Anlage 1 – Technisch-organisatorische Maßnahmen

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

1.1 Zutrittskontrolle

Über die Zutrittskontrolle wird Unbefugten der Zutritt verwehrt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden.

Es existieren folgende Maßnahmen zur Zutrittskontrolle:

Rechenzentrum

(1) Im Rechenzentrum befinden sich die Server, auf denen zentral die Daten gespeichert und verarbeitet werden. Das Rechenzentrum wird von der Fa. Profitbricks betrieben (Standort: Karlsruhe, doppelt redundante Speicherung, zertfiziert nach ISO 27001, ISO 9001). Es wird darauf geachtet, dass:

a) der Zutritt zum Rechenzentrum nur autorisierten Personen gestattet ist;

b) der Zutritt durch ein materielles (RFID-Chip) und ein geistiges (PIN) Identifikationsmerkmal gesichert ist. Es wird zwischen fest zugewiesenen und beim Sicherheitsdienst zur Abholung hinterlegten Zutrittsberechtigungen unterschieden. Bei Zutrittsberechtigungen, die zur Abholung hinterlegt sind, wird die Autorisierung durch Kontrolle des Personalausweises sichergestellt. Die Daten werden bei einem Sicherheitsdienst hinterlegt (Whitelist), so wird gewährleistet, dass nur berechtigte Personen das Rechenzentrum betreten können;

c) der Zutritt zu den einzelnen Kundenschränken oder -flächen ausschließlich durch den Kunden und durch das zuständige Personal möglich ist;

d) die Zutrittskontrollsysteme sowie die Alarmanlagen über USV und Netzersatzanlage gegen Stromausfall gesichert sind;

e) das Rechenzentrum, insbesondere der Zutritt zu Sicherheitsbereichen mit Videoüberwachung ausgestattet ist; Auffälligkeiten werden berichtet. Die vorgegebenen Laufwege des Wachdienstpersonals werden protokolliert.

Büroräume

(1) In den Büroräumen der AHB Systeme in Mannheim befinden sich normalerweise keine unverschlüsselten Daten. Einzige Ausnahme ist eine temporäre Kopie der Daten einzelner Kunden für spezielle Support-Aufgaben (z.B. Fehlersuche mittels Debugger, s. Zugriffskontrolle).

(2) Die Zugänge zu den Büroräume der AHB Systeme in Mannheim sind gegen unbefugten Zutritt abgesichert – d.h. dass:

a) jedwede Außentüren mit einem manuellen und technischen Schließsystem (Sicherheitsschlösser) versehen und grundsätzlich verschlossen sind;

b) die den Mitarbeitern zur Verfügung gestellten Schlüssel personengebunden registriert sowie die Schlüsselausgabe quittiert wird;

c) VPN-Technologie (SSL/TLS) eingesetzt wird;

d) Besucher nur in Begleitung eines Mitarbeiters sich in den Räumlichkeiten bewegen können;

e) Personal von Dritten, insbesondere für Reinigungs- und Wartungsaufgaben sorgfältig ausgewählt wird;

1.2 Zugangskontrolle

Über die Zugangskontrolle wird verhindert, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.

Es existieren folgende Maßnahmen zur Zugangskontrolle:

(1) Die Server im **Rechenzentrum** verfügen zur Administration über entsprechende Benutzerkonten. Die Administration der Server erfolgt über das Internet über ein verschlüsseltes TLS-Protokoll. Die Kennwörter für diese Benutzerkonten sind nur der Geschäftsführung bekannt. Zusätzlich gibt es ein Administrator-Konto für den Zugriff von Mitarbeitern des Rechenzentrums zur Ausführung von Arbeiten im Rahmen des vertraglich vereinbarten Service-Managements.

(2) Der Zugang zu den Rechnern in den **Büroräumen** wird über Benutzerkonten kontrolliert. Hierzu hat jeder Mitarbeiter ein eigenes Benutzerkonto sowohl für den lokalen Rechner, als auch für die Verwaltungssoftware, mit deren Hilfe auf die Kunden- und Verwaltungsdaten im Rahmen des Supports kontrolliert zugegriffen werden kann.

1.3 Zugriffskontrolle

Die Zugriffskontrolle gewährleistet, 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.

Die unerlaubte Tätigkeit in Datenverarbeitungssystemen außerhalb eingeräumter Berechtigungen wird im Besonderen verhindert, dadurch dass:

(1) die Zugriffsrechte (sowohl für Anwender, wie auch für Administratoren) sich an den aufgabenbedingten und datenschutzrechtlichen Erfordernissen orientieren (Berechtigungskonzept nach dem need-to-know-Prinzip),

(2) Passwortrichtlinien inkl. Passwortlänge und Passwortwechsel vorgegeben werden,

(3) der Zugriff auf Anwendungen (Eingabe, Veränderung und Löschung) protokolliert wird und ausgewertet werden kann (mindestens für 14 Tage),

(4) Schutz gegen unberechtigte interne und externe Zugriffe durch Verschlüsselung und Firewalls besteht.

