GRUNDIG
Business Systems

Vertrag zur Auftragsverarbeitung zwischen

Grundig Business Systems GmbH & Co. KG Emmericher Strasse 17
90411 Nürnberg, Deutschland
– nachfolgend GBS bzw. Auftragnehmer genannt –

und

Firma
Straße, Hausnummer
Postleitzahl, Ort

– nachfolgend Auftraggeber genannt –

§ 1 Gegenstand und Dauer des Auftrags

(1) GBS führt die im Anhang 1 beschriebenen Dienstleistungen oder Teile davon für den Auftraggeber durch. Gegen stand, Dauer, Art und Zweck der Verarbeitung, die Art der personenbezogenen Daten sowie die Kategorien betroffener Personen werden dort beschrieben.

(2) Gegenstand des Vertrages ist nicht die originäre Nutzung oder Verarbeitung von personenbezogenen Daten durch GBS. Im Zuge der vertragsgegenständlichen Leistungserbringung kann ein Zugriff auf personenbezogene Daten nicht gänzlich ausgeschlossen werden.

(3) GBS ist verpflichtet, die ihr zur Verfügung gestellten personenbezogenen Daten ausschließlich zur Erbringung der in diesem Vertrag vereinbarten Leistungen zu verwenden. GBS ist es gestattet, Duplikats-Dateien zur leistungsgemäßen Erbringung der vereinbarten Leistungen zu erstellen, soweit dies nicht zu einer inhaltlichen Umgestaltung führt.

(4) Dieser Vertrag tritt – solange keine anderweitigen Regelungen vereinbart wurden – mit Unterzeichnung beider Parteien in Kraft und gilt, solange GBS für den Auftraggeber die vereinbarten Leistungen erbringt.

§ 2 Weisungen des Auftraggebers

(1) Der Auftraggeber ist für die Einhaltung der gesetzlichen Bestimmungen des Datenschutzrechts, insbesondere für die Rechtmäßigkeit der Verarbeitung sowie für die Wahrung der Betroffenenrechte verantwortlich. Gesetzliche oder vertragliche Haftungsregelungen bleiben hiervon unberührt.

(2) GBS verarbeitet die ihr zur Verfügung gestellten personenbezogenen Daten ausschließlich nach den Weisungen des Auftraggebers und im Rahmen der getroffenen Vereinbarungen bzw. Aufträge. Daten dürfen nur berichtigt, gelöscht und gesperrt werden, wenn der Auftraggeber dies anweist.

(3) Grundsätzlich können Weisungen mündlich erteilt werden. Mündliche Weisungen sind anschließend von dem Auftraggeber zu dokumentieren. Weisungen sind schriftlich oder in Textform zu erteilen, wenn GBS dies verlangt.

(4) Ist GBS der Ansicht, dass eine Weisung des Auftraggebers gegen datenschutzrechtliche Vorschriften verstößt, hat GBS den Auftraggeber unverzüglich darauf hinzuweisen.

§ 3 Technische und organisatorische Maßnahmen

(1) GBS verpflichtet sich, für die zu verarbeitenden Daten angemessene technische und organisatorische Sicherheitsmaßnahmen zu treffen und zu dokumentieren (Anhang 2). Die Sicherheitsmaßnahmen haben ein dem Risiko angemessenes Schutzniveau zu gewährleisten.

(2) Die getroffenen Maßnahmen können im Laufe der Zeit der technischen und organisatorischen Weiterentwicklung angepasst werden. GBS darf entsprechende Anpassungen nur vornehmen, wenn diese mindestens das Sicherheitsniveau der bisherigen Maßnahmen erreichen. Soweit nichts anderes bestimmt ist, muss GBS dem Auftraggeber nur wesentliche Anpassungen mitteilen.

(3) GBS unterstützt den Auftraggeber bei der Einhaltung aller gesetzlichen Pflichten hinsichtlich der einzuhaltenden technischen und organisatorischen Maßnahmen. GBS hat auf Anfrage an der Erstellung und der Aktualisierung des Verzeichnisses der Verarbeitungstätigkeiten des Auftraggebers mitzuwirken. GBS wirkt bei der Erstellung einer Datenschutz-Folgenabschätzung und ggf. bei der vorherigen Konsultation der Aufsichtsbehörden mit. Sie hat dem Auftraggeber alle erforderlichen Angaben und Dokumente auf Anfrage offenzulegen.

