Präambel

Ab dem 25. Mai 2018 ist die DSGVO einzuhalten. Als europaweit unmittelbar anwendbares Gesetz enthält die DSGVO in Art. 28 teilweise andere Anforderungen an eine Auftragsdatenverarbeitung, als dies bis zum 24. Mai 2018 gem. § 11 BDSG der Fall ist. Daher enthält dieser Vertrag drei Hauptteile: Der erste Teil enthält überwiegend allgemeine Regelungen, die gleichermaßen für die Zeit der Anwendbarkeit des BDSG wie auch der Anwendbarkeit der DSGVO gelten. Der zweite Teil entspricht den Anforderungen des BDSG und gilt ausschließlich für die Zeit der Anwendbarkeit des BDSG bis zum 24. Mai 2018. Der dritte Teil ersetzt ab dem 25. Mai 2018 ersatzlos den zweiten Teil und entspricht den Anforderungen der ab dann geltenden DSGVO.

1 Technische und organisatorische Maßnahmen

Die nachfolgende Beschreibung der technischen und organisatorischen Maßnahmen gemäß § 9 BDSG (Datenschutz- und Datensicherheitskonzept) und § 78a SGB X[1] werden Teil dieser Vereinbarung. Die hier festgelegten Maßnahmen müssen die personenbezogenen Daten vor der zufälligen oder unrechtmäßigen Zerstörung, vor dem zufälligen Verlust, der unberechtigten Änderung oder Weitergabe oder dem unberechtigten Zugang schützen. Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem AN gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren. Der AN hat auf Anforderung die Angaben nach § 4g Abs. 2, S.1 BDSG dem AG zur Verfügung zu stellen.

2.1 Zutrittskontrolle

	Akten- und Datenträger vernichtung	Physische Archivierung mit Funktionalität AS	Digitalisierung
▪ Zutrittssicherung an allen Zutrittsmöglichkeiten zur Anlage	x	x	x
▪ Zutritt von Dritten nur mit Voranmeldung	x	x	x
▪ Einbruchmeldeanlage gegen unbefugten Zutritt	x	x	x
▪ Zutrittsschleusen für Personen und LKW	x	x	x
▪ Brandmeldeanlage	x	x	x
▪ Schlüsselverzeichnis	x	x	x
▪ Elektronische Schließsysteme an allen Zutrittsmöglichkeiten	x	x	x
▪ VDS-Einbruchmeldeanlage gegen unbefugten Zutritt	-	x	x
▪ VDS-Legitimationsprüfung der zugriffsberechtigten Personen	-	x	x
▪ Datenverarbeitungsserver befindet sich in einem Sicherheits-Rechenzentrum mit Laser-Feuermelder und Löschgas	-	x	x

2.2 Zugangskontrolle

	Akten- und Datenträger vernichtung	Physische Archivierung mit Funktionalität AS	Digitalisierung
▪ Verpflichtungserklärungen für Mitarbeiter und Besucher	x	x	x
▪ Besuchernachweis	x	x	x
▪ Passwortkontrolle/Zugangsdatenkontrolle	x	x	x
▪ Mitarbeiterausweis	x	x	x
▪ Einsatz von Firewalls	-	x	x
▪ VPN Leitungen	-	x	x

1 Der Bezug auf § 78a SGB X gilt nur wenn es sich beim AG um eine öffentliche Stelle handelt.

2.3 Zugriffskontrolle

	Akten- und Datenträger vernichtung	Physische Archivierung mit Funktionalität AS	Digitalisierung
▪ Verpflichtungserklärung aller Mitarbeiter auf § 5 BDSG und § 35 SGB I	x	x	x
▪ Mitarbeiterausweis	x	x	x
▪ Besucherausweis	x	x	x
▪ Sorgfältige Auswahl der Mitarbeiter (polizeiliches Führungszeugnis)	x	x	x
▪ Innensicherheitsrevision	x	x	x
▪ Sicherheitsschleusen	x	x	x
▪ Personenbezogene Passwortvergabe für Datenverarbeitungssysteme	x	x	x
▪ Benutzerbezogene Rechtevergabe für Mitarbeiter	x	x	x
▪ Stellenbeschreibungen zur Definition von Mitarbeiterrechten	x	x	x
▪ EDV: benutzerbezogene Rechtevergabe für Mitarbeiter	x	x	x

