Technische und organisatorische Maßnahmen gemäß Art. 28 Abs. 3 S.2 lit. c i.V.m. Art. 32, Art. 30 Abs. 2 lit. d und g DS-GVO

1. Sicherstellung der Rechtmäßigkeit der Datenverarbeitung

Die Maßnahmen sollen primär die Einhaltung der Gewährleistungsziele Vertraulichkeit, Transparenz, Zweckbindung, Datenminimierung, Nichtverkettbarkeit und Authentizität sicherstellen. Dabei sind auch die Rechte der betroffenen Personen auf Information und nach Art. 7 Abs. 3, 15 ff. DS-GVO sicherzustellen, einschließlich der Schadensminimierungsmaßnahmen und Informationsverpflichtungen gegenüber der Verantwortlichen.

☒ Alle Mitarbeitenden sind über eine Dienstanweisung auf die besondere Sensibilität des Umgangs mit datenschutzrechtlich relevanten Kundendaten hingewiesen worden.	☒ Es liegt ein fortlaufend aktualisiertes Berechtigungskonzept vor, das sicherstellt, dass nur die Mitarbeitenden und auch nur im jeweils erforderlichen Umfang auf die für ihre Aufgabenerfüllung erforderlichen Daten Zugriff erlangen.
☒ Eine über den Auftragsverarbeitungsvertrag hinausgehende Verarbeitung im eigenen Interesse des Auftragnehmers findet derzeit nicht statt, wird den betroffenen Personen in einem solchen Fall aber transparent bekannt gemacht.	☒ Eine Übertragung von personenbezogenen Daten auf private Endgeräte oder Systeme ist technisch und / oder organisatorisch unterbunden.
☒ Datenschutzfreundliche Voreinstellungen der eingesetzten Systeme zur Datenverarbeitung, insbesondere durch eine umfangreiche Pseudonymisierung von personenbezogenen Daten.	☒ Ein Lösch- / Sperrkonzept liegt vor: Nicht mehr erforderliche Daten werden gelöscht oder gesperrt.

2. Zutrittskontrolle

Diese Maßnahmen sollen die Einhaltung der Gewährleistungsziele der Vertraulichkeit, Rechtmäßigkeit, Transparenz, Integrität, Intervenierbarkeit sowie der Nichtverkettbarkeit sicherstellen. Sie betreffen vorrangig Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Gebäuden und Räumen, in denen Daten / Datenträger aufbewahrt werden, oder Datenverarbeitungsanlagen, mit denen schützenswerte Daten verarbeitet oder genutzt werden, enthalten sind, zu verwehren bzw. zu detektieren. Als Maßnahmen zur Zutrittskontrolle können unter anderem automatische Zutrittskontrollsysteme wie Schließsysteme mittels Chipkarten und Transpondern, Kontrolle des Zutritts durch Pförtnerdienste und, ergänzend dazu, Alarmanlagen eingesetzt werden. Server, Telekommunikationsanlagen, Netzwerktechnik und ähnliche Anlagen sind in verschlossenen Schränken (Racks) zu schützen. Darüber hinaus ist es sinnvoll, die Zutrittskontrolle auch durch organisatorische Maßnahmen (z. B. Dienstanweisung, die das Verschließen der Diensträume bei Abwesenheit oder auch das Schließen von Fenstern vorsieht) zu stützen.

☒ Die Schlüsselvergabe zu Büroräumen erfolgt nur an ausgewählte vertrauenswürdige Personen, Inhaber der Schlüssel sind dokumentiert.	☒ Dienstanweisung zum Verschließen von Räumen bei Abwesenheit
☒ Die zugangsberechtigten Personen zur Verfügung gestellten Schlüssel werden personengebunden registriert und die Schlüsselausgabe quittiert.	☒ Geordneter Prozess zur Vergabe und zum Entzug von Zutrittsrechten
☒ Elektronisch gesichertes Zutritts-System mit der Möglichkeit der Sperrung einzelner Schlüssel.	

