Anlage 1

Technische und organisatorische Maßnahmen
zur Gewährleistung der Sicherheit der Datenverarbeitung

Der Auftragsverarbeiter sichert zu, folgende technische und organisatorische Maßnahmen getroffen zu haben:

A. Maßnahmen zur Pseudonymisierung

Maßnahmen, die den unmittelbaren Personenbezug während der Verarbeitung in einer Weise reduzieren, dass nur mit Hinzuziehung zusätzlicher Informationen eine Zuordnung zu einer spezifischen betroffenen Person möglich ist. Die Zusatzinformationen sind dabei durch geeignete technische und organisatorische Maßnahmen von dem Pseudonym getrennt aufzubewahren.

Beschreibung der Maßnahmen zur Pseudonymisierung:

- Es werden verschiedene komplexe Methoden genutzt, um Daten zu pseudonymisieren insbesondere Data Masking, Data Salting und Hashing.
- Masking-Vorgaben, Salting-Parameter und Hashing-Algorithmus, die pseudonymisierten Daten sowie die Bezugsdaten werden jeweils getrennt voneinander aufbewahrt.
- Dynamisches Data Masking ermöglicht es den Kunden selbst zu bestimmen, inwieweit Daten mit minimaler Auswirkung auf die Anwendungsschicht offengelegt werden sollen.
- Es ist sichergestellt, dass personenbezogene Daten nur insoweit entpseudonymisiert und eingesehen werden können, wie es für die konkrete Verarbeitung nötig ist. Daten können sicher und umgehend anonymisiert werden. Pseudonymisieren, Anonymisieren und Überschreiben personenbezogener Daten kann vollständig und umgehend umgesetzt werden.

B. Maßnahmen zur Verschlüsselung

Maßnahmen oder Vorgänge, bei denen ein klar lesbarer Text / Information mit Hilfe eines Verschlüsselungsverfahrens (Kryptosystem) in eine unleserliche, das heißt nicht einfach interpretierbare Zeichenfolge (Geheimtext) umgewandelt wird:

Beschreibung der Verschlüsselungsmaßnahmen:

- Alle sensiblen Daten werden per 256-bit AES verschlüsselt.
- Ende-zu-Ende-Verschlüsselung mit vom Kunden verwalteten Schlüssel.
- Ver- und Entschlüsselung der Datenbank, der zugehörigen Backups und der Transaktionsprotokolldateien im Ruhezustand in Echtzeit.
- Jegliche Kommunikation mit TLS-Verschlüsselung über das jeweils aktuelle TLS-Protokoll.

C. Maßnahmen zur Sicherung der Vertraulichkeit

1. Zutrittskontrolle

Maßnahmen, die unbefugten Personen den Zutritt zu IT-Systemen und Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet werden, sowie zu vertraulichen Akten und Datenträgern physisch verwehren:

Beschreibung des Zutrittskontrollsystems:

Bürostandort:

- Gebäudezutritt gesichert über Chipkarte/Schlüssel.
- Mieterbezogene Chipkartenverwaltung/Schlüsselverwaltung.
- Organisationsanweisung für Chipkartenausgabe/Schlüsselausgabe.
- Geräte werden nach Dienstschluss in verschlossenen Schränken verwahrt.

Serverstandort (Subdienstleister):

- Wachpersonal 24/7.
- Gesichertes Gelände (Zaun, Kameras).
- Gesicherte Gebäude mit zweistufiger Authentifizierung.
- Zutritt zur Rechenzentrumsetage nur nach vorheriger Personenkontrolle mit Metalldetektor. Beides wird beim Verlassen wiederholt.
- Dokumentiertes Zutritts- und Identifizierungssystem.
- Zutritt nur nach vorheriger Anmeldung unter Angabe eines triftigen Grundes (z. B. Compliance-Maßnahmen).

2. Zugangskontrolle

Maßnahmen, die verhindern, dass Unbefugte datenschutzrechtlich geschützte Daten verarbeiten oder nutzen können.