§ 4 Pflichten von GBS

(1) GBS bestätigt, dass ihr die einschlägigen datenschutzrechtlichen Vorschriften bekannt sind. Sie gestaltet in ihrem Verantwortungsbereich die innerbetriebliche Organisation so, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird.

(2) GBS bietet hinreichende Garantien dafür, dass die geeigneten technischen und organisatorischen Maßnahmen durchgeführt werden, die gewährleisten, dass die Verarbeitung im Einklang mit den datenschutzrechtlichen Vorschriften und den Rechten der betroffenen Person steht.

(3) GBS sichert zu, dass sie die bei der Durchführung der Arbeiten beschäftigten Mitarbeiter mit den für sie maßgebenden Bestimmungen des Datenschutzes vertraut macht und die zur Verarbeitung der personenbezogenen Daten befugten Personen sich zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Sie überwacht die Einhaltung der datenschutzrechtlichen Vorschriften.

(4) GBS nimmt keinen weiteren Auftragsverarbeiter (Subunternehmer) ohne vorherige gesonderte oder allgemeine schriftliche Genehmigung des Auftraggebers in Anspruch. Im Fall einer allgemeinen schriftlichen Genehmigung informiert GBS den Auftraggeber immer über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung von Subunternehmern, wodurch der Auftraggeber die Möglichkeit erhält, gegen derartige Änderungen Einspruch zu erheben.

(5) GBS verpflichtet sich, alle nach Art. 32 der Datenschutz-Grundverordnung erforderlichen Maßnahmen zu ergreifen.

(6) GBS darf im Rahmen der Auftragsverarbeitung nur dann auf personenbezogene Daten des Auftraggebers zugreifen, wenn dies für die Durchführung der Auftragsverarbeitung zwingend erforderlich ist.

(7) GBS darf die personenbezogenen Daten nur auf dokumentierte Weisung des Auftraggebers – auch in Bezug auf die Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation – verarbeiten, sofern sie nicht durch das Recht der Union oder des Mitgliedstaats, dem GBS unterliegt, hierzu verpflichtet ist; in einem solchen Fall teilt GBS dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet;

(8) GBS bestellt einen Beauftragten für den Datenschutz. Die Kontaktdaten des Beauftragten für den Datenschutz werden dem Auftraggeber zum Zweck der direkten Kontaktaufnahme mitgeteilt.

(9) GBS darf die ihr zur Verfügung gestellten personenbezogenen Daten ausschließlich im Gebiet der Bundesrepublik Deutschland oder in einem Mitgliedsstaat der Europäischen Union verarbeiten. Die Verarbeitung von personenbezogenen Daten in einem Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen gesetzlichen Voraussetzungen erfüllt sind.

(10) GBS unterstützt den Auftraggeber mit geeigneten technischen und organisatorischen Maßnahmen, damit dieser seine bestehenden Pflichten gegenüber der betroffenen Person erfüllen kann, z.B. die Information und Auskunft an die betroffene Person, die Berichtigung oder Löschung von Daten, die Einschränkung der Verarbeitung oder das Recht auf Datenübertragbarkeit und Widerspruch. GBS benennt einen Ansprechpartner, der den Auftraggeber bei der Erfüllung von gesetzlichen Informations- und Auskunftspflichten, die im Zusammenhang mit der Auftragsverarbeitung entstehen, unterstützt und teilt dem Auftraggeber dessen Kontaktdaten unverzüglich mit. Soweit der Auftraggeber besonderen gesetzlichen Informationspflichten bei unrechtmäßiger Kenntnis erlangung von Daten unterliegt, unterstützt GBS den Auftraggeber hierbei. Auskünfte an die betroffene Person oder Dritte darf GBS nur nach vorheriger Weisung des Auftraggebers erteilen. Soweit eine betroffene Person ihre datenschutzrechtlichen Rechte unmittelbar gegenüber der Auftragnehmerin geltend macht, wird GBS dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

(11) Es obliegt dem Auftraggeber, die Bewertung vorzunehmen, welche der zu verarbeitenden Daten dem Schutz von § 203 StGB unterliegen und dies für GBS kenntlich zu machen.

GBS verpflichtet sich, über Berufsgeheimnisse Stillschweigen zu bewahren und sich nur insoweit Kenntnis von diesen Daten zu verschaffen, wie dies zur Erfüllung der ihm zugewiesenen Aufgaben erforderlich ist.