3. Zugangskontrolle

Diese Maßnahmen sollen die Einhaltung der Gewährleistungsziele der Vertraulichkeit, Verfügbarkeit, Authentizität, Rechtmäßigkeit, Transparenz. Integrität, Intervenierbarkeit sowie der Nichtverkettbarkeit sicherstellen. Sie betreffen in Abgrenzung zur Zutrittskontrolle den Zugang zu Daten und Datenträgern direkt. Um Unbefugten den Zugang zu Daten oder Datenträgern zu verwehren ist mindestens eine Authentifizierung am System vorzusehen.
Möglichkeiten der Zugangskontrolle sind beispielsweise Bootpasswort, Benutzerkennung mit Passwort für Betriebssysteme und eingesetzte Softwareprodukte, automatische Sperre des Bildschirms nach einer angemessenen Spanne von Inaktivität, Verpflichtung der Nutzenden, dessen ungeachtet auch manuell den Bildschirm zu sperren, wenn der Arbeitsplatz verlassen wird oder der Einsatz von Chipkarten zur Anmeldung. Darüber hinaus können auch organisatorische Maßnahmen notwendig sein, um beispielsweise eine unbefugte Einsichtnahme zu verhindern z. B. Dienstanweisungen zur sichtgeschützten Aufstellung von Bildschirmen, Herausgabe von Orientierungshilfen für die Anwender zur Wahl von Passwörtern oder dergleichen.

☒ Mitarbeiter arbeiten ausschließlich mit personalisiert angelegten Benutzerprofilen	☒ Dienstanweisung zum sicherem Umgang mit mobilen Datenträgern und Geräten sowie der Anlage von und dem Umgang mit Passwörtern.
☒ Der Zugang zu IT-Systemen erfolgt mit angemessenem Passwortschutz, der der Sensitivität der verarbeiteten Daten entspricht.	☒ Soweit es für den jeweiligen Zweck ausreichend ist, ist der Zugang zu schützenswerten Daten pseudonymisiert.
☒ Die Verschlüsselung der Daten erfolgt durch die Services der eingesetzten Subdienstleister (insbesondere Microsoft) nach dem aktuellen Stand der Technik.	☒ Schutzsoftware (z. B. Anti-Schadsoftware-Lösungen, Firewalls etc.) wird dem Stand der Technik entsprechend eingesetzt.

4. Zugriffskontrolle

Die Maßnahmen sollen die Einhaltung der Gewährleistungsziele: Vertraulichkeit, Transparenz, Rechtmäßigkeit, Integrität, Authentizität und, Intervenierbarkeit gewährleisten.
Sie sollen gewährleisten, dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können. Die Zugriffskontrolle kann unter anderem gewährleistet werden durch geeignete Berechtigungskonzepte, die eine differenzierte Steuerung des Zugriffs auf Daten ermöglichen. Weiterhin sind geeignete Prozesse, Kontrollmechanismen und Verantwortlichkeiten zu definieren, um die Vergabe und den Entzug der Berechtigungen zu dokumentieren und auf dem aktuellen Stand zu halten (z. B. bei Einstellung, Wechsel des Arbeitsplatzes, Beendigung des Arbeitsverhältnisses). Besondere Aufmerksamkeit ist immer auch auf die Rolle und Möglichkeiten der Benutzerkonten mit erhöhten Berechtigungen (Administratorinnen und Administratoren) zu richten.

