Beschreibung der technischen und organisatorischen Maßnahmen

1 Allgemeine organisatorische Maßnahmen

Maßnahmen, die geeignet sind, eine Sensibilität für Datenschutz zu schaffen.
Folgende allgemeine organisatorische Maßnahmen sind beim Auftragnehmer umgesetzt:

- ☒ Datenschutzbeauftragter wurde bestellt
- ☒ Beschäftigte erhalten Datenschutzschulung/-unterweisung (Art der Schulung: Präsenzschulung)
- ☒ Datenschutzschulungen werden wiederholt:
- ☒ Beschäftigte wurden/werden auf Betriebs-/Geschäftsgeheimnis verpflichtet
- ☒ Beschäftigte wurden/werden auf Datengeheimnis verpflichtet
- ☒ Beschäftigte unterschreiben Verschwiegenheitserklärung

2 Pseudonymisierung / Verschlüsselung

(Art. 32 Abs. 1 lit. a EU-DSGVO)

Maßnahmen, um den Schutz personenbezogener Daten zu gewährleisten, indem diese mittels Hilfsmechanismen in eine pseudonymisierte Form umgewandelt und verarbeitet werden oder mit einer dem Stand der Technik entsprechenden Verschlüsselung vor Zugriffen zu schützen:

- ☐ Personenbezogene Daten werden generell mithilfe eines Verfahrens pseudonymisiert (bitte beschreiben):
- ☐ Personenbezogene Daten werden für Test- und Entwicklungszwecke mithilfe eines Verfahrens pseudonymisiert (bitte beschreiben):
- ☐ Die Rückführung pseudonymisierter Daten in Klardaten ist nur einem begrenzten und autorisierten Personenkreis möglich.
- ☐ Pseudonymisierung und Rückführung werden protokolliert.
- ☐ Daten werden pseudonymisiert an andere Bereiche oder Auftragsverarbeiter übermittelt.
- ☐ Zuordnungsdatei wird getrennt von den pseudonymisierten Daten aufbewahrt (z.B. auf einem separaten, abgesicherten IT-System)
- ☐ Personenbezogene Daten werden generell mithilfe eines Verfahrens anonymisiert (bitte beschreiben):
- ☐ Personenbezogene Daten werden für Test- und Entwicklungszwecke mithilfe eines Verfahrens anonymisiert (bitte beschreiben):
- ☐ Personenbezogene Daten werden bei Erhebung verschlüsselt.
- ☒ Speicherung erfolgt auf verschlüsselten Datenträgern und gesicherten Servern.
- ☒ Einsatz einer starken Verschlüsselung nach Stand der Technik (Bitlocker, FileVault)
- ☒ Verschlüsselte Speicherung personenbezogener Daten auf mobilen Datenträgern (Notebook, Smartphone, USB-Stick, etc.).

- ☒ Mobilgeräte (insbesondere Laptops) sind standardmäßig mit einer Festplatten-verschlüsselung ausgestattet.
- ☐ Einsatz spezieller, verschlüsselter Container bei Nutzung privater Mobilgeräte (z.B. im Rahmen von Bring-Your-Own-Device):
- ☐ Verschlüsselung von Smartphone-Administrations-Software (z. B. zum externen Löschen von Daten)
- ☐ Zugriff über unverschlüsselte Datenträger wird technisch unterbunden (z.B. mittels Policy).
- ☐ Verschlüsselte E-Mail-Kommunikation an interne Adressaten (z.B. PGP, S/MIME).
- ☐ Verschlüsselte E-Mail-Kommunikation an externe Adressaten (z.B. PGP, S/MIME).
- ☐ Nutzung verschlüsselter und gesicherter Austauschplattformen und Sharepoints (z.B. Accellion).
- ☒ Daten werden verschlüsselt an andere Bereiche oder Auftragsverarbeiter übertragen.
- ☐ Für zur Wiederherstellung bestimmte Datenträger werden verschlüsselt an den Lagerort transportiert.
- ☐ Verschlüsselung von Smartphone-Administrations-Software (z. B. zum externen Löschen von Daten)
- ☒ Backups der Datenbank werden vor der Langzeitspeicherung AES-256 verschlüsselt.

