ANLAGE 2 zum Vertrag über die Verarbeitung personenbezogener Daten im Auftrag

Technische und organisatorische Maßnahmen gemäß § 64 Abs. 3 BDSG-neu

Der Auftragnehmer (AN) sichert dem Auftraggeber (AG) zu, folgende technische und organisatorische Maßnahmen gemäß § 64 Abs. 3 BDSG-neu und der dazugehörigen Anlage getroffen zu haben:

1. Zugangskontrolle

Verwehrung des Zugangs zu Verarbeitungsanlagen, mit denen die Verarbeitung durchgeführt wird, für Unbefugte.

Die Applikationsserver des AN werden ausschließlich in den Rechenzentren der jeweiligen Cloud Services Provider in dem Gebiet der Europäischen Union gehostet, so findet die Datenspeicherung und Datenverarbeitung von Personenbezogenen Daten ausschließlich in dem EU-Gebiet statt. Der physische Zugang zu den Einrichtungen, mit denen personenbezogene Daten verarbeitet wird, ist durch den jeweiligen Cloud Services Provider ausschließlich auf benannte autorisierte Personen beschränkt, so dass der Zutritt zu IT-Systemen und Datenverarbeitungsanlagen für unbefugten Personen verwehrt wird.

In der Cloud verwendet der AN sowohl Plattform as a Service Dienste (PaaS) als auch Infrastructure as a Service Dienste (IaaS).

Für die Plattform as a Service (PaaS) Dienste:

Cloud Provider führt regelmäßige Systemupdates und Patches auf den unterliegenden physischen und virtuellen Maschinen durch.

Für die Infrastructure as a Service (IaaS):

Der AN führt regelmäßige OS-Aktualisierungen und Sicherheitsupdates auf allen virtuellen Maschinen des Cloud IaaS durch.

Beschreibung des Zugangskontrollsystems:

☒	Alarmanlage	☒	Absicherung von Gebäudeschächten
☒	Automatisches Zugangskontrollsystem	☒	Chipkarten-/Transponder-Schließsystem
☒	Schließsystem mit Codesperre	☒	Manuelles Schließsystem
☐	Biometrische Zugangssperren	☒	Videoüberwachung der Zugänge
☒	Lichtschranken / Bewegungsmelder	☒	Sicherheitsschlösser

☒ Schlüsselregelung (Schlüsselausgabe etc.)

☒ Protokollierung der Besucher

☒ Sorgfältige Auswahl von Wachpersonal

☒ Personenkontrolle beim Pförtner / Empfang

☒ Sorgfältige Auswahl von Reinigungspersonal

☒ Tragepflicht von Berechtigungsausweisen

2. Datenträgerkontrolle

Verhinderung des unbefugten Lesens, Kopierens, Veränderns oder Löschens von Datenträgern.

Die Daten werden auf logischen Datenträgern gespeichert, der physische Transport der Datenträger findet nicht statt, da die Anwendungs-Infrastruktur vollständig beim Cloud Services Provider betrieben wird. Für die Verbindung vom Office zum Rechenzentrum wird eine VPN-Verbindung verwendet (Verschlüsselung: AES 256). Die Übermittlung der personenbezogenen Daten zwischen dem Backend und dem Anwender-UI erfolgt mit einer SSL-Verschlüsselung (minimale erlaubte Verschlüsselung: TLS 1.0). Die Speicherung von nichtverschlüsselten Personenbezogenen Daten in getrennten Applikationsmodulen erfolgt in einer pseudonymisierten Form, so dass die Zuordnung der Daten zu Personen nur über die Referenz-IDs erfolgen kann. Die AN IT-Administratoren haben keinen Zugriff auf gespeicherte personenbezogene Daten, da die einzelnen Datensätze durch die Applikationslogik verschlüsselt und nur durch die Applikationslogik wieder entschlüsselt werden können.