☒ Der Zugriff auf personenbezogene Daten wird intern abgestuft nach der jeweiligen Aufgabe eines Mitarbeiters vergeben	☒ Dienstanweisung, die vorsieht, dass Datenanzeigen vor Sichtung durch Unbefugte zu schützen sind und der Arbeitsplatz durch eine passwortgeschützte Bildschirmsperre für Unbefugte zu sperren ist.
☒ Die Daten des Kunden sowie deren Übermittlung werden standardmäßig verschlüsselt. Für die eingesetzten Microsoft-Dienste gilt hierfür der „Datenschutznachtrag zu den Produkten und Services von Microsoft“, für Dropbox das Dokument „Dropbox Business Security“ in seiner jeweiligen Fassung	

5. Trennungskontrolle

Die Maßnahmen sollen primär sicherstellen, dass die Gewährleistungsziele der Transparenz, der Rechtmäßigkeit / Erforderlichkeit sowie der Nichtverkettbarkeit von personenbezogenen Daten eingehalten werden.
Schützenswerte Daten anderer Auftraggeber oder die zu eigenen Zwecken verarbeiteten Daten sind von denen, die im Rahmen dieses Auftragsverarbeitungsvertrages verarbeitet werden, zu trennen.
Zu unterschiedlichen Zwecken erhobene Daten sollen getrennt verarbeitet werden. Insbesondere sollen schützenswerte Daten des Auftraggebers nicht nachteilig von Datenschutz- oder Sicherheitsvorfällen betreffend die Daten des Auftragnehmers oder anderer Kunden in Mitleidenschaft gezogen werden. Dieses kann beispielsweise durch logische oder physikalische Trennung der Daten gewährleistet werden. Jeder Versuch einer nicht gerechtfertigten Re-Identifizierung von pseudonymen Daten ist technisch und / oder organisatorisch zu unterbinden. So sollte zum Beispiel kein Kontakt zu betroffenen Personen hergestellt werden.

☒ Mandantentrennung in den eingesetzten Systemen	☒ Trennung von Test- und Produktionsdaten
☒ Durch ein Berechtigungskonzept ist organisatorisch und technisch sichergestellt, dass Zugriffe auf Dateien nur durch dazu befugte Personen und nur im jeweils erforderlichen Umfang erfolgt.	☒ Dienstanweisung zum Verbot der Datenübertragung auf private Endgeräte oder Datenträger.
☒ Umfangreiche Pseudonymisierung aller personenbezogenen Daten, die nicht im Klartext benötigt werden. Der De-Pseudonymisierungsschlüssel liegt ausschließlich in Systemen des Kunden	

6. Weitergabekontrolle

Die Maßnahmen sollen primär die Einhaltung der Gewährleistungsziele der Verfügbarkeit, der Vertraulichkeit, der Rechtmäßigkeit / Erforderlichkeit, Transparenz, Verfügbarkeit, Intervenierbarkeit sowie der Nichtverkettbarkeit gewährleisten. Personenbezogene Daten dürfen nicht an unbefugte Personen weitergeben werden. Bei der Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträgern dürfen diese nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können. Es muss überprüft und festgestellt werden können, an welchen Stellen eine Übermittlung personenbezogener Daten erfolgt. Zur Gewährleistung der Vertraulichkeit bei der elektronischen Datenübertragung können z. B. Verschlüsselungstechniken (z. B. Virtual Private Network, VPN) eingesetzt werden. Maßnahmen beim Datenträgertransport bzw. Datenweitergabe sind Transportbehälter mit Schließvorrichtung und Regelungen für eine datenschutzgerechte Vernichtung von Datenträgern.

☒ Die Daten des Kunden sowie deren Übermittlung werden standardmäßig verschlüsselt. Für die eingesetzten Microsoft-Dienste gilt hierfür der „Datenschutznachtrag zu den Produkten und Services von Microsoft“, für Dropbox das Dokument „Dropbox Business Security“ in ihrer jeweils aktuellen Fassung	☒ Mitarbeiter arbeiten ausschließlich mit personalisiert angelegten, passwortgeschützten Benutzerprofilen
☒ Dienstanweisung zum Verbot der Datenübertragung auf private Endgeräte oder Datenträger.	☒ Der Zugriff auf personenbezogene Daten wird intern abgestuft nach der jeweiligen Aufgabe eines Mitarbeiters vergeben