Der Auftraggeber weist GBS darauf hin, dass sich Personen, die an der beruflichen Tätigkeit eines Berufsgeheim nisträgers mitwirken und unbefugt ein fremdes Geheimnis offenbaren, das ihnen bei der Ausübung oder bei Gelegenheit ihrer Tätigkeit bekannt geworden ist, strafbar machen nach § 203 Abs. 4 S. 1 StGB.

Zudem macht sich eine mitwirkende Person nach § 203 Abs. 4 S. 2 StGB strafbar, sollte sie sich einer weiteren mitwirkenden Person bedienen, die ihrerseits unbefugt ein fremdes, ihr bei der Ausübung oder bei Gelegenheit ihrer Tätigkeit bekannt gewordenes Geheimnis offenbart, und nicht dafür Sorge getragen hat, dass diese zur Geheimhaltung verpflichtet wurde.

(12) GBS stellt sicher, dass alle mit der Verarbeitung von dem Berufsgeheimnis unterliegenden Daten des Auftraggebers befassten Beschäftigten, andere für GBS tätigen Personen und in Anhang 3 aufgeführten Subunternehmer, die damit befasst sind, sich in Textform dazu verpflichtet haben, die ihnen bei der Ausübung oder bei Gelegenheit ihrer Tätigkeit bekannt gewordenen Berufsgeheimnisse nicht unbefugt zu offenbaren und sie über die mögliche Strafbarkeit nach § 203 Abs. GBs4 StGB belehrt wurden.

Der Auftraggeber weist GBS darauf hin, dass sich eine mitwirkende Person nach § 203 Abs. 4 S. 2 StGB strafbar macht, sollte sie sich einer weiteren mitwirkenden Person bedienen, die ihrerseits unbefugt ein fremdes, ihr bei der Ausübung oder bei Gelegenheit ihrer Tätigkeit bekannt gewordenes Geheimnis offenbart, und die mitwirkende Person nicht dafür Sorge getragen hat, dass die weitere mitwirkende Person zur Geheimhaltung verpflichtet wurde.

(13) GBS ist im Rahmen seiner vertraglichen Verpflichtungen zur Begründung von weiteren Unterauftragsverhältnissen mit Subunternehmern („Subunternehmerverhältnis“) befugt. Er setzt den Auftraggeber hiervon unverzüglich in Kenntnis. GBS ist verpflichtet, Subunternehmer sorgfältig nach deren Eignung und Zuverlässigkeit auszuwählen. GBS hat bei der Einschaltung von Subunternehmern diese entsprechend den Regelungen dieses Vertrages zu verpflichten und dabei sicherzustellen, dass der Auftraggeber seine Rechte aus diesem Vertrag (insbesondere seine Kontrollrechte) auch direkt gegenüber den Subunternehmern wahrnehmen kann. Sofern eine Einbeziehung von Subunternehmern in einem Drittland erfolgen soll, hat GBS sicherzustellen, dass beim jeweiligen Subunternehmer ein angemessenes Datenschutzniveau gewährleistet ist (z. B. durch Abschluss einer Vereinbarung auf Basis der EU-Standarddatenschutzklauseln) und gem. §4 Abs.9 die vorherige Zustimmung des Auftraggebers eingeholt wurde.

(14) Unterauftragsverhältnisse mit Subunternehmern im Sinne dieser Bestimmungen liegen nicht vor, wenn der GBS Dritte mit Dienstleistungen beauftragt, die als reine Nebenleistungen anzusehen sind. Dazu gehören z. B. Post-, Transport- und Versandleistungen, Reinigungsleistungen, Telekommunikationsleistungen ohne konkreten Bezug zu Leistungen, die der Auftragnehmer für den Auftraggeber erbringt und Bewachungsdienste.

§ 5 Kontrollrechte des Auftraggebers

GBS erklärt sich damit einverstanden, dass der Auftraggeber oder eine von ihm beauftragte Person berechtigt ist, die Einhaltung der Vorschriften über den Datenschutz und der vertraglichen Vereinbarungen im erforderlichen Umfang zu kontrollieren, insbesondere durch die Einholung von Auskünften und Anforderung von relevanten Unterlagen, die Einsichtnahme in die Verarbeitungsprogramme oder durch Zutritt zu den Arbeitsräumen der Auftragnehmerin zu den ausgewiesenen Geschäftszeiten nach vorheriger Anmeldung. Durch geeignete und gültige Zertifikate zur IT-Sicherheit (z.B. IT-Grundschutz, ISO 27001) kann auch der Nachweis einer ordnungsgemäßen Verarbeitung erbracht werden, sofern hierzu auch der jeweilige Gegenstand der Zertifizierung auf die Auftragsverarbeitung im konkreten Fall zutrifft. Die Vorlage eines relevanten Zertifikats ersetzt jedoch nicht die Pflicht der Auftragnehmerin zur Dokumentation der Sicherheitsmaßnahmen im Sinne des § 3 dieser Vereinbarung.

