskonzept
☒ Physikalische Trennung (Systeme/Datenbanken/Datenträger)	☒ Festlegung von Datenbankrechten
☒ Mandantenfähigkeit relevanter Anwendungen	

1.5 Pseudonymisierung (Art. 32 Abs. 1 lit. a DSGVO; Art. 25 Abs. 1 DSGVO)

Anforderung / Ziel:
Die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechende technischen und organisatorischen Maßnahmen unterliegen.

Technische Maßnahmen	Organisatorische Maßnahmen
☒ Im Falle der Pseudonymisierung: Trennung der Zuordnungsdaten und Aufbewahrung in getrenntem und abgesicherten System (mögl. verschlüsselt)	☒ Interne Anweisung, personenbezogene Daten im Falle einer Weitergabe oder auch nach Ablauf der gesetzlichen Löschfrist möglichst zu anonymisieren/pseudonymisieren

2 Integrität

2.1 Weitergabekontrolle

Anforderung:
Maßnahmen zur Weitergabekontrolle müssen geeignet sein, um sicherzustellen, das personenbezogene Daten bei der Übertragung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.
Zu diesen Maßnahmen gehört regelmäßig auch die überprüfbare Dokumentation, welche Empfänger personenbezogene Daten erhalten haben.
Ziel:
Es soll verhindert werden, dass unberechtigte Dritte Kenntnis von personenbezogenen Daten erhalten. Es soll ermöglicht werden zu überprüfen und festzustellen, an welchen Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen sind.

Technische Maßnahmen	Organisatorische Maßnahmen
☒ Email-Verschlüsselung	☒ Dokumentation der Datenempfänger sowie der Dauer der geplanten Überlassung bzw. der Löschfristen
☒ Einsatz von VPN	☒ Übersicht regelmäßiger Abruf- und Übermittlungsvorgängen
☒ Protokollierung der Zugriffe und Abrufe	☒ Weitergabe in anonymisierter oder pseudonymisierter Form
☒ Sichere Transportbehälter	☒ Sorgfalt bei Auswahl von Transport-Personal und Fahrzeugen
☒ Übermittlung und Bereitstellung von Daten über verschlüsselte Verbindungen wie sftp, https	☒ Persönliche Übergabe mit Protokoll
☒ Nutzung von Signaturverfahren	☒ Richtlinie zum Umgang mit Daten und Datenträgern
☒ Datensicherungen werden in einem feuerfesten Safe verschlossen	☒ Verwendung von Verschlüsselungstechniken, die nach dem aktuellen Stand der Technik als sicher gelten
☒ Ausgediente Datenträger werden mechanisch nach gefordertem Schutzniveau vernichtet	☒ Unterweisung der Mitarbeiter im Datenschutz, Datensicherheit und Informationssicherheit
☒ Verschlüsselung der Daten beim Transport auf Datenträgern	☒ Eine Pseudoanonymisierung von Daten findet in dem Rahmen statt, wie sie von Auftraggeber beauftragt wird

2.2 Eingabekontrolle

Anforderung:
Die Maßnahmen zur Eingabekontrolle müssen gewährleisten, dass alle sicherheitsrelevanten Abläufe und alle Vorgänge, die personenbezogene Daten betreffen, durch das System protokolliert (geloggt) werden.
Ziel:
Mit der Eingabekontrolle soll gewährleistet werden, dass (durch den DSB oder die Aufsichtsbehörde) nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten eingeben, verändert oder entfernt worden sind.

- Es ist gewährleistet, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.
- Sicherheitsvorfälle werden gemeldet und bearbeitet.

Technische Maßnahmen	Organisatorische Maßnahmen
☒ Technische Protokollierung der Eingabe, Änderung und Löschung von Daten	☒ Übersicht, mit welchen Programmen welche Daten eingegeben, geändert oder gelöscht werden können
☒ Manuelle oder automatisierte Kontrolle der Protokolle	☒ Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)
	☒ Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts
	☒ Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen wurden
	☒ Klare Zuständigkeiten für Löschungen
	☒ Sicherheitsvorfälle werden gemeldet und bearbeitet

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

3.1 Verfügbarkeitskontrolle

Anforderung:
Maßnahmen zur Verfügbarkeitskontrolle müssen sicherstellen, dass personenbezogene Daten nicht unbeabsichtigt zerstört werden oder „verloren" gehen.
Ziel:
Negative Auswirkungen für den Betroffenen durch die unbeabsichtigte Löschung von Daten sollen verhindert werden. Die Verfügbarkeit der Daten ist für die ordnungsgemäße Erfüllung der Verarbeitungszwecke notwendige Voraussetzung.

