Anlage 2 - Allgemeine technische und organisatorische Maßnahmen gemäß Art. 32 Abs.1 und Anlage 1 AV des Auftragnehmers

Für die Vertragsparteien ist Datenschutz von besonderer Bedeutung.
Zu den gesetzlich auferlegten Pflichten der Auftraggeber gehört es gemäß Art. 28 DS-GVO, zu prüfen, dass die beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen eingehalten, sowie vor Beginn als auch regelmäßig während der Datenverarbeitung dokumentiert werden.
Bei der Inanspruchnahme der Leistungen des Auftragnehmers kann der Auftraggeber davon ausgehen, dass die Anforderungen des Datenschutzes im Sinne der DS-GVO in vollem Umfang gewährleistet sind.
Der folgende Katalog des Auftragnehmers dient als Nachweis für die gesetzlich geforderte Dokumentation der technischen und organisatorischen Maßnahmen zum Datenschutz.

I. Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)

1. Zutrittskontrolle

Maßnahmen, die gewährleisten, dass Unbefugte keinen Zutritt zu den Datenverarbeitungsanlagen erhalten, mit denen personenbezogene Daten verarbeitet werden:

#	Maßnahmen	Maßnahme vorhanden
1	Berechtigungsausweise	Nein
2	Schlüsselregelung	Ja
3	Anwesenheitsaufzeichnungen, Dokumentationspflicht	Ja
4	Sicherung auch außerhalb der Arbeitszeit durch Alarmanlage und/oder Werkschutz	Nein
5	Definierte Sicherheitsbereiche und kontrollierter Zutritt	Ja
6	Gesicherter Eingang für An- und Ablieferung	Ja
7	Türsicherung (elektrischer Türschließer, Ausweisleser, Fernsehmonitor, Pförtner)	Ja
8	Kontrolle durch die Mitarbeiter (4-Augen-Prinzip)	Nein
9	Maßnahmen zur Objektsicherung (z. B. Spezialverglasung, Alarmanlage, Geländebewachung)	Nein
10	Der RZ-Zutritt ist gesichert.	Ja
11	Die Server sind in abschließbaren Räumen.	Ja
12	Datenträger sind unter Verschluss bzw. in abgeschlossenen Räumen.	Ja
13	Die Aufbewahrung von Datensicherungen (z.B. Bänder, CDs) erfolgt im zutrittsgeschützten Safe.	Ja
14	Eine Anweisung zur Ausgabe von Schlüsseln liegt vor.	Ja

2. Zugangskontrolle

Maßnahmen, die sicherstellen, dass Unbefugte an der Benutzung der Datenverarbeitungsanlagen und -verfahren gehindert werden. Diese beziehen sich – im Gegensatz zur Zutrittskontrolle – auf das Eindringen in das EDV-System selbst seitens unbefugter Personen:

#	Maßnahmen	Maßnahme vorhanden
1	Verschlüsselung von Netzwerken liegt vor.	Ja
2	Verschließbarkeit von Datenverarbeitungsanlagen wird gewährleistet.	Ja
3	Identifizierung eines Terminals und/oder eines Terminalbenutzers gegenüber der Datenverarbeitungsanlage	Ja
4	Sicherung von Bildschirmarbeitsplätzen	Ja
5	Regelung der Benutzerberechtigung	Ja
6	Jeder Berechtigte verfügt über ein eigenes nur ihm bekanntes Passwort	Ja
7	Es gibt eine Passwortregelung	Ja
8	Verpflichtung der Mitarbeiter auf das Datengeheimnis liegt vor	Ja
9	Richtlinien für die Dateiorganisation	Ja
10	Protokollierung und Auswertung der Systembenutzung	Ja
11	Kontrollierte Vernichtung von Datenträgern	Ja
12	Arbeitsanweisung und Bearbeitungsverfahren für Datenerfassung	Ja
13	Prüf-, Abstimm- und Kontrollsysteme	Ja
14	Programmprüfungs- und Freigabeverfahren	Ja

3.

4. Zugriffskontrolle

Maßnahmen, die gewährleisten, dass die zur Benutzung der Datenverarbeitungsverfahren Befugten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden personenbezogenen Daten zugreifen können und dass die bei der Bearbeitung verwendeten Daten nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können:

#	Maßnahmen	Maßnahme vorhanden
1	Festlegung der Zugriffsberechtigung, Berechtigungskonzept	Ja
2	Festlegung der Befugnis zur Dateneingabe, -änderung, -löschung	Ja
3	Es besteht eine Trennung von Berechtigungsbewilligung (organisatorisch) und Berechtigungsvergabe (technisch)	Ja
4	Es liegt ein Konzept der Laufwerksnutzung und -zuordnung vor	Ja
5	Auswertung von Protokollen wird durchgeführt.	Ja
6	Ausweisleser am Terminal sind vorhanden.	Nein

7	Teilzugriffsmöglichkeiten auf Datenbestände und Funktionen sind geregelt.	Ja
8	Kontrolle des Zugriffs erfolgt.	Ja

5. Trennungskontrolle

Maßnahmen, die sicherstellen, dass zu unterschiedlichen Zwecken erhobene personenbezogene Daten getrennt verarbeitet werden können.
Es besteht keine Notwendigkeit zu einer physischen Trennung. Eine logische Trennung ist ausreichend.