§ 6 Mitzuteilende Verstöße von GBS

GBS unterrichtet den Auftraggeber unverzüglich über Störungen des Betriebsablaufs, die Gefahren für die Daten des Auftraggebers mit sich bringen, sowie bei Verdacht auf Datenschutzverletzungen im Zusammenhang mit den Daten des Auftraggebers. Gleiches gilt, wenn GBS feststellt, dass die bei ihr getroffenen Sicherheitsmaßnahmen den gesetzlichen Anforderungen nicht genügen. GBS ist bekannt, dass der Auftraggeber verpflichtet ist, umfassend alle Verletzungen des Schutzes personenbezogener Daten zu dokumentieren und ggf. den Aufsichtsbehörden bzw. der betroffenen Person unverzüglich zu melden. Sofern es zu solchen Verletzungen gekommen ist, wird GBS den Auftraggeber bei der Einhaltung von dessen Meldepflichten unterstützen. Sie wird die Verletzungen des Auftraggebers unverzüglich melden und hierbei zumindest folgende Informationen mitteilen:

a) eine Beschreibung der Art der Verletzung, der Kategorien und ungefähre Anzahl der betroffenen Personen und Datensätze,

b) Name und Kontaktdaten eines Ansprechpartners für weitere Informationen,

c) eine Beschreibung der wahrscheinlichen Folgen der Verletzung sowie

d) eine Beschreibung der ergriffenen Maßnahmen zur Behebung oder Abmilderung der Verletzung.

§ 7 Haftung

Die Haftung von GBS richtet sich nach Artikel 82 der Datenschutz-Grundverordnung, vorbehaltlich folgender Regelungen für Ansprüche des Auftraggebers:

a) Die Haftung von GBS bei Vorsatz ist unbeschränkt.

b) Bei grober Fahrlässigkeit haftet GBS in Höhe des typischen und bei Auftragserteilung vorhersehbaren Schadens.

c) Bei einfach fahrlässiger Verletzung einer wesentlichen Vertragspflicht haftet GBS in Höhe des typischen und bei Vertragsschluss vorhersehbaren Schadens. In diesem Fall ist der Anspruch auf das doppelte der vom Auftraggeber vertragsgemäß für die letzten 12 Monate vor der Verletzungshandlung geschuldeten Vergütung begrenzt: bei kürzerer Vertragslaufzeit gilt die auf 12 Monate hochgerechnete Vergütung.

d) Die Haftung bei Verletzung von Leben, Körper und Gesundheit und aus dem Produkthaftungsgesetz richtet sich nach den gesetzlichen Vorschriften.

e) Wird der Auftraggeber von einer betroffenen Person auf Schadenersatz in Anspruch genommen, so richtet sich sein Anspruch auf Gesamtschuldnerausgleich gegen GBS nach den vorhergehenden Regelungen.

§ 8 Beendigung des Auftrags

(1) Nach Abschluss der Auftragsverarbeitung hat GBS alle personenbezogenen Daten zu löschen oder zurückzuge ben, soweit nicht eine gesetzliche Verpflichtung zur Speicherung der personenbezogenen Daten besteht.

(2) Der Auftraggeber kann das Auftragsverhältnis ohne Einhaltung einer Frist kündigen, wenn GBS einen schwerwiegenden Verstoß gegen die Bestimmungen dieses Vertrags oder gegen datenschutzrechtliche Bestimmungen begeht und der Auftraggeber aufgrund dessen die Fortsetzung der Auftragsverarbeitung bis zum Ablauf der Kündigungsfrist oder bis zu der vereinbarten Beendigung des Auftrags nicht zugemutet werden kann.