Beschreibung der Datenträgerkontrollsystems:

☒ Verwaltung der Rechte durch Systemadministrator

☒ Anzahl der Administratoren auf das „Notwendigste“ reduziert

☒ Erstellen eines Berechtigungskonzepts

☒ Passwortrichtlinie inkl. Passwortlänge, Passwortwechsel

☒ Verschlüsselung von Datenträgern

☒ physische Löschung von Datenträgern vor Wiederverwendung

☐ Einsatz von Aktenvernichtern bzw. Dienstleistern (nach Möglichkeit mit Datenschutz-Gütesiegel)

☒ Weitergabe von Daten in anonymisierter oder pseudonymisierter Form

☐ Beim physischen Transport: sichere Transportbehälter/-verpackungen

☐ Beim physischen Transport: sorgfältige Auswahl von Transportpersonal und -fahrzeugen

☒ Verschlüsselung/Passwortschutz von Datenträgern in Laptops / Notebooks

☒ Sichere Aufbewahrung von Datenträgern

☒ ordnungsgemäße Vernichtung von Datenträgern (DIN 32757)

☐ Protokollierung der Vernichtung

3. Speicherkontrolle

Verhinderung der unbefugten Eingabe von personenbezogenen Daten sowie der unbefugten Kenntnisnahme, Veränderung und Löschung von gespeicherten personenbezogenen Daten.

Die Erteilung und Änderung der Zugriffsrechte für die AN-Anwendungsadministratoren erfolgt durch die Rollen- und Rechteverwaltung in der Anwendung. Die AN IT-Administratoren haben keinen Zugriff auf gespeicherte personenbezogene Daten, da die einzelnen Datensätze durch die Applikationslogik verschlüsselt und nur durch die Applikationslogik wieder entschlüsselt werden können. Die physikalische Speicherung der Daten erfolgt in der Cloud auf die logische Storage-Einheiten, so dass die Daten dabei fragmentiert und auf mehrere physikalische Laufwerke aufgeteilt werden. Die Daten-Fragmente werden beim Lesen durch die Software-Layer erneut zusammengesetzt.

Beschreibung des Speicherkontrollsystems:

☒	Fragmentierung der Daten bei Speicherung	☒	Verschlüsselung von Datenträgern
☒	Authentifikation mit Benutzername / Passwort	☒	Verschlüsselung/Passwortschutz von Datenträgern in Laptops / Notebooks
☐	Authentifikation mit biometrischen Verfahren	☒	Zuordnung von Benutzerprofilen zu Mandanten

4. Benutzerkontrolle

Verhinderung der Nutzung automatisierter Verarbeitungssysteme mit Hilfe von Einrichtungen zur Datenübertragung durch Unbefugte.

Die AN IT-Infrastruktur befindet sich vollständig in der Cloud. Die IT-Administratoren haben Zugang ausschließlich über persönliche asymmetrische RSA-Keys (2048 Bit), die Keys sind zusätzlich mit individuellen Passwörtern geschützt. Die Anmeldungen der IT-Administratoren auf den Servern werden protokolliert. Jede Erteilung bzw. Änderung der Zugriffsrechte erfolgt nach Vier-Augen-Prinzip und wird protokolliert. Die Erforderlichkeit der Zugriffsrechte der Nutzer wird regelmäßig, alle 90 Tage überprüft. Der Offboarding-Prozess stellt sicher, dass Nutzerzugänge im Falle eines Ausscheidens rechtzeitig widerrufen werden. Die Benutzerkennungen sind eindeutig und individuell. Die Passwörter sind min. 8 Zeichen lang und müssen Ziffern, Sonderzeichen sowie kleine und große Buchstaben enthalten. Die Passwörter müssen nach 90 Tagen geändert werden. In der Passwort-Historie werden die 6 letzten Passwörter gespeichert. Nach 3-facher Fehleingabe erfolgt eine automatische Account-Sperrung.

