ANHANG zum AV-Vertrag

Beschreibung der zwischen den Parteien vereinbarten technischen und organisatorischen Maßnahmen zum angemessenen Schutz der Daten des Auftraggebers nach Art. 32 EU-DS-GVO.

Durch die technischen und organisatorischen Maßnahmen werden die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit diesem AV-Vertrag sichergestellt.

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

1.1 Zutrittskontrolle

Maßnahmen, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen die personenbezogenen Daten verarbeitet und genutzt werden, zu verwehren.

		Ja	Nein
a)	Für alle relevanten Standorte sind Sicherheitszonen und deren physischer Schutz in einem Sicherheitszonenkonzept definiert, dokumentiert und kann auf Anfrage vorgelegt werden.	☒	☐
b)	Das definierte Sicherheitszonenkonzept ist für alle relevanten Standorte umgesetzt.	☒	☐
c)	Das Sicherheitszonenkonzept wird min. 1x pro Jahr überprüft.	☒	☐
d)	Die Sicherheitszonen sind für alle relevanten Standorte durch physische Barrieren (Zaun, feste Wände, Türen, Zutrittskontrollanlage, Einbruchmeldeanlage etc.) geschützt, um nur autorisierten Personen Zutritt zu gewährleisten. Besucher in Sicherheitszonen werden durch autorisiertes Personal begleitet.	☒	☐
e)	Es existiert ein dokumentiertes und wirksames Verfahren zur Vergabe, Änderung und Entzug von Zutrittsrechten inkl. Rückgabe der Zutrittsmittel.	☒	☐
Etwaige Abweichungen oder Erläuterungen: Der Server steht in einem abgeschlossenen Raum in einem feuerfesten Serverschrank			

1.2 Zugangskontrolle

Maßnahmen, um zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.

		Ja	Nein
a)	Es existiert ein dokumentiertes und wirksames Zugangskontrollkonzept inkl. Netzwerksicherheitszonen und Netzsegmentierung.	☒	☐
b)	Das Zugangskontrollkonzept definiert die Vergabe, Änderungen und den Entzug von Zugangsrechten sowie deren Freigabe für interne und externe Mitarbeiter.	☒	☐
c)	Die Vorgänge für die Vergabe, Änderungen und den Entzug von Zugangsrechten sowie deren Freigabe werden nachvollziehbar protokolliert.	☒	☐
d)	Das Zugangskontrollkonzept wird mindestens 1x pro Jahr überprüft.	☒	☐
e)	Jede Benutzerkennung ist zu jedem Zeitpunkt eindeutig einer natürlichen Person zugeordnet.	☒	☐

		Ja	Nein
f)	Es werden sichere Passworte verwendet. Aufbau und Handhabung erfolgt gemäß einer dokumentierten Passwortrichtlinie.	☒	☐
g)	Default Passwörter von Systemen und Applikationen (z.B. Oracle, SAP) werden grundsätzlich geändert.	☒	☐
h)	Es wird sichergestellt das Initialkennwörter für Benutzer nach einer kurzen Frist wieder ungültig werden, sofern sie nicht unverzüglich geändert wurden.	☒	☐
i)	Passwörter dürfen nur von dafür berechtigten Personen gemäß definiertem Prozess zurückgesetzt oder geändert werden.	☒	☐
j)	Administratoren nutzen separate Zugänge für das Management von Systemen und deren privilegierte Aktivitäten werden protokolliert.	☒	☐
k)	Die Delegation von Rechten (Vertretungsregelung) erfolgt ausschließlich gemäß definierter Vorgaben.	☒	☐
l)	Alle Mitarbeiter sind angewiesen, ihre Arbeitsplätze zu sperren, wenn sie diese verlassen. Standardmäßig werden Arbeitsplätze mit automatischer Sperre konfiguriert.	☒	☐
m)	Alle Zugänge zu Systemen (Applikationen, Betriebssystemen, BIOS, Boot-Devices etc.) sind mit Passwort gesichert oder gesperrt.	☒	☐
n)	Der externe Zugriff VPN (Remote Access) wird über eine Fritz box mittels starker Verschlüsselung Authentisierung gesichert.	☒	☐

Etwaige Abweichungen oder Erläuterungen:

k) Eine Delegation von Rechten erfolgt nicht – nur Original Rechteinhaber können Funktionen ausüben