§ 9 Schlussbestimmungen

(1) Sollte das Eigentum der Auftraggeber bei GBS durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlag nahme), durch ein Insolvenzverfahren oder durch sonstige Ereignisse gefährdet werden, so hat GBS den Auftrag geber unverzüglich zu verständigen. Ein Zurückbehaltungsrecht ist in Bezug auf Datenträger und Datenbestände des Auftraggebers ausgeschlossen.

(2) DieVertragsbegründung,VertragsänderungenundNebenabredensindschriftlichabzufassen,was ab dem 25.05.2018 auch in einem elektronischen Format erfolgen kann.

(3) Sollten einzelne Teile dieses Vertrags unwirksam sein, so berührt dies die Wirksamkeit des Vertrags im Übrigen nicht.

Für den Auftraggeber:

Unterschrift / Digitale Signatur:

Ort		
Ort	Datum	Vorname, Name

Für den Auftragnehmer:

Bayreuth,		
Ort, Datum	i.A. Michael Traxler Leiter Service	i.A. Serat Keskin Sachbearbeiter Service

Anhang 1: Auflistung der beauftragten Dienstleistungen, Einzelheiten der Datenverarbeitung und Kontaktdaten des Datenschutzbeauftragten

Gegenstand der Verarbeitung	• Gerätereparaturen • Datenrettung von Diktaten • Installation von Soft- und Hardware beim Auftraggeber (auch Remote) • Wartung, Service und Fehlerbehebung in der GBS- und Fremdsoft- und Hardware (auch Remote) • Managed Server und Services; Bereitstellung von Rechenkapazitäten und Speicherplatz in einem Rechenzentrum sowie Einrichtung, Wartung, Konfiguration und Überwachung der Server
Dauer der Verarbeitung	• Die Daten werden nur zur Erfüllung des Auftrages verarbeitet und für die Dauer der gesetzlichen Gewährleistung aufbewahrt.
Art der personenbezogenen Daten	Da die originäre Verarbeitung von personenbezogenen Daten nicht Gegenstand der hier betroffenen Aufträge ist, kann GBS grundsätzlich mit jeder Art, auch personenbezogenen Daten besonderer Kategorien (Art. 9 DSGVO), in Berührung kommen. Hier zu können u.a. Namen, Adress- und Bankdaten, Mandantendaten und Gesundheitsdaten aus Krankenakten zählen.
Kategorien der betroffenen Personen	Auftraggeber der Dienstleistungen, sowie Kunden, Patienten Mandanten und sonstige Vertragspartner des Auftraggebers
Art und Zweck der Verarbeitung	• Bei der Erbringung der genannten Leistungen kann ein Zugriff bzw. Kenntnis von personenbezogenen Daten nicht ausgeschlossen werden. Bei der Datenrettung werden Diktate wiederhergestellt und gespeichert, bevor sie dem Auftraggeber verschlüsselt zugeschickt werden. • Bei Technikereinsätzen oder dem Remotezugriff auf die Systeme des Auftraggebers oder im GBS Rechenzentrum kann der ausführende Mitarbeiter von GBS ggf. Einsicht in personenbezogene Daten bekommen. • Werden Remotezugriffe mit Einwilligung des Auftraggebers zu Dokumentationszwecken im Rahmen der Gewährleistung aufgezeichnet, können personenbezogene Daten mit der Aufzeichnung abgespeichert werden.

Name und Kontaktdaten des Datenschutzbeauftragten von GBS	Armin Schymala datenschutzbeauftragter@grundig-gbs.com Am Schlag 39 93138 Lappersdorf Telefon: +49 (0) 941 29 84 868 Mobil: +49 (0) 151 50 036 105

Anhang 2: Technische und organisatorische Maßnahmen zum Erhalt des Datenschutzes bei der Grundig Business Systems GmbH & Co. KG

Inhaltsverzeichnis

Technische und organisatorische Maßnahmen zum Erhalt des Datenschutzes bei der Grundig Business Systems GmbH & Co. KG