3 Vertraulichkeit

(Art. 32 Abs. 1 lit. b EU-DSGVO)

Maßnahmen, welche die Vertraulichkeit der Systeme und Dienste bei der Verarbeitung personenbezogener Daten sicherzustellen.

- ☒ **Angemessene Zugangskontrollen zu Gelände, Gebäude und Serverraum:**
  - ☐ Empfang / Pförtner
  - ☐ Drehkreuz
  - ☐ Alarmanlage
  - ☐ Lichtschranken / Bewegungsmelder
  - ☒ Bereich kann nicht durch mehrere Türen unbemerkt verlassen werden (Notausgänge)
  - ☐ Türen haben Selbstschließer
  - ☒ Sorgfältige Auswahl von Reinigungspersonal
  - ☐ Sorgfältige Auswahl von Wachpersonal
  - ☐ Tragepflicht von Berechtigungsausweisen der Mitarbeiter
  - ☒ Schließsystem zum Firmengelände/Büroräumen mit:
    - ☒ Schlüssel
    - ☐ Magnetstreifenkarte
    - ☐ RFID-Transponder
    - ☐ Codesperre
    - ☐ Smartcard
    - ☐ Fingerabdruck (oder andere biometrische Zugangssperren)

- ☒ Schlüsselausgabe wird protokolliert

☐ ~~Schließsystem zum Serverraum mit~~

- ☐ ~~Schlüssel~~
- ☐ ~~Magnetstreifenkarte~~
- ☐ ~~RFID-Transponder~~
- ☐ ~~Codesperre~~
- ☐ ~~Smartcard~~
- ☐ ~~Fingerabdruck (oder andere biometrische Zugangssperren)~~
- ☐ ~~Zutrittsprotokoll:~~
- ☐ ~~Schlüsselausgabe wird protokolliert~~

☐ ~~Videoüberwachung des Serverraums~~

☐ ~~Videoüberwachung der Türen/Tore o.ä.~~

☒ Besucherregelung vorhanden

- ☐ Hinterlegung von Ausweisen oder anderen Identifikationsdokumenten
- ☐ Abholung des Besuchers durch angestellten Mitarbeiter
- ☒ Besucher werden permanent in den Räumlichkeiten begleitet

☐ **Angemessene Datenträgerkontrollen:**

☒ Führen einer Inventarliste sämtlicher Datenträger in der Infrastruktur

☒ Regelmäßige Kontrolle, ob personenbezogene Datenspeicherung notwendig ist (Umfang und Zweck)

☐ Gehäuseverriegelungen (Rechner, Server, NAS, Multifunktionsdrucker, etc.)

☒ Ordnungsgemäße Vernichtung/Löschung von Daten/Datenträgern/Papier:

- ☒ Physische Löschung von Datenträgern vor Wiederverwendung
- ☐ Ordnungsgemäße Vernichtung von Datenträgern (DIN 66399): Sicherheitsstufe
- ☒ Ordnungsgemäße Vernichtung von Papier (DIN 66399): Sicherheitsstufe
- ☒ Papiervernichtung durch:
- ☐ Protokollierung der Vernichtung

☒ **Angemessene Benutzerverwaltung, sowie dediziertes Benutzer- und Berechtigungskonzept:**

☒ Eindeutige Benutzerkennung

☒ Zentrales Anlegen der Benutzer

☒ Beantragung im 4-Augen-Prinzip

☒ Zuordnung von Benutzerrechten

☒ Erstellen von Benutzerprofilen

☒ Initialpasswort mit Änderungspflicht

☐ Passwortrichtlinie: Passwortlänge mind. 8 Zeichen, Passwortalter max. 99 Tage, Länge Chronik (Anzahl unterschiedlicher Passwörter) 32, Sperrschwelle (Anzahl fehlerhafter Anmeldungen) 5, Bildschirmschoner (mit Sperre) nach 10 Minuten

☐ Passwortkomplexität: 4 Kategorien (Kleinbuchstaben, Großbuchstaben, Zahlen, Sonderzeichen), davon Kategorien:

☐ Sperre Trivialpassworte (Namen usw.)