Beschreibung des Benutzerkontrollsystems:

☒ Zuordnung von Benutzerprofilen zu IT-Systemen	☒ Verwaltung der Rechte durch Systemadministrator
☒ Authentifikation mit Benutzername / Passwort	☐ Authentifikation mit biometrischen Verfahren
☒ Passwortrichtlinie inkl. Passwortlänge, Passwortwechsel	☒ Einsatz von VPN-Technologie
☒ Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten	☒ Einsatz von Anti-Viren-Software

5. Zugriffskontrolle

Gewährleistung, dass die zur Benutzung eines automatisierten Verarbeitungssystems Berechtigten ausschließlich zu den von ihrer Zugangsberechtigung umfassten personenbezogenen Daten Zugang haben.

Die Überwachung des Berechtigungskonzeptes auf der Applikationsebene obliegt dem AG. Das dafür notwendige UI zum Verwalten der Rollen und der Zugriffsrechte wird vom AN zur Verfügung gestellt. Die Änderungen werden protokolliert. Die Erteilung und Änderung der Zugriffsrechte für die AN-Anwendungsadministratoren erfolgt durch dieselbe Rollen- und Rechteverwaltung in der Anwendung.

Beschreibung des Zugriffskontrollsystems:

☒ Erstellen eines Berechtigungskonzepts	☒ Verwaltung der Rechte durch Anwendungs-Administratoren
☒ Anzahl der Administratoren auf das „Notwendigste“ reduziert	☒ Passwortrichtlinie inkl. Passwortlänge, Passwortwechsel
☒ Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten	☒ Mandantentrennung

6. Übertragungskontrolle

Gewährleistung, dass überprüft und festgestellt werden kann, an welche Stellen personenbezogene Daten mit Hilfe von Einrichtungen zur Datenübertragung übermittelt oder zur Verfügung gestellt wurden oder werden können.

Es werden keine Daten weitergegeben, da die Infrastruktur vollständig beim Cloud Provider betrieben wird. Für die Verbindung vom Office zum Rechenzentrum wird eine VPN-Verbindung verwendet (Verschlüsselung: AES 256). Die Übermittlung der personenbezogenen Daten zwischen dem Backend und dem Anwender-UI erfolgt mit einer SSL-Verschlüsselung

(minimale erlaubte Verschlüsselung: TLS 1.0). Die Speicherung von nichtverschlüsselten Personenbezogenen Daten in getrennten Applikationsmodulen erfolgt in einer pseudonymisierten Form, so dass die Zuordnung der Daten zu Personen nur über die Referenz-IDs erfolgen kann.

Beschreibung der Weitergabekontrolle:

- ☒ Einrichtungen von Standleitungen bzw. VPN-Tunneln
- ☐ E-Mail-Verschlüsselung
- ☐ Dokumentation der Empfänger von Daten und der Zeitspannen der geplanten Überlassung bzw. vereinbarter Löschfristen
- ☒ Weitergabe von Daten in anonymisierter oder pseudonymisierter Form
- ☐ Erstellen einer Übersicht von regelmäßigen Abruf- und Übermittlungsvorgängen

7. Eingabekontrolle

Gewährleistung, dass nachträglich überprüft und festgestellt werden kann, welche personenbezogenen Daten zu welcher Zeit und von wem in automatisierte Verarbeitungssysteme eingegeben oder verändert worden sind.

Die Änderungen werden in derselben Datenbank protokolliert, in der auch die zu ändernden Daten gespeichert werden. So gelten für die Protokollierungsdaten die gleichen Regeln wie für die Daten selbst. Die Log-Dateien der Applikationsserver verlassen das geschützte Netzwerk nicht und werden nach 30 Tagen gelöscht. Nur die AN IT-Administratoren haben Zugriff auf das geschützte Netzwerk. Der Zugriff erfolgt über den asymmetrischen RSA-Verfahren mit der 2048-Bit Key-Länge (individuelle Keys).

Beschreibung des Eingabekontrollsystems:

- ☒ Protokollierung der Eingabe, Änderung und Löschung von Daten
- ☒ Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)
- ☒ Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts
- ☐ Erstellen einer Übersicht, aus der sich ergibt, mit welchen Applikationen welche Daten eingegeben, geändert und gelöscht werden können.
- ☐ Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen worden sind

8. Transportkontrolle

Gewährleistung, dass bei der Übermittlung personenbezogener Daten sowie beim Transport von Datenträgern die Vertraulichkeit und Integrität der Daten geschützt werden.