2.4 Weitergabekontrolle

	Akten- und Datenträger vernichtung	Physische Archivierung mit Funktionalität AS	Digitalisierung
▪ Transport in geschlossenen Fahrzeugen	x	x	x
▪ Transport in geschlossenen Behältern	x	x	x
▪ Dokumentation mittels Lieferschein oder digitaler Unterschrift	x	x	x
▪ Tourenplan	x	x	x
▪ Einsatz von Verschlossenen Sicherheitsbehältern und LKW	x	x	x
▪ Dienstanweisung im Fahrerhandbuch	x	x	x
▪ GPS-Ausstattung in Fahrzeugen	x	x	x
▪ Obligatorische SSL-verschlüsselte Datenleitungen für den Kundenzugang über das Internet	-	x	x
▪ Obligatorischer VPN-Tunnel für die abhörsichere Datenübertragung bei den ScanDOK-Standorten	-	x	x
▪ Zentraler Datenbankserver als prädestinierter Speicherort	-	x	x

2.5 Eingabekontrolle

	Akten- und Datenträger vernichtung	Physische Archivierung mit Funktionalität AS	Digitalisierung
▪ Schichtbericht	x	-	-
▪ Tourenplan	x	x	x
▪ Lieferschein	x	x	x
▪ Besuchernachweis	x	x	x
▪ Zugriffsprotokoll	-	x	x
▪ Zugriffsprotokoll für die Nutzung des Kundenzugangs	-	x	x
▪ Umfangreiches Protokoll zur Erfassung von Neueingaben, Änderungen und Löschungen von Daten	-	x	x
▪ EDV-Datensicherung	-	x	-
▪ AS (Archiv Software)	-	x	-

2.6 Auftragskontrolle

	Akten- und Datenträger vernichtung	Physische Archivierung mit Funktionalität AS	Digitalisierung
▪ Eindeutige Vertragsgestaltung	x	x	x
▪ Lieferschein oder digitale Unterschrift	x	x	x
▪ Videoüberwachung der Anlage/Zugangsdatenkontrolle	x	x	x
▪ Vernichtungsprotokoll / -bestätigung	x	x	x

2.7 Verfügbarkeitskontrolle

	Akten- und Datenträger vernichtung	Physische Archivierung mit Funktionalität AS	Digitalisierung
▪ Stellenbeschreibungen zur genauen Definition von Mitarbeiterpflichten	x	x	x
▪ Definition und Abgrenzung der Arbeitsprozesse im Qualitätsmanagementsystem	x	x	x
▪ Brandmeldeanlage	x	x	x
▪ Einbruchmeldeanlage	x	x	x
▪ Datensicherung/tägliche EDV-Datensicherung der gesamten Datenbankbestände und Ablage der Sicherungsdaten auf örtlich getrennten Hochsicherheitsservern	-	x	x
▪ Rechenzentrum mit Notstromaggregaten für mehrere Tage autonom durchgängigen Betrieb	-	x	x
▪ Feuerlöscher	-	x	x
▪ 24/7 Videoüberwachung	-	x	x
▪ Bewegungsmelder	-	x	x
▪ Zugangskontrollen	-	x	x

2.8 Trennungskontrolle

	Akten- und Datenträger vernichtung	Physische Archivierung mit Funktionalität AS	Digitalisierung
▪ ScanDOK sind die Zwecke der Erhebung unbekannt, die Trennungskontrolle muss insoweit vom AG gewährleistet werden	x	-	-
▪ getrennte Einlagerung	-	x	x
▪ zugriffsgeschützte Datenspeicherung in kundenspezifischen Datenbanksektoren	-	x	x

2 Berichtigung, Löschung und Sperrung von Daten

Der AN hat nach Weisung des AG die Daten, die im Auftrag verarbeitet werden, zu berichtigen, zu löschen oder zu sperren. Soweit ein Betroffener sich unmittelbar an den AN zwecks Berichtigung oder Löschung seiner Daten wenden sollte, wird der AN diesen Antrag unverzüglich an den AG weitergeben.

3 Pflichten des Auftragnehmers gemäß § 11 Abs. 4 BDSG und § 80 Abs. 4, 6 SGB X[2] sowie vorzunehmende Kontrollen

Der AN wird zur Durchführung des Vertrages nur Mitarbeiter oder sonstige Erfüllungsgehilfen einsetzen, die auf das Datengeheimnis nach § 5 BDSG und § 35 SGB I[3] verpflichtet und in geeigneter Weise mit den Anforderungen des Datenschutzes vertraut gemacht sind.