#	Maßnahmen	Maßnahme vorhanden
1	Die Datensicherungen erfolgt auf separaten Datenträgern und ohne Vermischung von Auftraggeber -Daten mit Daten von Dritten.	Separat: Nein Ohne Vermischung: Ja
2	Es existiert ein Berechtigungskonzept, das der getrennten Verarbeitung der Auftraggeber-Daten von Daten anderer Kunden/Mandanten Rechnung trägt.	Ja
3	Funktionstrennung wird vorgenommen.	Ja
4	Trennung von Entwicklungs-, Test- und Produktivsystem	Ja

6. Auftragskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.
Keine Auftragsdatenverarbeitung im Sinne von Art. 28 DS-GVO ohne entsprechende Weisung des Auftraggebers, z.B.:

#	Maßnahmen	Maßnahme vorhanden
1	Die Mitarbeiter des Auftragnehmers und der Unterauftragnehmer sind auf das Datengeheimnis verpflichtet.	Ja
2	Es liegt ein schriftlicher Vertrag nach § 11 BDSG / Art. 28 DS-GVO zwischen Auftraggeber und Auftragnehmer vor.	Ja
3	Regelung der Rechte und Pflichten des Auftragnehmers und Auftraggebers sind vorhanden.	Ja
4	Regelungen zu technisch-organisatorischen Maßnahmen wurden getroffen.	Ja
5	Die Mitarbeiter des Auftragnehmers und der Unterauftragnehmer sind auf das Datengeheimnis verpflichtet.	Ja

7. Pseudonymisierung (Art. 32 Abs. 1 lit. a DS-GVO; Art. 25 Abs. 1 DS-GVO)

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;

#	Maßnahmen	Maßnahme vorhanden
1	Pseudonymisierung mittels einer eindeutigen Identifikationsnummer (ID). Diese ID wird im System verwendet.	Nein
2	Anonymisierung mittels vollständiger Entfernung / Ersetzung von personenbezogener Daten, ohne das ein erneuter Rückschluss auf eine natürliche Person möglich wäre.	Nein

II. Integrität (Art. 32 Abs. 1 lit.b DS-GVO)

1. Weitergabekontrolle

Maßnahmen, die sicherstellen, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können:

#	Maßnahmen	Maßnahme vorhanden
1	Werden Daten vom Auftragnehmer an den Auftraggeber geschickt?	Ja
2	Erhält der Auftragnehmer Daten vom Auftraggeber?	Ja
3	Welche Versendungsart der Daten besteht zwischen Auftraggeber und Auftragnehmer? ▪ VPN-Verbindung ▪ SSH-Verschlüsselt ▪ SFTP-Transfer ▪ E-Mail Versand mit verschlüsselten ZIP-Dateien ▪ Citrix-Verbindung (128 Bit verschlüsselt)	Ja
4	Verschlüsselung von Daten und Verbindungen beim Transport	Ja
5	Ein Berechtigungskonzept ist vorhanden.	Nein
6	Kontrolle durch Mitarbeiter (4 Augen Prinzip) wird durchgeführt.	Nein
7	Gesicherter Eingang für An- und Ablieferung	nicht relevant
8	Verwaltung von Datenträgern, Bestandskontrolle	Ja
9	Festlegung der Bereiche, in dem sich Datenträger befinden müssen	Nein
10	Verschlüsselung vertraulicher Datenträger	Ja
11	Sicherheitsschränke	Ja
12	Kontrollierte Vernichtung von Datenträgern	Ja
13	Regelung zur Anfertigung von Kopien	Ja
14	Dokumentation der Stellen, an die eine Übermittlung vorgesehen ist, sowie der Übermittlungswege	Ja
15	Plausibilitätsprüfung	Nein
16	Vollständigkeits- und Richtigkeitsprüfung	Nein

2. Eingabekontrolle

Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

#	Maßnahmen	Maßnahme vorhanden
1	Kennzeichnung erfasster Daten wird vorgenommen.	Ja
2	Benutzerberechtigungen (Profile) sind festgelegt?	Ja
3	Sind die Benutzerberechtigungen differenziert? ▪ Lesen, Ändern, Löschen ▪ Teilzugriff auf Daten bzw. Funktionen ▪ Feldzugriff bei Datenbanken	Ja
4	Organisatorische Festlegungen der Zuständigkeiten für die Eingabe liegen vor.	Ja
5	Protokollierung von Eingaben erfolgt.	Nicht alle Systeme Protokollieren eingaben (Server) Teils
6	Es erfolgt eine Kontrolle der Dateneingabe.	Ja
7	Regelungen der Zugriffsberechtigungen liegen vor.	Ja

III. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. B DS-GVO)

1. Verfügbarkeitskontrolle

Maßnahmen, die sicherstellen, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind:

#	Maßnahmen	Maßnahme vorhanden
1	Datensicherungs- und Backupkonzepte sind vorhanden.	Ja
2	Es erfolgt eine redundante Datensicherung.	Ja
3	Aufbewahrung der Daten erfolgt in Datensicherungsschränken, Tresoren.	Ja
4	Es gibt eine USV-Anlage (Unterbrechungsfreie Stromversorgung).	Ja
5	Es werden unberechtigte Benutzer abgewiesen.	Ja
6	Es werden entsprechende Sicherheitssysteme (Software/Hardware) eingesetzt ▪ Virenscanner ▪ Firewalls ▪ SPAM-Filter ▪ Verschlüsselungsprogramme	Ja

2. Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DS-GVO)

#	Maßnahmen	Maßnahme vorhanden
1	Desaster Recovery Plan	Nein
2	Wieder-Anlauftests	Ja
3	Backup-Restore-Tests	Ja
4	Backup-Management	Ja
5	Backup-Überwachung	Ja

IV. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DS-GVO)

#	Maßnahmen	Maßnahme vorhanden
1	Datenschutz-Management	Ja
2	Incident-Response-Management	Ja
3	Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO)	Ja