☒ Schulung zu Passwörtern

☐ Authentifikation mit biometrischen Verfahren

☒ Authentifikation mit Benutzername / Passwort

☒ Zuordnung von Benutzerprofilen zu IT-Systeme

☐ Erstellen eines Berechtigungskonzepts mit Definition der zugeordneten Rechte zu den Rollen

☒ Verwaltung der Rechte durch Systemadministrator

☒ Anzahl der Administratoren auf das „Notwendigste" reduziert

☐ Auswertung unberechtigter Zugriffsversuche

☐ **Einsatz und regelmäßiges Update von Malware-Erkennungs-Software („Antivirensoftware"=AV):**

Updateintervall der AV-Software am Client: Stunden

Updateintervall der AV-Software am Server: Stunden

☒ **Angemessene Benutzerkontrollmaßnahmen:**

☒ Nur autorisierte Personen und Geräte erhalten Zugriff

☒ Anwender müssen sich für Netzwerkanmeldungen authentifizieren

☐ Zugriff auf das Firmennetz nur durch gesicherte Geräte

☐ Firmeneigene Geräte unterliegen einem MDM (Mobile Device Management)

☒ Es gibt ein gesichertes WLAN (mindestens WPA2):

☐ Einsatz einer Hardware-Firewall

☒ Einsatz einer Software-Firewall

☒ Regelmäßige Kontrolle der Firewall-Einstellungen

☒ Fernwartungszugänge werden nur bei Bedarf freigegeben

☒ Benutzerkonten von ausgeschiedenen Mitarbeitern werden unverzüglich gesperrt

☐ Sperrung von cmd/Konsole

☐ Ausschließlich Nutzung von firmeneigenen Mobilgeräten (u.a. Laptops, Tablet-PCs, Smartphones)

☒ Nutzung von privaten Mobilgeräten (u.a. Laptops, Tablet-PCs, Smartphones), z.B. im Rahmen einer Bring-Your-Own-Device-Regelung erlaubt

☐ **Angemessene Protokollierungen:**

- ☐ Protokollierung von Zugriffen und Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten
- ☐ Protokollierung von Zugriffen auf Dateien

☒ **Sicherung bei Übermittlung personenbezogener Daten:**

- ☐ Sichere Transportbehälter/-verpackungen
- ☐ Sorgfältige Auswahl von Transportpersonal und –fahrzeugen
- ☒ Art der Sicherung der Daten zwischen Auftraggeber und Auftragnehmer: Verschlüsselung

☐ **Maßnahmen zur Auftragskontrolle**

- ☒ Auswahl von Subauftragnehmern unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit)
  - ☒ Anhand der Vereinbarung zur Auftragsdatenverarbeitung
  - ☒ Anhand weiterer Dokumente: Standartvertragsklauseln, Privacy-Shield Zertifizierung
  - ☐ Vor-Ort-Kontrolle des Dienstleisters (☐ Mit Bericht, einsehbar)
  - ☒ Dokumentation der Eignung ist einsehbar
  - ☐ Laufende Überprüfung des Sub und seiner Tätigkeiten
- ☐ Verträge mit den Dienstleistern enthalten:
  - ☒ Es gibt zu jedem Dienstleister eine Vereinbarung nach Art. 28 EU-DSGVO
  - ☐ Nur schriftliche Weisungen an den Auftragnehmer zulässig
  - ☐ Es sind weitere Subdienstleister verboten
  - ☐ Es sind weitere Subdienstleister generell erlaubt
  - ☒ Es sind weitere Subdienstleister genehmigungspflichtig
  - ☐ Die Verarbeitung darf nur in D/EU/EWR stattfinden
  - ☐ Weisungskette wurde geprüft und ist sichergestellt
  - ☐ Zusicherung der Vor-Ort-Kontrolle des Dienstleisters
  - ☐ Verpflichtung der Mitarbeiter des Auftragnehmers auf das Datengeheimnis (Art. 29)
  - ☒ Auftragnehmer hat Datenschutzbeauftragten bestellt
  - ☐ Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags
  - ☐ Vertragsstrafen bei Verstößen mit Sub