Beschreibung des Zugangskontrollsystems:

- Personalisierte Nutzerkonten.
- Kennwortverfahren, d.h. persönlicher und individueller User Log-In bei Anmeldung am System (u.a. Sonderzeichen, Mindestlänge von 16 Zeichen, regelmäßiger Wechsel des Kennwortes).
- Protokollierung der Anmeldeversuche und Abbruch des Anmeldevorgangs nach individueller Zahl von erfolglosen Versuchen. Smart Lockout: wird immer wieder das gleiche falsche Passwort versucht (Indiz für Berechtigte, die ihr Passwort verwechselt oder vergessen haben) wird langsamer gesperrt, als wenn verschieden Passwörter ausprobiert werden (Indiz für Eindringling). Dies geschieht selbstverständlich über Hash-Werte, so dass die Vertraulichkeit der Passwörter jederzeit gewahrt ist.
- Vollständige Trennung der verschiedenen Umgebungen (Test-, Produktiv-, Entwicklungssystem) in Virtual Sub-Networks.

- Vollständige Trennung der verschiedenen Kunden in Virtual Sub-Networks.
- Access Management.
- Protokollierung der internen Nutzeraktivitäten.
- Keinerlei Nutzung externer Speichermedien (z. B. USB-Sticks).
- Multi-Faktor-Authentifizierung bei Zugang zu sensiblen Daten.
- Automatische Rechnersperre bei Inaktivität.
- Verbindliche Vorgaben zur Berechtigungsvergabe und Passwortrücksetzung.
- Begrenzung der Anzahl berechtigter Mitarbeiter.
- Automatische und regelmäßige Überprüfung der Antiviren- und Spyware-Filter.

3. **Zugriffskontrolle**

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

Beschreibung des Zugriffskontrollsystems:

- Rollenbasiertes, granulares Berechtigungskonzept.
- Dokumentation der Berechtigungsvergabe.
- Trennung des Berechtigungsbewilligung von technischer Berechtigungsvergabe.
- Datenbankzugriff streng reglementiert.
- Protokollierung der internen Nutzeraktivitäten.
- Protokollierung von Zugriffen und Missbrauchsversuchen.
- Blockieren von Ein- und Ausgabeschnittstellen (z.B. USB-Sticks).

4. Trennungsgebot

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden und so von anderen Daten und Systemen getrennt sind, dass eine ungeplante Verwendung dieser Daten zu anderen Zwecken ausgeschlossen ist.

Beschreibung des Trennungskontrollvorgangs:

- Rollenbasiertes, granulares Berechtigungskonzept, das die getrennte Verarbeitung von Daten verschiedener Kunden gewährleistet.
- Dokumentation der Berechtigungsvergabe.
- Verschlüsselte Speicherung sensibler Daten (256-bit AES).
- Vollständige Trennung der verschiedenen Umgebungen (Test-, Produktiv-, Entwicklungssystem) in Virtual Sub-Networks.

D. Maßnahmen zur Sicherung der Integrität

1. Datenintegrität

Maßnahmen, die gewährleisten, dass gespeicherte personenbezogene Daten nicht durch Fehlfunktionen des Systems beschädigt werden:

Beschreibung der Datenintegrität:

- Einspielen neuer Releases und Patches unter strengem mehrstufigem Management: Proofing, Aprooving, Testing (funktionales und nicht-funktionales Testing, Ergebniskontrolle) vor dem Release.
- Logging des Release- und Patch-Management sowie der Geschäftsprozesse.
- Redundante Speichersysteme und Datenbanken.
- Tägliche Backups.

2. Übertragungskontrolle

Maßnahmen, die gewährleisten, 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:

Beschreibung der Übertragungskontrolle:

- Logging der Geschäftsprozesse sowie der Datenübertragungen.
- Überwachung und Kontrolle unbefugter Datenübertragungen.
- Es ist sicherheitsarchitektonisch sichergestellt, dass Daten nur verschlüsselt und gemäß des rollenbasierten, granularen Berechtigungskonzepts übertragen werden.