1.3 Zugriffskontrolle

Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

		Ja	Nein
a)	Es wird sichergestellt, dass nur die Zugriffsrechte vergeben werden, die zur Erfüllung der jeweiligen Aufgabenstellung erforderlich sind.	☒	☐
b)	Die Vergabe und Freigabe von Zugriffsrechten ist nachvollziehbar dokumentiert, sodass festgestellt werden kann, wer auf die Daten Zugriff hat.	☒	☐
c)	Das Vergabeverfahren und die Zugriffrechte werden regelmäßig geprüft und bestätigt. Zugriffsrechte werden unverzüglich entzogen, sofern sie nicht mehr erforderlich sind.	☒	☐
d)	Für alle Daten ist jeweils ein Verantwortlicher festgelegt, der entscheidet, wer welchen Zugriff erhalten darf.	☒	☐
e)	Zugriffsrechte werden angepasst, wenn sich die Aufgabenstellungen in den Geschäftsabläufen ändern.	☒	☐
f)	In den Applikationen ist sichergestellt, dass die zugeteilten Zugriffsrechte technisch umgesetzt sind.	☒	☐
g)	In allen Umgebungen, die Produktionsdaten enthalten (auch Entwicklung, Test etc.), wird der unbefugte Zugriff ausgeschlossen.	☒	☐

Etwaige Abweichungen oder Erläuterungen:

1.4 Trennungskontrolle

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

		Ja	Nein
a)	Daten, die zu unterschiedlichen Zwecken erhoben wurden, werden so separiert (physisch oder logisch), dass diese dem Zweck entsprechend getrennt verarbeitet, gespeichert und gelöscht werden (Rollen und Berechtigungskonzept).	☒	☐
b)	Entwicklungs-, Test- und Produktivumgebungen sind getrennt.	☒	☐
Etwaige Abweichungen oder Erläuterungen:			

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

	Ja	Nein
Sofern möglich, erfolgt die Verarbeitung mit pseudonymisierten Daten. Die Verarbeitung personenbezogener Daten erfolgt dann in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können.	☐	☒
Etwaige Abweichungen oder Erläuterungen: Das ist nicht gewünscht und möglich, da wir auf Grund der Verarbeitungstätigkeit die wir ausführen, die Klardaten benötigen.		

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

2.1 Weitergabekontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transportes oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

		Ja	Nein
a)	Die Daten werden bei Transport, Speicherung, Übertragung und Verarbeitung außerhalb des geschützten Bereiches des Unternehmens mit Verfahren wie starker Verschlüsselung, Zwei-Faktor-Authentifizierung gesichert (z. B. Festplattenverschlüsselung).	☒	☐
b)	Es sind Anweisungen für die Handhabung von Informationen festgelegt und die Mitarbeiter werden geschult, um den Missbrauch der Daten zu verhindern (z.B. zertifizierte Entsorgung von Papier und Datenträger, Auswahl der Übermittlungsverfahren).	☒	☐
c)	Kryptografische Schlüssel zum Schutz der Daten werden sicher in einem entsprechenden Managementsystem verwaltet.	☒	☐

	Ja	Nein
Etwaige Abweichungen oder Erläuterungen:		

2.2 Eingabekontrolle

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

		Ja	Nein
a)	Die folgenden Ereignisse werden protokolliert (systemseitig oder anderweitig): • An- und Abmelden • Konfigurationsänderungen • Passwortänderungen • Erstellen, Ändern und Löschen von Konten und Gruppen • Änderungen in der Protokollkonfiguration • Aktivierung und Deaktivierung von Sicherheitssoftware wie Virenscanner oder lokaler Firewall • Änderungen von personenbezogenen Daten in Applikationen	☒	☐
b)	Die Nutzung und die Administration von System- und Netzwerkressourcen wird überwacht und die Überwachungsergebnisse werden regelmäßig überprüft.	☒	☐
c)	Log-Systeme und Logging-Informationen werden vor unbefugtem Zugriff, Änderung und Löschung geschützt und regelmäßig ausgewertet.	☒	☐
d)	Die Uhren aller kritischen Systeme werden mit einem zuverlässigen und vereinbarten Zeitserver synchronisiert.	☒	☐
Etwaige Abweichungen oder Erläuterungen:			