Ferner ist der AN verpflichtet, die einschlägigen Vorschriften zur Bestellung des Datenschutzbeauftragten gemäß §§ 4f, 4g BDSG zu erfüllen.

Er unterwirft sich eventuellen Kontrollmaßnahmen der Datenschutzaufsichtsbehörde und wird den AG über eine eventuelle Kontrollmaßnahme unverzüglich informieren, wenn personenbezogene Daten des AG betroffen sind.

4 Unterauftragsverhältnisse

Der AN kann im Einzelfall zur Vertragsdurchführung Dritte einsetzen, soweit der AG vorher schriftlich zustimmt.

Im Bereich der Akten- und Datenträgervernichtung werden grundsätzlich keine Unterauftragnehmer zur Vertragsdurchführung eingesetzt.

Der AG ist mit der Einschaltung der in Anlage 4 (entfällt bei Akten- & Datenträgervernichtung) genannten Unternehmen als Unterauftragnehmer des AN einverstanden.

Der AN wird alle mit diesem Vertrag übernommenen Verpflichtungen dem Subunternehmen selbständig auferlegen. Der Unterauftrag ist schriftlich zu fixieren. Die allgemeinen Vorschriften hinsichtlich des Verhältnisses zwischen dem AN und dem Subunternehmen bleiben unberührt.

2 Der Bezug auf § 80 Abs. 4, 6 SGB X gilt nur wenn es sich beim AG um eine öffentliche Stelle handelt.
3 Der Bezug auf § 35 SGB I gilt nur wenn es sich beim AG um eine öffentliche Stelle handelt.

5 Kontrollrechte des Auftraggebers und Mitwirkungspflichten des Auftragnehmers

Der AN räumt dem AG und dessen zur Verschwiegenheit verpflichteten auf § 5 BDSG und § 35 SGB I[4] Bevollmächtigten bezüglich der getroffenen Datenschutz- und Datensicherungsvorkehrungen ein jederzeitiges Besichtigungs- und Kontrollrecht, grundsätzlich nach vorheriger Ankündigung, ein. Der AN ist unter Wahrung der Rechte Dritter verpflichtet, im Falle von Auskünften und Einsichtnahmen die erforderliche Unterstützung bereitzustellen.

Unabhängig davon hat sich der AG vor Beginn der Datenverarbeitung und sodann regelmäßig von der Einhaltung der beim AN getroffenen technischen und organisatorischen Maßnahmen zu überzeugen. Das Ergebnis ist zu dokumentieren.

6 Mitzuteilende Verstöße des Auftragnehmers

Bei begründetem Verdacht der Verletzung von in dieser Vereinbarung festgelegten Datenschutz- und Datensicherheitsbestimmungen durch den AN selbst, Mitarbeiter des AN oder durch den AN beauftragte Dritte ist der AN verpflichtet, den AG unverzüglich zu benachrichtigen. Das Gleiche gilt auch bei Verstößen gegen die allgemeinen Vorschriften zum Schutz personenbezogener Daten. Dies gilt insbesondere, wenn personenbezogene Daten des AG betroffen sind.

7 Umfang der Weisungsbefugnisse

Der AG ist für die Einhaltung des BDSG und anderer Vorschriften über den Datenschutz sowie die Rechtmäßigkeit der Datenweitergabe an den AN verantwortlich. Der AN darf die Daten nur im Rahmen der Weisungen des AG verarbeiten. Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind gemeinsam abzustimmen.

Falls der AN eine Weisung, gleich aus welchen Gründen, nicht einhalten kann, verpflichtet er sich, den AG unverzüglich davon in Kenntnis zu setzen.

Der AN wird den AG unverzüglich darauf aufmerksam machen, wenn eine vom AG erteilte Weisung seiner Meinung nach gegen das BDSG oder eine andere Vorschrift über den Datenschutz verstößt.

8 Löschung der Daten nach Beendigung des Auftrags

Die protokollierte Vernichtung/Löschung von Daten ist Zweck des Vertrages, sodass § 11 Abs. 2 Ziffer 10 BDSG bzw. § 80 Abs. 2 Ziffer 10 SGB X[5] im Rahmen, der in diesem Vertrag vereinbarten Auftragsdatenverarbeitung, keine Anwendung findet.