Es sind Dienstleister im Einsatz für:

☐ Aktenvernichtung	☐ Datenträgervernichtung
☐ IT incl. Fernwartung	☒ Telefonanlage
☐ Kopierer/Drucker (Miete)	☒ Lohnbuchhaltung
☐ Videoüberwachung	☐ Brandschutz/Gebäudesicherheit
☐ Maßnahmen zur Trennbarkeit	

☐ **Weitere Maßnahmen der Zweckbindung/des Trennungsgebots:**

- ☐ Physikalisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern
- ☐ Logische Mandantentrennung (softwareseitig)
- ☐ Erstellung eines Berechtigungskonzepts
- ☐ Eigenständige DB
- ☒ Festlegung von Datenbankrechten
- ☐ Verschlüsselung von Datensätzen, die zu demselben Zweck verarbeitet werden
- ☐ Versehen der Datensätze mit Zweckattributen/Datenfeldern

4 Integrität

(Art. 32 Abs. 1 lit. b EU-DSGVO)

Maßnahmen, die die Integrität der verarbeiteten personenbezogenen Daten sicherstellen.

☐ Maßnahmen zur Speicherkontrolle

- ☐ Einsatz von Intrusion-Detection-Systemen
- ☐ Einsatz und regelmäßiges Update von Malware-Erkennungs-Software („Antivirensoftware"=AV)

  Updateintervall der AV-Software am Client: Stunden

  Updateintervall der AV-Software am Server: Stunden

☒ Fernwartungszugänge werden nur bei Bedarf freigegeben

☐ Maßnahmen zur Zugriffskontrolle

☐ Protokollierung von Zugriffen und Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten

☐ Protokollierung von Zugriffen auf Dateien

Welche Programme sind nicht unter o.g. Benutzerverwaltung (AD, LDAP,…)

☐ Maßnahmen zur Übertragungskontrolle

Für die Datenübermittlung zwischen AN und AG gibt es:

- ☐ Elektronische Übersicht
- ☐ Papier-Übersicht
- ☐ Protokollierung aller Übermittlungen

☐ Maßnahmen zur Eingabekontrolle

Protokollierung der Eingabe, Änderung und Löschung von Daten auf:

- ☐ Dateiebene
- ☐ Maskenebene
- ☐ Feldebene

Die Protokollierung erfolgt durch:

- ☐ Windows
- ☐ Anwendungsprogramm
- ☐ Übergreifendes Tool:

Für die Protokolldaten gibt es:

- ☐ Regelungen zu den Zugriffsbefugnissen
- ☐ Löschregelungen
- ☐ Archivierungsregelungen

☐ Arbeiten mit Gruppenkennungen

☐ Maßnahmen zur Datenintegritätsprüfung

- ☐ Prüfsummen
- ☐ Prüfprogramme und Prüfsummendateien sind gegen Manipulation geschützt:
- ☐ Kryptologische Hashverfahren, welche
- ☐ Prüfintervall
- ☐ Integritätsprüfungen des Dateisystems
- ☐ Integritätsprüfungen des Arbeitsspeichers
- ☐ Automatischer Hinweis im Falle eines Integritätsverlustes:

☒ Auswahl von Subauftragnehmern unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit)

☐ Maßnahmen zur Trennbarkeit

- ☐ Physikalisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern
- ☒ Trennung von Produktiv- und Testsystem
- ☐ Logische Mandantentrennung (softwareseitig)
- ☐ Erstellung eines Berechtigungskonzepts
- ☐ Eigenständige DB
- ☒ Festlegung von Datenbankrechten
- ☐ Verschlüsselung von Datensätzen, die zu demselben Zweck verarbeitet werden
- ☐ Versehen der Datensätze mit Zweckattributen/Datenfeldern

5 Verfügbarkeit

(Art. 32 Abs. 1 lit. b EU-DSGVO)

Maßnahmen und Gewährleistung, dass personenbezogene Daten gegen Zerstörung oder Verlust geschützt sind.