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b+c EU-DS-GVO)

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

		Ja	Nein
a)	Es sind Schutzmaßnahmen (USV, Netzersatzanlage, Feuerlöscher, Branderkennung etc.) gegen elementare Gefährdungen - insb. Feuer, Wasser, Ausfall von Versorgungsnetzen, Denial of Service - vorhanden.	☒	☐
b)	Die Daten werden in physisch geschützten Bereichen verarbeitet, die Maßnahmen zur Absicherung des Bereiches sind dokumentiert und werden regelmäßig geprüft.	☒	☐
c)	Anlagen zur Versorgung der Datenverarbeitungssysteme werden regelmäßig gewartet.	☒	☐
d)	Die Nutzung von (System-) Ressourcen wird überwacht und ggf. angepasst, um eine ausreichende Systemkapazität sicherzustellen.	☒	☐
e)	Auf allen Informationssystemen ist ein aktueller Schutz vor Malware, Zero-Day-Exploits oder böswilligem Verhalten von Software installiert, wird zentral verwaltet und auf dem aktuellen Stand gehalten.	☒	☐
f)	Serversysteme werden in sicheren Umgebungen betrieben (z.B. Serverräume oder Rechenzentren) und die Installation in Büros wird unterbunden.	☒	☐

		Ja	Nein
g)	Daten werden so gesichert, dass sie dem Zweck entsprechend separiert in einer definierten Zeit wiederhergestellt werden können.	☒	☐
h)	Bei der Datensicherung werden der Umfang, die Häufigkeit, die Art (voll, differentiell, inkrementell), der Zeitrahmen, eine Verschlüsselung und physisch getrennte Aufbewahrung berücksichtigt und nachvollziehbar dokumentiert.	☒	☐
i)	Bei jeder Änderung des Datensicherungsverfahrens wird die Wiederherstellbarkeit der Daten aus der Datensicherung geprüft.	☒	☐
j)	Eingerichtete Redundanzen (z.B. RAID, Cluster, Load-Balancer) werden, sofern diese nicht kontinuierlich in Betrieb sind, regelmäßig auf Funktion überprüft. Durchgeführte Prüfungen werden dokumentiert.	☒	☐
Etwaige Abweichungen oder Erläuterungen:			

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d EU-DS-GVO; Art. 25 Abs. 1 EU-DS-GVO), Datenschutz-Management

Maßnahmen, die gewährleisten, dass die Datenschutzanforderungen umgesetzt werden und diese auch nachweisbar sind.

		Ja	Nein
a)	Relevante interne und externe Mitarbeiter werden in den Datenschutz eingewiesen und auf diesen verpflichtet.	☒	☐
b)	Interne und externe Mitarbeiter werden für Verarbeitungstätigkeiten/Anwendungen geschult und auf die Folgen von Verletzungen des Datenschutzes hingewiesen.	☒	☐
c)	Die Austrittsverfahren für Mitarbeiter gewährleisten, dass Sicherheitsverletzungen vermieden werden und zur Verfügung gestellte Ausstattung zurückgegeben wird.	☒	☐
d)	Geräte werden so entsorgt, dass keine Daten rekonstruiert werden können.	☒	☐
e)	Die IT-Betriebsverfahren (z. B. User Management, Backup, Netzwerkmanagement) sind nachvollziehbar dokumentiert, werden regelmäßig geprüft und bei Bedarf angepasst.	☒	☐
f)	Alle Änderungen werden im Rahmen eines nachvollziehbar dokumentierten Change-Management Prozesses abgewickelt.	☒	☐
g)	Das Risiko von Datenpannen wird durch Trennung von Verantwortlichkeiten (z. B. System- getrennt von Datenadministration) reduziert.	☒	☐
h)	Identifizierung, Bereitstellung und Test von Updates sind Bestandteil des Regelbetriebes.	☒	☐
i)	Sicherheitsfunktionen von Systemen und Anwendungen sind konfiguriert und aktiviert.	☒	☐
j)	Es existiert ein Regelwerk für Informationssicherheit und Datenschutz.	☒	☐
k)	Das Regelwerk für Informationssicherheit und Datenschutz sowie die Sicherheitsmaßnahmen werden regelmäßig auf Einhaltung und Wirksamkeit geprüft.	☒	☐
l)	Es gibt eine System- und Softwareentwicklungsrichtlinie, die die Aspekte des Datenschutzes beinhaltet.	☒	☐
Etwaige Abweichungen oder Erläuterungen:			

5. Incident-Response-Management

Maßnahmen, die gewährleisten, dass Datenpannen schnell erkannt und gemeldet werden.