Teil 3 - Auftragsverarbeitung gemäß Art. 28 DSGVO

Dieser Teil 3 gilt ab dem 25. Mai 2018 aufgrund der ab diesem Zeitpunkt verbindlichen Datenschutz-Grundverordnung. Er ersetzt den Teil 2 dieses Vertrages. Für diesen Teil 3 gelten die Begriffsbestimmungen der Datenschutz-Grundverordnung.

Im **Hauptvertrag** werden sämtliche Bezugnahmen auf das BDSG und dessen Vorschriften durch solche der DSGVO wie folgt ersetzt:

(a) Die Angabe „BDSG“ wird jeweils durch die Angabe „DSGVO“ ersetzt.
(b) Die Angabe „§ 11 BDSG“ wird jeweils durch die Angabe „Art. 28 DSGVO“ ersetzt.
(c) Die Angabe „§ 9 BDSG“ wird jeweils durch die Angabe „Art. 32 DSGVO“ ersetzt.

1 Weisungsgebundene Verarbeitung und Remonstrationspflicht

Der Auftragsverarbeiter darf personenbezogene Daten nur auf dokumentierte Weisung des Verantwortlichen verarbeiten, sofern er nicht durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragsverarbeiter unterliegt, hierzu verpflichtet ist; in einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

Weisungen werden vom Verantwortlichen grundsätzlich in Textform (z.B. per E-Mail) erteilt.
Soweit eine Weisung ausnahmsweise mündlich erfolgt, wird diese vom Verantwortlichen entsprechend in Textform (z.B. per E-Mail) bestätigt.

4 Der Bezug auf § 35 SGB I gilt nur wenn es sich beim AG um eine öffentliche Stelle handelt.

5 Der Bezug auf § 80 Abs. 2 Ziffer 10 SGB X gilt nur wenn es sich beim AG um eine öffentliche Stelle handelt.

Der Auftragsverarbeiter wird den Verantwortlichen unverzüglich darauf hinweisen, wenn die Befolgung einer vom Verantwortlichen erteilten Weisung nach seiner Ansicht gegen die DSGVO oder eine andere Vorschrift über den Datenschutz verstößt (Remonstrationspflicht).

2 Vertraulichkeits-/ Verschwiegenheitspflicht

Der Auftragsverarbeiter wird zur Durchführung des Vertrages nur Personen beschäftigen, die er zur Vertraulichkeit verpflichtet hat oder die einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

3 Sicherheit der Verarbeitung / Technische und organisatorische Maßnahmen gemäß Art. 32 DSGVO

Der Auftragsverarbeiter ergreift alle erforderlichen technischen und organisatorischen Maßnahmen gem. Artikel 32 DSGVO.

Technische und organisatorische Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Während der Dauer dieses Auftrags sind diese durch den Auftragsverarbeiter fortlaufend an die Anforderungen dieses Auftrags anzupassen und dem technischen Fortschritt entsprechend weiterzuentwickeln. Das Sicherheitsniveau der im Folgenden festgelegten technischen und organisatorischen Maßnahmen darf nicht unterschritten werden.

Der Auftragsverarbeiter verpflichtet sich, Änderungen der technischen und organisatorischen Maßnahmen, die einen wesentlichen Einfluss auf das gewährleistete Sicherheitsniveau haben, als Ergänzung der folgenden Maßnahmen schriftlich zu dokumentieren, was auch in einem elektronischen Format erfolgen kann, und dem Verantwortlichen zur Kenntnis zu geben.

Der Auftragsverarbeiter ergreift folgende Maßnahmen:

1. Pseudonymisierung

Personenbezogene Daten des Verantwortlichen können in einer Weise verarbeitet werden, sodass sie ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die eine unbefugte Identifizierung der Betroffenen gewährleisten. Dies erfolgt wie folgt:

	Akten- und Datenträger vernichtung	Physische Archivierung mit Funktionalität AS	Digitalisierung
▪ Verschlüsselung von Zusatzinformationen zur Identifikation	-	x	x
▪ Verwaltung und Dokumentation von differenzierten Berechtigungen auf die Zusatzinformationen zur Identifikation	-	x	x
▪ Autorisierungsprozess oder Genehmigungsroutinen für Berechtigungen zur Verarbeitung von Zusatzinformationen zur Identifikation	-	x	x
▪ Kopierschutz hinsichtlich Zusatzinformationen zur Identifikation	-	x	x
▪ Vier-Augen-Prinzip für Identifikation	-	-	x