☒ Maßnahmen zur Gewährleistung der Verfügbarkeit

- ☒ Erstellen eines Backup- & Recoverykonzepts
- ☒ Umfang der Sicherung:
  - ☐ Betriebssystem
  - ☐ Betriebssystem und Konfiguration
  - ☒ Datenbanken
  - ☒ Fileserver
- ☒ Art der Sicherung:
  - ☒ Band

- ☒ Festplatte
- ☒ Auf einem anderen System
- ☐ Hot-Standby (Redundant gespiegelt und ständig einsatzbereit)

☐ Maßnahmen zur Transportkontrolle

- ☐ Physische Sicherung beim Transport von Papier/Ordnern/Akten (ggf. auch Datenträger, wenn nicht elektronisch gesichert):
  - ☐ Sichere Transportbehälter/-verpackungen
  - ☐ Sorgfältige Auswahl von Transportpersonal und –fahrzeugen

☒ Maßnahmen zur Wiederherstellbarkeit

- ☒ Notfallpläne vorhanden / gepflegt (letzte Aktualisierung:)
- ☒ Testen von Datenwiederherstellung, Häufigkeit: jährlich, letzte April 2017

☒ Maßnahmen zur Verfügbarkeitskontrolle

- ☒ Unterbrechungsfreie Stromversorgung (USV) ist installiert
- ☐ Unterbrechungsfreie Stromversorgung (USV) wurde getestet
- ☒ Klimaanlage in Serverräumen
- ☒ Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen
- ☒ Aufbewahrung von Datensicherung:
  - ☒ an einem sicheren, ausgelagerten Ort (Art der Datenübertragung: digital, verschlüsselt)
  - ☐ Tresor (Schutzklasse DIS 90)

  Rhythmus (Vollsicherung: , inkrementelle Sicherung:)
- ☒ Nutzung von Cloud-Services
  - ☐ Office 365
  - ☐ Office 365 On-Premise
  - ☐ iCloud
  - ☒ Amazon Cloud
  - ☒ Google-Docs
  - ☐ sonstige:
- ☐ Serverräume nicht unter sanitären Anlagen
- ☐ In Hochwassergebieten: Serverräume über der Wassergrenze

6 Belastbarkeit der Systeme

(Art. 32 Abs. 1 lit. b EU-DSGVO)

Gewährleistung, dass IT-Systeme auch unter hoher Inanspruchnahmefrequenz ordnungsgemäß funktionieren (Performanz). Die Belastbarkeit der IT-Systeme ist grundlegend für die Aufrechterhaltung des Geschäftsbetriebs, also für die Business Continuity. In der englischen Fassung wird von „resilience" gesprochen, so dass hier eher/auch die Begriffe Resilienz bzw. Widerstandsfähigkeit der Systeme bzw. Dienste gemeint sind.
Maßnahmen, welche die Belastbarkeit von Systemen und Diensten sicherstellen sollen:

☒ Maßnahmen zur Belastbarkeit

- ☒ redundante WAN-Anschlüsse
- ☒ Multi-Channel-Bonding (z.B. UMTS/LTE/Glasfaser/Kupfer)

- ☒ Ausreichende Dimensionierung der Storage-Systeme
- ☒ Ausreichende Dimensionierung der Arbeitsspeicher
- ☐ Simulation von Speicherverbrauch durch unter Last angeforderten, aber nicht freigegebenen Speicher
- ☐ provozierter Systemabsturz durch Überlast (Crash-Tests)

☒ Monitoring der Systeme

☒ Monitoring des Netzwerks

☒ Ausfallraten-Statistik

☒ Verfügbarkeits-Statistik

☐ MTBF (mittlere Zeit zwischen zwei Ausfällen)

☒ Ticketsystem

☒ Mit Dienstleistern abgeschlossene Service-Level-Agreements (SLA).