		Ja	Nein
a)	Es ist ein an „best practices“ ausgerichteter Prozess (ITIL) eingerichtet, der sicherstellt, dass Sicherheitsvorfälle identifiziert, bewertet und angemessen behandelt werden.	☒	☐
b)	Mit allen relevanten Parteien sind Eskalationsverfahren und organisatorische Schnittstellen definiert und der Datenschutzbeauftragte wird unverzüglich involviert.	☒	☐
c)	Alle Informationssicherheitsvorfälle, die über eine typische geringfügige Störung im Tagesgeschäft hinausgehen, werden unverzüglich ohne weitere Prüfung an festgelegte Stellen gemeldet.	☒	☐
d)	Mitarbeiter, die für die Verwaltung von IT-Systemen / Anwendungen zuständig sind, werden geschult, um Sicherheitsvorfälle zu erkennen, zu klassifizieren und zu melden.	☒	☐
e)	Es ist ein Prozess etabliert, der auch während einer Krise oder eines Desasters für alle kritischen Geschäftsprozesse die Informationssicherheit gewährleistet.	☒	☐
f)	Für einen Notfall / eine Krise sind Prozesse und Verantwortlichkeiten definiert und es finden entsprechende Übungen statt.	☒	☐
Etwaige Abweichungen oder Erläuterungen:			

6. Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 EU-DS-GVO);

Maßnahmen, die gewährleisten, dass Privacy by Default und Privacy by Design berücksichtigt sind.

		Ja	Nein
a)	Bestandteil eines neuen oder zu ändernden Datenverarbeitungsvorgangs ist eine Bewertung der Risiken der Betroffenen und davon abhängig die Identifikation und Realisierung technischer und organisatorischer Sicherheitsmaßnahmen.	☒	☐
b)	Vor Produktionsaufnahme eines neuen oder geänderten Datenverarbeitungsvorgangs wird im Rahmen einer Abnahme geprüft, ob der Datenschutz durch entsprechende Voreinstellungen gegeben ist.	☒	☐
Etwaige Abweichungen oder Erläuterungen:			

7. **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 EU-DS-GVO ohne entsprechende Weisung des Auftraggebers, z.B.: Eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement, strenge Auswahl des Dienstleisters, Vorabüberzeugungspflicht, Nachkontrollen.

		Ja	Nein
a)	Es existieren formelle Vereinbarungen über den Informationsaustausch zwischen den o.g. Vertragsparteien, die die Sicherheit der Daten berücksichtigen.	☒	☐

		Ja	Nein
b)	Vor Aufnahme einer Auftragsverarbeitung wird mit jedem Dienstleister rechtsverbindlich im Rahmen einer AV festgelegt, wie Informationen/Daten zu handhaben sind.	☒	☐
c)	Vor der Beauftragung externer Dienstleister erfolgt eine Bewertung hinsichtlich ihrer Reputation, Qualifikation, Software, Hardware, personellen und finanziellen Ressourcen und Sicherheitsaspekten in Bezug auf ihre zukünftigen Aufgaben.	☒	☐
d)	Die Einhaltung der Verträge wird durch regelmäßige Kontrolle der Vertragsausführung überwacht. Bei Abweichungen werden die definierten Ansprechpartner für Informationssicherheit / Datenschutz involviert und ggf. der Vertrag oder die Vertragsausführung angepasst.	☒	☐
e)	Im Falle einer fristlosen Kündigung werden zusätzliche Maßnahmen ergriffen, die den vorsätzlichen Missbrauch von Infrastruktur oder Daten durch den externen Dienstleister verhindern (z. B. durch Sperren von Zugängen).	☒	☐
f)	Weisungsgeber auf Seiten des Auftraggebers bzw. Weisungsempfänger auf Seiten des Auftragnehmers sind namentlich (oder als Rolle) bekannt.	☒	☐
Etwaige Abweichungen oder Erläuterungen:			