Zutrittskontrolle			vorhanden ja	vorhanden nein	Beschreibung	geplante Maßnahmen
Zutritts-kontrolle	Schutz vor unbefugten Zutritt zu Datenverarbeitungsanlagen	Automatisches Zugangskontrollsystem	✓		Eingang Gelände	
Zutritts-kontrolle		Bewegungsmelder	✓		im Bereich der Eingänge	
Zutritts-kontrolle		Videoüberwachung der Zugänge	✓			
Zutritts-kontrolle		Schlüsselregelung	✓			
Zutritts-kontrolle		Serverraum abgeschlossen	✓			Integration in automat. Schließsystem
Zutritts-kontrolle		Netzverteiler abgeschlossen	✓			
Zutritts-kontrolle		Chipkarten-Transponder -Schließsystem	✓		Eingang Gelände, Außentüren am Gebäude, Außentore, Serverraum, Abteilungseingänge	
Zutritts-kontrolle		Besucherkontrolle am Empfang	✓		Für alle Besucher, insbesondere Lieferanten	
Zutritts-kontrolle		Externer Wachdienst	✓		täglich 2 Revierkontrollen (nachts)	
Zutritts-kontrolle		Regelung Homeoffice	✓		Mobiles Arbeiten im Rahmen der Betriebsvereinbarung 02/2020 geregelt	

Zugangskontrolle			vorhanden ja	vorhanden nein	Beschreibung	geplante Maßnahmen
Zugangs-kontrolle	Schutz vor unbefugter Nutzung der Datenverarbeitungsanlagen	Zuordnung von Benutzerrechten	✓			
Zugangs-kontrolle		Passwortvergabe	✓			
Zugangs-kontrolle		Authentifizierung mit Nutzername/ und Passwort	✓			
Zugangs-kontrolle		Einsatz von Antiviren Software	✓		Automatische Updates	
Zugangs-kontrolle		Einsatz einer Hardware-Firewall	✓		Sophos XG310 (BT) Sophos XG115 (NBG)	
Zugangs-kontrolle		Einsatz einer Software-Firewall	✓		Microsoft Defender for Business	
Zugangs-kontrolle		Erstellung von Benutzerprofilen	✓			
Zugangs-kontrolle		Einsatz von VPN	✓		Sophos Connect	
Zugangs-kontrolle		Verschlüsselung von Datenträgern in Notebooks	✓		Notebooks der Außendienstmitarbeiter: Bitlocker	

Zugriffskontrolle			vorhanden ja	vorhanden nein	Beschreibung	geplante Maßnahmen
Zugriffs-kontrolle	Maßnahmen, um sicherzustellen, dass die berechtigten Nutzer nur auf Ihre erlaubten Daten zugreifen können und dass personenbezogene Daten nicht unerlaubt verarbeitet werden können	Berechtigungskonzept erstellt.	✓			
Zugriffs-kontrolle		Verwaltung der Rechte durch Systemadministrator	✓		ein Domain-Administratorzugang; Ausführung durch Mitarbeiter IT	
Zugriffs-kontrolle		Anzahl der Systemadministratoren auf das Nötigste beschränkt	✓		2 interne Systemadministratoren und extern 1x EDV-BV	
Zugriffs-kontrolle		Anzahl der lokalen Administratoren auf das Nötigste beschränkt	✓		3 MA auf lokale Adminrechte begrenzt	
Zugriffs-kontrolle		Passwortrichtlinie inkl. Passwortlänge und -wechsel	✓		mind. 8 Stellen /Groß, Klein und Sonderzeichen	
Zugriffs-kontrolle		Einsatz von Dienstleistern bzw. Aktenvernichtern (Datenschutz-Gütesiegel)	✓		Vernichtungsprotokoll	
Zugriffs-kontrolle		Sperre des Rechners beim Verlassen des Arbeitsplatzes	✓		Automatisiert, nicht änderbar durch Benutzer	
Zugriffs-kontrolle		Absperren der Büros im Personalbereich bei Verlassen	✓		separates Schließsystem	

Weitergabekontrolle			vorhanden ja	vorhanden nein	Beschreibung	geplante Maßnahmen
Weitergabe-kontrolle	Maßnahmen, um sicherzustellen, dass personenbezogene Daten während der Übertragung nicht unbefugt verarbeitet werden können	Einrichtung von Standleitungen und VPN-Tunneln	✓		Sophos Connect, SSL Verschlüsselung bei Serverzugriff mit MFA	
Weitergabe-kontrolle		Beim physischen Transport sichere Behälter		■	ein Domain-Administratorzugang; Ausführung durch Mitarbeiter IT	nicht erforderlich
Weitergabe-kontrolle		Erstellen einer Übersicht von regelmäßigen Abruf- und Übermittlungsvorgängen		■	2 interne Systemadministratoren und extern 1x EDV-BV	Übersicht wird erstellt
Weitergabe-kontrolle						