2. Maßnahmen zur Verschlüsselung

	Akten- und Datenträger vernichtung	Physische Archivierung mit Funktionalität AS	Digitalisierung
▪ Verschlüsselung von mobilen Endgeräten wie Laptops, Tablets, Smartphones	x	x	x
▪ Verschlüsselung von Dateien	x	x	x
▪ Verschlüsselung von Systemen/Anlagen	x	x	x
▪ Verschlüsselte Aufbewahrung von Passwörtern	x	x	x
▪ Gesicherte Datenweitergabe (z.B. SSL, FTPS, TLS)	x	x	x
▪ Gesichertes WLAN	x	x	x
▪ Sonstiges/Spezifizierung der o.g. Maßnahmen: **Gesicherte Datenverbindungen, VPN (intern/extern)**	x	x	x

3. Maßnahmen zur Sicherstellung von Vertraulichkeit

a. Zutrittskontrolle			
	Akten- und Datenträger vernichtung	Physische Archivierung mit Funktionalität AS	Digitalisierung
▪ Zutrittskontrollsystem, Ausweisleser (Magnet-/Chipkarte)	x	x	x
▪ Türsicherungen (elektrische Türöffner, Zahlenschloss, etc.)	x	x	x
▪ Sicherheitstüren	x	x	x
▪ Zaunanlagen	x	-	-
▪ Schlüsselverwaltung/Dokumentation der Schlüsselvergabe	x	x	x
▪ Alarmanlage	x	x	x
▪ Videoüberwachung	x	x	x
▪ Spezielle Schutzvorkehrungen des Serverraums	x	x	x
▪ Spezielle Schutzvorkehrungen für die Aufbewahrung von Back-Ups und/oder sonstigen Datenträgern	x	x	x
▪ Nicht-reversible Vernichtung von Datenträgern	x	x	x
▪ Mitarbeiter- und Berechtigungsausweise	x	x	x
▪ Sperrbereiche	x	x	x
▪ Besucherregelung (Bspw. Abholung am Empfang, Dokumentation von Besuchszeiten, Besucherausweis, Begleitung nach dem Besuch bis zum Ausgang)	x	x	x

b. Zugangskontrolle			
	Akten- und Datenträger vernichtung	Physische Archivierung mit Funktionalität AS	Digitalisierung
▪ Persönlicher und individueller User-Log-In bei Anmeldung am System bzw. Unternehmensnetzwerk	x	x	x
▪ Autorisierungsprozess für Zugangsberechtigungen	x	x	x
▪ Begrenzung der befugten Benutzer	x	x	x
▪ Single Sign-On	x	-	-
▪ Kennwortverfahren (Angabe von Kennwortparametern hinsichtlich Komplexität und Aktualisierungsintervall)	x	x	x
▪ Elektronische Dokumentation von Passwörtern und Schutz dieser Dokumentation vor unbefugtem Zugriff	x	x	x
▪ Personalisierte Chipkarten, Token, PIN-/TAN, etc.	x	x	x
▪ Protokollierung des Zugangs	x	x	x
▪ Zusätzlicher System-Log-In für bestimmte Anwendungen	x	x	x
▪ Automatische Sperrung der Clients nach gewissem Zeitablauf ohne Useraktivität (auch passwortgeschützter Bildschirmschoner oder automatische Pausenschaltung)	x	x	x
▪ Firewall	x	x	x

c. Zugriffskontrolle			
	Akten- und Datenträger vernichtung	Physische Archivierung mit Funktionalität AS	Digitalisierung
▪ Verwaltung und Dokumentation von differenzierten Berechtigungen	x	x	x
▪ Auswertungen/Protokollierungen von Datenverarbeitungen	x	x	x
▪ Autorisierungsprozess für Berechtigungen	x	x	x
▪ Genehmigungsroutinen	x	x	x
▪ Profile/Rollen	x	x	x
▪ Verschlüsselung von CD/DVD- ROM, externen Festplatten und/oder Laptops (etwa per Betriebssystem, Safe Guard Easy, PGP)	x	x	x
▪ „Mobile Device Management-System“	x	x	x
▪ Vier-Augen-Prinzip	x	x	x
▪ Funktionstrennung „Segregation of Duties“	x	x	x
▪ Fachkundige Akten- und Datenträgervernichtung gemäß DIN 66399	x	x	x
▪ Nicht-reversible Löschung von Datenträgern	x	x	x