Technische Maßnahmen	**Organisatorische Maßnahmen**
☒ Feuer- und Rauchmeldeanlagen	☒ Backup & Recovery-Konzept (ausformuliert)
☒ Feuerlöscher Serverraum	☒ Kontrolle des Sicherungsvorgangs (täglich an Werktagen)
☒ Serverraumüberwachung Temperatur und Feuchtigkeit	☒ Regelmäßige Tests zur Datenwiederherstellung und Protokollierung der Ergebnisse
☒ Serverraum klimatisiert	☒ Aufbewahrung der Sicherungsmedien an einem sicheren Ort außerhalb des Serverraums
☒ USV, Überspannungsschutz	☒ Keine sanitären Anschlüsse im oder oberhalb des Serverraums
☒ Schutzsteckdosenleisten Serverraum	☒ Existenz eines Notfallplans
☒ Datenschutztresor	☒ Getrennte Partitionen für Betriebssysteme und Daten
☒ RAID System / Festplattenspiegelung	☒ Monitoring und Prüfung der Produktivsysteme
☒ Videoüberwachung Serverraum	☒ Notfallmanagementsystem, das der Wiederherstellung der Verfügbarkeit nach Eintreten eines Notfalls dient. Die Notfallstrategie besteht aus Vorsorgemaßnahmen, Übungen und dokumentierten Wiederanlaufplänen der IT-Prozesse. Sie ist in einem Notfallhandbuch mit Notfallplan festgelegt.
☒ Aktualisierung Virenschutz (Intervall < 4h)	☒ Regelmäßige Wartung der Hardwaresysteme durch Technogroup IT-Service GmbH
☒ Redundante Firewall-Systeme	☒ Supportverträge mit Herstellern und/oder Dienstleistern für kritische Softwaresysteme
☒ Redundante Internetanschlüsse	

4 Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 DSGVO; Art. 25 Abs. 1 DSGVO)

4.1 Datenschutz Management

Anforderung / Ziel:
Rechtskonformität

Technische Maßnahmen	Organisatorische Maßnahmen
☒ Software-Lösungen für Datenschutz Management im Einsatz	☒ Interner Informationssicherheits- & Datenschutzbeauftragter
☒ Zentrale Dokumentation aller Verfahrensweisen und Regelungen zum Datenschutz mit Zugriffsmöglichkeit für Mitarbeiter nach Bedarf / Berechtigung	☒ Mitarbeiter geschult und auf Vertraulichkeit / Datengeheimnis verpflichtet
☒ Sicherheitszertifizierung nach ISO 27001	☒ Regelmäßige Sensibilisierung der Mitarbeiter (jährlich)
☒ Dokumentiertes Sicherheitskonzept	☒ Die Datenschutz-Folgenabschätzung (DSFA) wird bei Bedarf durchgeführt
☒ Eine Überprüfung der Wirksamkeit der technischen Schutzmaßnahmen wird mind. jährlich durchgeführt	☒ Die Organisation kommt den Informationspflichten nach Art. 13 und 14 DSGVO nach
	☒ Formalisierter Prozess zur Bearbeitung von Auskunftsanfragen seitens Betroffener ist vorhanden

4.2 Incident Response Management

Anforderung / Ziel:
Unterstützung bei der Reaktion auf Sicherheitsverletzungen

Technische Maßnahmen	Organisatorische Maßnahmen
☒ Einsatz von Firewall und regelmäßige Aktualisierung	☒ Dokumentierter Prozess zur Erkennung und Meldung von Sicherheitsvorfällen / Datenpannen (auch im Hinblick auf Meldepflicht gegenüber Aufsichtsbehörde)
☒ Einsatz von Spamfilter und regelmäßige Aktualisierung	☒ Dokumentierte Vorgehensweise zum Umgang mit Sicherheitsvorfällen
☒ Einsatz von Virenscanner und regelmäßige Aktualisierung	☒ Einbindung von DSB und ISB in Sicherheitsvorfälle und Datenpannen
☒ Intrusion Detection System (IDS)	☒ Dokumentation von Sicherheitsvorfällen und Datenpannen via Ticketsystem
☒ Intrusion Prevention System (IPS)	☒ Formaler Prozess und Verantwortlichkeiten zur Nachbearbeitung von Sicherheitsvorfällen und Datenpannen