☒ Unterbrechungsfreie Stromversorgung (USV) ist installiert

☐ Unterbrechungsfreie Stromversorgung (USV) wurde getestet (letzter Test): Januar 2018

☒ Klimaanlage in Serverräumen

☒ Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen

☐ redundante WAN-Anschlüsse

☐ Multi-Channel-Bonding (z.B. UMTS/LTE/Glasfaser/Kupfer)

☒ Ausreichende Dimensionierung der Storage-Systeme

☒ Ausreichende Dimensionierung der Arbeitsspeicher

☐ Simulation von Speicherverbrauch durch unter Last angeforderten, aber nicht freigegebenen Speicher

☐ provozierter Systemabsturz durch Überlast (Crash-Tests)

7 Verarbeitung auf Dauer

(Art. 32 Abs. 1 lit. b EU-DSGVO)

Maßnahmen, die sicherstellen, dass eine Verarbeitung auf Dauer integer gewährleistet wird und andererseits die Dauer der Verarbeitung nicht überschritten wird.

☒ Monitoring der Systeme

☒ Monitoring des Netzwerks

☒ Datensicherungsformate ermöglichen langfristige Sicherung und Rücksicherung

☒ Changemanagement vorhanden; Updates werden bspw. nur nach vorherigem Test eingespielt

8 Wiederherstellbarkeit

(Art. 32 Abs. 1 lit. c EU-DSGVO)

Maßnahmen, die sicherstellen, dass Systeme und Dienste zur Verarbeitung personenbezogener Daten im Störungsfall wiederhergestellt werden können.

☐ Systeme und Dienste nach Kritikalität kategorisiert.

- ☒ Backup-Prozeduren nach Kategorisierung und Ressourcen vorhanden.
- ☒ Erreichbarkeit von Administratoren geregelt (ggf. Rufbereitschaft)
- ☒ Vorhandensein von Ausweichrechenzentren (Hot site, warm site, cold site):
- ☐ Verträge mit Notfalllieferanten vorhanden.
- ☒ Mit Dienstleistern abgeschlossene Service-Level-Agreements (SLA).

9 Speicherbegrenzung

(Art. 5 Abs. 1 lit. e EU-DSGVO)

Gewährleistung, dass personenbezogene Daten in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist; personenbezogene Daten dürfen länger gespeichert werden, soweit die personenbezogenen Daten vorbehaltlich der Durchführung geeigneter technischer und organisatorischer Maßnahmen, die von dieser Verordnung zum Schutz der Rechte und Freiheiten der betroffenen Person gefordert werden, ausschließlich für im öffentlichen Interesse liegende Archivzwecke oder für wissenschaftliche und historische Forschungszwecke oder für statistische Zwecke gemäß Artikel 89 Absatz 1 verarbeitet werden („Speicherbegrenzung")
Folgende Maßnahmen der Speicherbegrenzung sind beim Auftragnehmer umgesetzt:

- ☒ Vorliegen Löschkonzept (insbesondere für CRM- und ERP-Systeme)
- ☐ Vorliegen Löschkonzept (für Bürokommunikation wie MS-Office u.a.)
- ☒ Nachweis der Datenlöschung durch Systemprotokolle

10 Regelmäßige Evaluation der Wirksamkeit

(Art. 32 Abs. 1 lit. d EU-DSGVO)

Ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.
Folgende Maßnahmen zur regelmäßigen Evaluation der Wirksamkeit sind beim Auftragnehmer umgesetzt:

- ☐ DSMS
- ☐ ISMS
- ☒ Auswertung von Vorfällen
- ☒ Auswertung und Umsetzung von Verbesserungsvorschlägen
- ☒ Überprüfung der Managementsysteme durch die Geschäftsführung
- ☒ Überprüfung durch den DSB (mit Bericht)
- ☐ Regelmäßige Penetrationstests
- ☐ Regelmäßige Tests zur Datenrücksicherung