7. Eingabekontrolle

Die Maßnahmen sollen primär die Einhaltung der Gewährleistungsziele der, Integrität, Richtigkeit, Rechtmäßigkeit / Transparenz, Authentizität, Verfügbarkeit gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind. Die Eingabekontrolle wird durch Protokollierungen erreicht, die auf verschiedenen Ebenen (z. B. Betriebssystem, Netzwerk, Firewall, Datenbank, Anwendung) stattfinden können. Dabei ist weiterhin zu klären, welche Ereignisse protokolliert werden, wer Zugriff auf Protokolle hat, durch wen und bei welchem Anlass / Zeitpunkt diese kontrolliert werden, wie lange eine Aufbewahrung erforderlich ist und wann eine Löschung der Protokolle stattfinden muss.

☒ Berechtigungskonzept unterscheidet mindestens in Lese – und Schreibrechte.	☒ Eine Eingabe von nicht berechtigten Personen ist ausgeschlossen: ☒ technisch ☒ organisatorisch
☒ Änderungen und Löschungen von Dateien in elektronischen Datenverarbeitungssystemen werden protokolliert	

8. Verfügbarkeitskontrolle

Die Maßnahmen sollen primär die Einhaltung der Gewährleistungsziele der Verfügbarkeit, Transparenz und Intervenierbarkeit gewährleisten. Personenbezogene Daten müssen gegen zufällige Zerstörung oder Verlust geschützt sein. Dazu gehören Maßnahmen zum Diebstahlschutz, unterbrechungsfreie Stromversorgungsanlagen, Klimaanlagen, Brandschutzmaßnahmen, Datensicherungen, sichere Aufbewahrung von Datenträgern, Virenschutz, Raidsysteme, Plattenspiegelungen etc.

☒ Backup- und Wiederherstellungskonzept nach dem Stand der Technik	☒ Regelmäßige stichprobenartige Verfügbarkeitskontrollen für Datenträger.
☒ Vorkehrungen zur Wiederherstellung entsprechend „Datenschutznachtrag zu den Produkten und Services von Microsoft“ und „Dropbox Business Security“ in ihrer jeweils aktuellen Fassung	

9. Datenschutz-Management

Die Maßnahmen sollen die angemessene Umsetzung **aller** datenschutzrechtlichen Gewährleistungsziele bei dem Auftragnehmer sicherstellen. Auf Anfrage ist der Auftraggeber berechtigt, beleghafte Informationen zu den konkreten Maßnahmen zu erhalten, vgl. Haupt- AV-Vertrag.

☒ Vorliegen eines datenschutzkonformen Lösch- / Sperrkonzeptes.	☒ Testverfahren für neue Verarbeitungstätigkeiten sind implementiert und finden nachvollziehbar statt.
☒ Führen eines Verzeichnisses von Verarbeitungstätigkeiten.	☒ Richtlinien zum Umgang mit der Wahrung der Rechte und Freiheiten betroffener Personen welche berücksichtigen ☒ Eine rechtzeitige Information des Auftraggebers über Datenschutz- oder Informationssicherheitsvorfälle ist sichergestellt. Auch Verdachtsfälle sind unverzüglich zu melden. ☒ Richtlinien / Arbeitsanweisungen zum Umgang mit meldepflichtigen Datenpannen.
☒ Administratives Personal für Passwortverwaltung ist benannt und auf das notwendige Maß reduziert.	

10. Auftragskontrolle (Outsourcing an Dritte)

Es muss dafür gesorgt werden, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können. Daher erfolgt keine Auftragsdatenverarbeitung im Sinne von Art 28 DS-GVO ohne entsprechende Weisung des Auftraggebers durch folgende **Mindestanforderungen**:

☒ Eindeutige Vertragsgestaltung	☒ Formalisiertes Auftragsmanagement
☒ Sicherstellung der Datenspeicherung in Europa	