3. Transportkontrolle

Maßnahmen, die gewährleisten, dass bei der Übermittlung personenbezogener Daten sowie beim Transport von Datenträgern die Vertraulichkeit und Integrität der Daten geschützt werden:

Beschreibung der Transportkontrolle:

- Übermittlung von Daten nur verschlüsselt (256-bit EAS, TLS 1.3).
- Transportprozesse mit individueller Verantwortlichkeit
- Verschlüsselungsverfahren, die Datenveränderungen während des Transports aufdecken.
- Keinerlei Nutzung externer Datenträger (USB-Sticks, externe Festplatten).
- Umfassende Protokollierungsverfahren.
- Regelmäßiges Patching der Verschlüsselungsverfahren.
- Automatische Rotation der Zugriffsschlüssel.

4. **Eingabekontrolle**

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

Beschreibung des Eingabekontrollvorgangs:

- Protokollierung aller Systemaktivitäten und Aufbewahrung der Protokolle für sechs Monate.
- Protokollierung der Administration (Anlegen und Ändern von Nutzern und Berechtigungen).
- Protokollauswertungssysteme.
- Digitale Signaturen.

E. Maßnahmen zur Sicherung der Verfügbarkeit und Belastbarkeit

1. Verfügbarkeitskontrolle

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

Beschreibung des Verfügbarkeitskontrollsystems:

- Datensicherungsverfahren.
- Unterbrechungsfreie Stromversorgung am Serverstandort.
- Archivierungskonzept.
- Feueralarmsystem (Büro- und Serverstandort).
- Feuerlöschsystem (Serverstandort).
- Klimaanlage (Serverstandort).
- Vollständiges Backup- und Recovery-Konzept (RPO: 5 Sekunden, TRO: 30 Sekunden) und katastrophensicherer Aufbewahrung der Datenträger.
- Notfall- und Wiederanlaufverfahren mit regelmäßiger Erprobung.
- Sachkundiger Einsatz von Schutzprogrammen (Virenscanner, Firewalls, Verschlüsselungsprogramme, SPAM-Filter).

2. Rasche Widerherstellbarkeit

Maßnahmen, die die Fähigkeit sicherstellen, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen.

Beschreibung der Maßnahmen zur raschen Widerherstellbarkeit:

- Redundante Auslegung aller Systeme.
- Regelmäßige Tests der Datenwiederherstellung.
- Notfallpläne.

3. Zuverlässigkeit

Maßnahmen, die gewährleisten, dass alle Funktionen des Systems zur Verfügung stehen und auftretende Fehlfunktionen gemeldet werden:

Beschreibung der Maßnahmen zur Zuverlässigkeit:

- Automatisches Monitoring mit E-Mail-Benachrichtigung.
- Notfallpläne mit Verantwortlichkeiten.
- IT-Notdienst 24/7.
- regelmäßige Tests der Datenwiederherstellung.

F. Maßnahmen zur regelmäßigen Evaluation der Sicherheit der Datenverarbeitung

1. Überprüfungsverfahren

Maßnahmen, die die datenschutzkonforme und sichere Verarbeitung sicherstellen.

Beschreibung der Überprüfungsverfahren:

- Verpflichtung der Mitarbeiter auf die Vertraulichkeit/ datenschutzrechtliche Schulung der Mitarbeiter.
- Regelmäßige Re-Zertifizierung.
- Formalisierte Prozesse für Datenschutzvorfälle.
- Weisungen der Auftraggeber werden dokumentiert.
- Formalisiertes Auftragsmanagement.

2. Auftragskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können:

Beschreibung der Maßnahmen zur Auftragskontrolle:

- Weisungen der Auftraggeber werden dokumentiert.
- Formalisiertes Auftragsmanagement.