4.3 Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO)

Anforderung / Ziel:
Privacy by design / Privacy by default

Technische Maßnahmen	Organisatorische Maßnahmen
☒ Es werden nicht mehr personenbezogene Daten erhoben, als für den jeweiligen Zweck erforderlich sind	
☒ Einfache Ausübung des Widerrufrechts des Betroffenen durch technische Maßnahmen	

4.4 Auftragskontrolle (Outsourcing an Dritte)

Anforderung:
Die Auftragskontrolle verpflichtet den Auftragnehmer, den Auftrag, bei den personenbezogenen Daten verarbeitet oder genutzt werden, gemäß den Vorschriften des Datenschutzes und den Vorgaben des Auftraggebers abzuwickeln und dem Auftraggeber als verantwortliche Stelle Kontrollen vor Ort zu ermöglichen. Maßnahmen zur Auftragskontrolle müssen sicherstellen, dass die überlassenen Daten nur im Rahmen des Auftrages verarbeitet werden können.
Ziel:
Unklare Regelungen sollen vermieden und Datenschutzverstöße durch unsachgemäßen Umgang mit Daten bei dem Auftragnehmer ausgeschlossen werden.

Technische Maßnahmen	Organisatorische Maßnahmen
	☒ Vorherige Prüfung der vom Auftragnehmer getroffenen Sicherheitsmaßnahmen und deren Dokumentation
	☒ Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten in Bezug auf Datenschutz und Datensicherheit
	☒ Abschluss der notwendigen Vereinbarung zur Auftragsverarbeitung bzw. EU Standardvertragsklauseln
	☒ Schriftliche Weisungen an den Auftragnehmer
	☒ Verpflichtung der Mitarbeiter des Auftragnehmers auf Datengeheimnis
	☒ Verpflichtung zur Bestellung eines Datenschutzbeauftragten durch den Auftragnehmer bei Bestellpflicht
	☒ Vereinbarung wirksamer Kontrollrechte gegenüber dem Auftragnehmer
	☒ Regelung zum Einsatz weiterer Subunternehmer
	☒ Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags
	☒ Bei längerer Zusammenarbeit: Laufende Überprüfung des Auftragnehmers und seines Schutzniveaus

4.5 Wirksamkeitskontrolle

Anforderung:
Maßnahmen der Wirksamkeitskontrolle müssen gewährleisten, dass die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste sicherzustellen, regelmäßig überprüft, bewertet und evaluiert wird. Dazu gehört die Sicherstellung der Benachrichtigungspflichten gegenüber Aufsichtsbehörden und Betroffenen durch die Einführung von Überwachungsmaßnahmen die geeignet sind, Schutzverletzungen und deren Auswirkungen rechtzeitigt festzustellen und deren mögliche Auswirkungen zu bestimmen.
Ziel:
Durch regelmäßige Prüfungen und Neubewertungen der Risiken werden die Maßnahmen auf dem Stand der Technik gehalten und der Nachweis für eine fortlaufende Sicherstellung der Angemessenheit des Schutzniveaus erbracht.

- Die bestehenden Zertifizierungen werden jährlich durch externe Auditoren überwacht. Alle drei Jahre erfolgt eine Re-Zertifizierung
- Für Verarbeitungen werden Datenschutzfolgenabschätzungen durchgeführt
- Dienstleister werden auditiert

Technische Maßnahmen	Organisatorische Maßnahmen
	☒ Durch ein Informationssicherheitsmanagement (ISMS-Management) wird die Verfügbarkeit, Vertraulichkeit und Integrität der Daten innerhalb der IT-Umgebung sichergestellt
	☒ Die bestehenden Zertifizierungen werden jährlich durch externe Auditoren überwacht. Alle drei Jahre erfolgt eine Re-Zertifizierung
	☒ Es wird jährlich ein internes Audit durchgeführt
	☒ Sicherheitsvorfälle werden gemeldet und im Rahmen des Informationssicherheitsmanagement behandelt
	☒ Risiken werden regelmäßig überprüft und bewertet