Eingabekontrolle			vorhanden ja	vorhanden nein	Beschreibung	geplante Maßnahmen
Eingabe-kontrolle	Maßnahmen die sicherstellen, dass festgestellt werden kann ob und von wem die Verarbeitung durchgeführt wurde.	Protokollierung der Eingabe, Änderung und Löschung von Daten	✓		Odoo, Sharepoint	
Eingabe-kontrolle		Nachvollziehbarkeit der Eingabe, Änderung und Löschung von Daten durch individuelle Benutzerdaten	✓			
Eingabe-kontrolle		Vergabe von Rechten zur Eingabe, Änderung und Löschung auf Basis eines Berechtigungskonzeptes	✓		Management Handbuch 17.4	

Auftragskontrolle			vorhanden ja	vorhanden nein	Beschreibung	geplante Maßnahmen
Auftragskontrolle	Maßnahmen, um sicherzustellen, dass personenbezogene Daten, die im Auftrag verarbeitet werden nur entsprechend der Weisung des Auftraggebers verarbeitet werden	Auswahl des (Unter-) Auftragnehmers unter Sorgfaltsgesichtspunkten	✓			
Auftragskontrolle		schriftliche Weisungen an den Auftragnehmer (durch Auftragsdaten-Verarbeitungsvertrag)	✓			
Auftragskontrolle		Auftragnehmer mit bestelltem Datenschutz-beauftragten	✓		soweit möglich	
Auftragskontrolle		Verpflichtung der Mit-arbeiter auf das Daten-geheimnis (§5 BDSG/ Artikel 29 EU DSGVO)	✓			
Auftragskontrolle		Vorherige Abfrage/ Prüfung der beim Auf-tragnehmer getroffenen Sicherheitsmaßnahmen	✓		langjährige Zusammen-arbeit; Auditierung tlw. durchgeführt	

Verfügbarkeitskontrolle			vorhanden ja	vorhanden nein	Beschreibung	geplante Maßnahmen
Verfügbar-keitskontrolle	Schutz personenbezogener Daten gegen zufällige Zerstörung und/oder Verlust	Unterbrechungsfreie Stromversorgung (USV) für die Server /und Netz-werkkomponenten	✓			
Verfügbar-keitskontrolle		Klimaanlage in den Serverräumen	✓			
Verfügbar-keitskontrolle		Testen von Datenwiederherstellung	✓			
Verfügbar-keitskontrolle		Aufbewahrung von Datensicherung an einem sichern, ausgelagerten Ort	✓		Datenspeicherung mit getrennten Speicherorten und Brandabschnitten.	
Verfügbar-keitskontrolle		Schutzsteckdosen-leisten in den Server-räumen	✓		VDE und DGUV- Prüfung jährlich	
Verfügbar-keitskontrolle		Serverräume nicht unter sanitären Anlagen	✓			
Verfügbar-keitskontrolle		Backup-& Recovery-konzept	✓			
Verfügbar-keitskontrolle		Serveraum im ersten Stock (Hochwasser)	✓			

Trennungsgebot			vorhanden ja	vorhanden nein	Beschreibung	geplante Maßnahmen
Trennungs-gebot	Maßnahmen, um sicherzustellen, dass zu unterschiedlichen Zwecken erhobe-ne Daten getrennt verarbeitet werden	physikalische getrennte Speicherung auf geson-derten Systemen	✓		Odoo, Sharepoint	
Trennungs-gebot		Logische Mandanten-trennung (SW-seitig)	✓			
Trennungs-gebot		Trennung von Produktiv- und Testsystem	✓		Odoo	
Trennungs-gebot		Festlegung von Daten-bankrechten	✓			

Anhang 3:

Subunternehmen

23 Media GmbH Johann-Krane-Weg 18 48149 Münster	Rechenzentrums- und Wartungsdienstleistungen
Nuance Communications Ireland Limited 20 Merrion Road, Ballsbridge Dublin 4 Irland	Rechenzentrums- und Wartungsdienstleistung, Betrieb von Spracherkennungsserver
EDV-BV GmbH Otto-Hahn-Straße 1 92507 Nabburg	IT-Dienstleister
Hippolyt Thum GmbH Gummistr. 21 95326 Kulmbach	IT Dienstleister für Drucker und Scanner
Braintec	Rechenzentrums- und ERP- Systembetreuung
Plusserver	Rechenzentrums- und Wartungsdienstleistungen