Es werden keine Daten sowie Datenträger transportiert, da die Infrastruktur vollständig beim Cloud Services Provider betrieben wird. Für die Verbindung vom Office zum Rechenzentrum wird eine VPN-Verbindung verwendet (Verschlüsselung: AES 256). Die Übermittlung der personenbezogenen Daten zwischen dem Backend und dem Anwender-UI erfolgt mit einer SSL-Verschlüsselung (minimale erlaubte Verschlüsselung: TLS 1.0). Die Speicherung von nichtverschlüsselten Personenbezogenen Daten in getrennten Applikationsmodulen erfolgt in einer pseudonymisierten Form, so dass die Zuordnung der Daten zu Personen nur über die Referenz-IDs erfolgen kann.

Beschreibung der Transportkontrollsystems:

- ☒ Einrichtungen von Standleitungen bzw. VPN-Tunneln
- ☒ Weitergabe von Daten in anonymisierter oder pseudonymisierter Form
- ☐ E-Mail-Verschlüsselung
- ☐ Erstellen einer Übersicht von regelmäßigen Abruf- und Übermittlungsvorgängen
- ☐ Beim physischen Transport: sorgfältige Auswahl von Transportpersonal und -fahrzeugen
- ☐ Beim physischen Transport: sichere Transportbehälter/-verpackungen

9. Wiederherstellbarkeit

Gewährleistung, dass eingesetzte Systeme im Störungsfall wiederhergestellt werden können.

Es werden regelmäßig Backups der Daten erstellt. Die Backups werden in demselben geschützten Netzwerk aufbewahrt, in dem auch die Daten verarbeitet werden. Die physikalische Speicherung der Backups erfolgt in der Cloud Umgebung auf den dedizierten logischen Storage-Einheiten.

Beschreibung des Wiederherstellbarkeitssystems:

- ☒ Unterbrechungsfreie Stromversorgung (USV)
- ☒ Klimaanlage in Serverräumen
- ☒ Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen
- ☒ Schutzsteckdosenleisten in Serverräumen
- ☒ Feuer- und Rauchmeldeanlagen
- ☐ Feuerlöschgeräte in Serverräumen

- ☒ Alarmmeldung bei unberechtigten Zutritten zu Serverräumen
- ☒ Erstellen eines Backup- & Recoverykonzepts
- ☒ Testen von Datenwiederherstellung
- ☒ Erstellen eines Notfallplans
- ☒ Aufbewahrung von Datensicherung in separaten logischen Storage-Einheiten
- ☒ Serverräume nicht unter sanitären Anlagen

10. Zuverlässigkeit

Gewährleistung, dass alle Funktionen des Systems zur Verfügung stehen und auftretende Fehlfunktionen gemeldet werden.

Die IT-Infrastruktur und die Funktionsfähigkeit der Anwendung wird permanent auf mehreren Ebenen überwacht. Bei Störungen werden qualifizierte Mitarbeiter alarmiert. Die Behebung der Störungen erfolgt nach dem Notfallplan.

Beschreibung des Zuverlässigkeitssystems:

- ☒ Monitoring der IT-Infrastruktur und der Anwendung auf mehreren Ebenen
- ☒ Feuer- und Rauchmeldeanlagen
- ☒ Alarmierung durch Emails und SMS
- ☒ Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen
- ☒ Erstellen eines Notfallplans
- ☒ Serverräume nicht unter sanitären Anlagen

11. Datenintegrität

Gewährleistung, dass gespeicherte personenbezogene Daten nicht durch Fehlfunktionen des Systems beschädigt werden können.

In der Applikationslogik werden umfangreiche Regeln zum Prüfen und Sicherstellen der Datenintegrität implementiert. In der Datenbank wird Datenintegrität u.A. durch Normalisierungskonzepte und Constraints sichergestellt.