4. Maßnahmen zur Sicherstellung von Integrität

	Akten- und Datenträger vernichtung	Physische Archivierung mit Funktionalität AS	Digitalisierung
▪ Zugriffsrechte	x	x	x
▪ Systemseitige Protokollierungen	x	x	x
▪ Dokumenten Management System (DMS) mit Änderungshistorie	x	x	x
▪ Sicherheits-/Protokollierungssoftware	x	x	x
▪ Funktionelle Verantwortlichkeiten, organisatorisch festgelegte Zuständigkeiten	x	x	x
▪ Mehraugenprinzip	x	x	x
▪ Protokollierung von Datenübertragung oder Datentransport	x	x	x
▪ Protokollierung von lesenden Zugriffen	x	x	x
▪ Protokollierung des Kopierens, Veränderns oder Entfernens von Daten	x	x	x

5. Maßnahmen zur Sicherstellung und Wiederherstellung von Verfügbarkeit

	Akten- und Datenträger vernichtung	Physische Archivierung mit Funktionalität AS	Digitalisierung
▪ Sicherheitskonzept für Software- und IT-Anwendungen	x	x	x
▪ Back-Up Verfahren	x	x	x
▪ Aufbewahrungsprozess für Back-Ups (brandgeschützter Safe, getrennter Brandabschnitt, etc.)	x	x	x
▪ Gewährleistung der Datenspeicherung im gesicherten Netzwerk	x	x	x
▪ Bedarfsgerechtes Einspielen von Sicherheits-Updates	x	x	x
▪ Spiegeln von Festplatten	x	x	x
▪ Einrichtung einer unterbrechungsfreien Stromversorgung (USV)	x	x	x
▪ Geeignete Archivierungsräumlichkeiten für Papierdokumente	x	x	x
▪ Brand- und/oder Löschwasserschutz des Serverraums	x	x	x
▪ Brand- und/oder Löschwasserschutz der Archivierungsräumlichkeiten	x	x	x

▪ Klimatisierter Serverraum	x	x	x
▪ Virenschutz	x	x	x
▪ Firewall	x	x	x
▪ Notfallplan	x	x	-
▪ Erfolgreiche Notfallübungen (Brandschutz)	x	x	x
▪ Redundante, örtlich getrennte Datenaufbewahrung (Offsite Storage)	x	x	x

6. Maßnahmen zur Sicherstellung der Belastbarkeit

	Akten- und Datenträger vernichtung	Physische Archivierung mit Funktionalität AS	Digitalisierung
▪ Notfallplan für Maschinenausfall	x	x	x
▪ Redundante Stromversorgung	x	x	x
▪ Ausreichende Kapazität von IT-Systeme und Anlagen	x	x	x
▪ Logistisch gesteuerter Prozess zur Verhinderung von Leistungsspitzen	x	x	x
▪ Redundanten Systeme/Anlagen	x	x	x
▪ Resilienz und Fehler-Management	x	x	x

7. Maßnahmen zur Gewährleistung der Wirksamkeitskontrolle

	Akten- und Datenträger vernichtung	Physische Archivierung mit Funktionalität AS	Digitalisierung
▪ Verfahren für regelmäßige Kontrollen/Audits	x	x	x
▪ Penetrationstests	-	-	x
▪ Notfalltests (e.g. Brand)	x	-	-

8. „Weisungskontrolle/Auftragskontrolle“

	Akten- und Datenträger vernichtung	Physische Archivierung mit Funktionalität AS	Digitalisierung
▪ Vertrag zur Auftragsdatenverarbeitung gem. Art. 28 Abs. 3 DSGVO mit Regelungen zu den Rechten und Pflichten des Auftragsverarbeiters und Verantwortlichen	x	x	x
▪ Prozess zur Erteilung und/oder Befolgung von Weisungen	x	x	x
▪ Bestimmung von Ansprechpartnern und/oder verantwortlichen Mitarbeitern	x	x	x
▪ Kontrolle/Überprüfung weisungsgebundener Auftragsdurchführung	x	x	x
▪ Schulungen/Einweisung aller zugriffsberechtigten Mitarbeiter beim Auftragnehmer	x	x	x
▪ Verpflichtung der Mitarbeiter zur Vertraulichkeit	x	x	x
▪ Vereinbarung von Konventionalstrafen für Verstöße gegen Weisungen	x	x	x

4 Inanspruchnahme der Dienste weiterer Auftragsverarbeiter

Der Auftragsverarbeiter darf weitere Auftragsverarbeiter in Anspruch nehmen, wobei im Bereich der Akten- und Datenträgervernichtung grundsätzlich keine weiteren Auftragsverarbeiter zur Vertragsdurchführung eingesetzt werden. Die zum Zeitpunkt des Vertragsschlusses in Anspruch genommenen weiteren Auftragsverarbeiter sind in Anlage 2 (entfällt bei Akten- & Datenträgervernichtung) zu diesem Vertrag aufgeführt. Sofern der Auftragsverarbeiter den Verantwortlichen nicht vor dem Wirksamwerden dieses Teil 3 über die Zusammenarbeit mit weiteren Auftragsverarbeitern schriftlich informiert hat, was auch in einem elektronischen Format erfolgen kann, darf der Auftragsverarbeiter andere Auftragsverarbeiter nur einsetzen, hinzuziehen oder bestehende weitere Auftragsverarbeiter ersetzen, wenn er den Verantwortlichen zuvor über die beabsichtigte Änderung informiert hat. Gegen derartige Veränderungen kann der Verantwortliche Einspruch erheben.

Nimmt der Auftragsverarbeiter die Dienste eines weiteren Auftragsverarbeiters in Anspruch, um bestimmte Verarbeitungstätigkeiten im Namen des Verantwortlichen auszuführen, so werden diesem weiteren Auftragsverarbeiter im Wege eines Vertrags, der schriftlich abzufassen ist, was auch in einem elektronischen Format erfolgen kann, oder eines anderen Rechtsinstruments nach dem Unionsrecht oder dem Recht des betreffenden Mitgliedstaats dieselben Datenschutzpflichten auferlegt, die in diesem Teil 3 festgelegt sind, wobei insbesondere hinreichende Garantien dafür geboten werden müssen, dass die geeigneten technischen und organisatorischen Maßnahmen so durchgeführt werden, dass die Verarbeitung entsprechend den Anforderungen der DSGVO erfolgt. Kommt der weitere Auftragsverarbeiter seinen Datenschutzpflichten nicht nach, so haftet der erste Auftragsverarbeiter gegenüber dem Verantwortlichen für die Einhaltung der Pflichten jenes anderen Auftragsverarbeiters.

5 Mitwirkungs-/ Unterstützungspflichten

Der Auftragsverarbeiter unterstützt den Verantwortlichen angesichts der Art der Verarbeitung mit geeigneten technischen organisatorischen Maßnahmen dabei, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der in Kapitel III der DSGVO genannten Rechte der betroffenen Person nachzukommen (Berücksichtigung von Betroffenenrechten hinsichtlich der Gewährleistung von Transparenz; Recht auf Auskunft; Berichtigungsrecht; Recht auf Löschung („Vergessenwerden“); Recht auf Einschränkung der Verarbeitung; Mitteilungsrecht bei Berichtigung und Löschung sowie Einschränkung der Verarbeitung; Recht auf Datenübertragbarkeit; Widerspruchsrecht; Rechte bei automatisierten Einzelfallentscheidungen).

6 Unterstützung zur Pflichterfüllung des Verantwortlichen

Der Auftragsverarbeiter unterstützt den Verantwortlichen unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen bei der Einhaltung der in den Artikeln 32 bis 36 DSGVO genannten Pflichten. (Gewährleistung der Sicherheit der Verarbeitung; Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörden; Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person; Datenschutz-Folgenabschätzung; Vorherige Konsultation).

7 Löschung und Rückgabe personenbezogener Daten

Die protokollierte Löschung von Daten ist Zweck des Vertrages, sodass Art. 28 Abs. 3 lit. g DSGVO im Rahmen der in diesem Hauptvertrag vereinbarten Auftragsverarbeitung keine Anwendung findet.

8 Pflichtennachweis und Unterstützung bei Überprüfungen

Der Auftragsverarbeiter stellt dem Verantwortlichen alle erforderlichen Informationen zum Nachweis der Einhaltung der in Art. 28 DSGVO niedergelegten Pflichten zur Verfügung. Er ermöglicht Überprüfungen - einschließlich Inspektionen -, die vom Verantwortlichen oder einem anderen von diesem beauftragten Prüfer durchgeführt werden, und trägt zu ihrer Durchführung bei.