Beschreibung des Datenintegritätssystems:

- ☒ Regeln zum Verifizieren der Daten bei der Eingabe und Änderungen
- ☒ Constraints auf Datenbankobjekten
- ☒ Daten-Normalisierung

12. Auftragskontrolle

Gewährleistung, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

Die Auswahl der Unterauftragnehmer erfolgt unter größter Sorgfalt, die Verarbeitung der Daten erfolgt auf Basis des AV-Vertrages gemäß Art. 28 Datenschutz-Grundverordnung.

Beschreibung des Auftragskontrollsystems:

- ☒ Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit)
- ☒ schriftliche Weisungen an den Auftragnehmer (z.B. durch Datenverarbeitungsvertrag)
- ☒ Auftragnehmer hat Datenschutzbeauftragten bestellt
- ☒ Wirksame Kontrollrechte gegenüber dem Auftragnehmer vereinbart
- ☒ vorherige Prüfung der und Dokumentation der beim Auftragnehmer getroffenen Sicherheitsmaßnahmen
- ☒ Verpflichtung der Mitarbeiter des Auftragnehmers auf das Datengeheimnis
- ☒ Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags
- ☒ laufende Überprüfung des Auftragnehmers und seiner Tätigkeiten

13. Verfügbarkeitskontrolle

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

Die Backups werden in demselben geschützten Netzwerk aufbewahrt, in dem auch die Daten verarbeitet werden. Keine Datenträger verlassen das geschützte Netzwerk. Die physikalische Speicherung der Daten erfolgt in der Cloud auf die logische Storage-Einheiten, so dass die Daten dabei fragmentiert und auf mehrere physikalische Laufwerke aufgeteilt werden. Die Daten-Fragmente werden beim Lesen durch die Software-Layer erneut zusammengesetzt. Nur die AN IT-Administratoren haben Zugriff auf das Netzwerk. Der Zugriff erfolgt über den asymmetrischen RSA-Verfahren mit der 2048-Bit Key-Länge (individuelle Keys).

Beschreibung des Verfügbarkeitskontrollsystems:

- ☒ Unterbrechungsfreie Stromversorgung (USV)
- ☒ Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen
- ☒ Feuer- und Rauchmeldeanlagen
- ☒ Alarmmeldung bei unberechtigten Zutritten zu Serverräumen
- ☒ Klimaanlage in Serverräumen
- ☒ Schutzsteckdosenleisten in Serverräumen
- ☐ Feuerlöschgeräte in Serverräumen
- ☒ Erstellen eines Backup- & Recoverykonzepts

☒ Testen von Datenwiederherstellung

☒ Erstellen eines Notfallplans

☒ Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort

☒ Serverräume nicht unter sanitären Anlagen

14. Trennbarkeit

Gewährleistung, dass zu unterschiedlichen Zwecken erhobene personenbezogene Daten getrennt verarbeitet werden können.

Bei der Speicherung der Kundendaten besteht eine logische, bei der Verarbeitung die physikalische Mandantentrennung. Produktiv- und Testsysteme sind voneinander physikalisch getrennt. Die Speicherung von nichtverschlüsselten Personenbezogenen Daten in getrennten Applikationsmodulen erfolgt in einer pseudonymisierten Form, so dass die Zuordnung der Daten zu Personen nur über die Referenz-IDs erfolgen kann.

Beschreibung des Trennbarkaietssystems:

☐ physikalisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern

☒ Logische Mandantentrennung (softwareseitig)

☒ Erstellung eines Berechtigungskonzepts

☐ Verschlüsselung von Datensätzen, die zu demselben Zweck verarbeitet werden

☐ Versehen der Datensätze mit Zweckattributen/Datenfeldern

☐ Bei pseudonymisierten Daten: Trennung der Zuordnungsdatei und der Aufbewahrung auf einem getrennten, abgesicherten IT-System

☒ Festlegung von Datenbankrechten

☒ Trennung von Produktiv- und Testsystem