1.4 Trennungskontrolle

Die Trennungskontrolle garantiert die getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden, z.B. Mandantenfähigkeit, Sandboxing.

Es existieren folgende Maßnahmen zur Trennungskontrolle:

(1) Alle AHB-Anwendungen sind per Design mandantenfähig. D.h. alle Zugriffe auf die Daten in der Datenbank erfolgen strikt nach der Mandantennummer des Kunden.

1.5 Pseudonymisierung (Art. 32 Abs. 1 lit. a) DSGVO; Art. 25 Abs. 1 DSGVO)

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.

Es existieren keine Maßnahmen zur Pseudonymisierung, da dies in den AHB-Anwendungen nicht sinnvoll bzw. relevant ist.

2. Integrität (Art. 32 Abs. 1 lit. b DSGVO)

2.1 Weitergabekontrolle

Die Weitergabekontrolle gewährleistet, 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, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

Es existieren folgende Maßnahmen zur Weitergabekontrolle:

(1) Einziger Speicherort der Daten ist das Rechenzentrum, die restriktive Zutritts- und Zugangskontrolle des Rechenzentrums garantieren die Weitergabekontrolle. Das unbefugte Lesen, Kopieren, Verändern oder Entfernen von im Rechenzentrum gespeicherten Daten durch den Rechenzentrumsbetreiber ist vertraglich ausgeschlossen.

(2) Der Transport außerhalb des jeweiligen Netzwerks erfolgt verschlüsselt (TLS, VPN). Hierzu werden starke Verschlüsselungsalgorithmen eingesetzt.

2.2 Eingabekontrolle

Die Eingabekontrolle gewährleistet, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

Es existieren folgende Maßnahmen zur Eingabekontrolle:

(1) Protokollierung und Nachvollziehbarkeit von Eingaben, Änderungen und Löschung von Daten (Änderungshistorie, Aufbewahrungsdauer 1 Jahr).

(2) Die Änderungshistorie ist von jedem Kunden für eine Daten einsehbar.

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)

3.1 Verfügbarkeitskontrolle (Art. 32 Abs. 1 lit. c) DSGVO)

Die Verfügbarkeitskontrolle gewährleistet, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

Zur Durchsetzung der Verfügbarkeit hat der Auftragnehmer veranlasst, dass:

(1) eine Backup Strategie existiert: neben der doppelt redundanten Datenspeicherung alle 4 Stunden verschlüsselte Komplettsicherungen der Kundendaten

(2) eine unterbrechungsfreie, redundante Stromversorgung besteht (USV und Notstromaggregate),

(3) Räumlichkeiten in Brandabschnitten versehen mit einzelnen Brandschutzeinrichtungen (Feuer- und Rauchmeldeanlagen, Feuerlöscher) eingeteilt sind,

(4) redundante Klimaanlagen vorhanden sind, Luftfilter gemäß DIN EN 779 G4,

(5) eine Notfallmatrix besteht.

3.2 Rasche Wiederherstellung (Art. 32 Abs. 1 lit. c DSGVO)

Es existieren folgende Maßnahmen zur raschen Wiederherstellung:

(1) Backup- und Recoverykonzept: Untertägige und tägliche Sicherung aller Daten, 7 Tage Aufbewahrung

(2) Regelmäßige Testläufe zur Datenwiederherstellbarkeit

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO; Art. 25 Abs. 1 DSGVO)

Es existieren folgende Maßnahmen zur regelmäßigen Überprüfung, Bewertung und Evaluierung:

4.1 Datenschutz-Management

Alle Mitarbeiter sind auf das Datengeheimnis verpflichtet. Es erfolgt eine regelmäßige Unterweisung der Mitarbeiter im Datenschutz. Ein Datenschutzkonzept und eine IT-Policy wurden erstellt.

4.2 Incident-Response-Management

Unterstützung bei der Reaktion auf Sicherheitsverletzungen.

Firewalls, Spamfilter und Virenscanner werden eingesetzt und regelmäßig aktualisiert. Eine interne Anweisung regelt den Umgang mit Sicherheitsvorfällen, falls erforderlich erfolgen Meldungen gegenüber den Aufsichtsbehörden.

4.3 Auftragskontrolle

Die Auftragskontrolle stellt sicher, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

Als einziger Datenverarbeiter mit möglichem Zugang zu den Daten ist die Fa. Profitbricks GmbH als Rechenzentrumsbetreiber nach vorheriger Prüfung der dort getroffenen Sicherheitsmaßnahmen beauftragt. Es besteht eine schriftliche Vereinbarung zur Auftragsverarbeitung über die sichergestellt ist, dass die Daten nur entsprechend den Weisungen der AHB Systeme verarbeitet werden. Eine Nutzung oder Weitergabe der Daten durch Mitarbeiter des Rechenzentrums ist vertraglich ausgeschlossen.

4.4 Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO)

Privacy by design / Privacy by default.

Es werden nicht mehr personenbezogene Daten erhoben, als für den jeweiligen Zweck erforderlich sind. Keine Vorbelegungen bei datenschutzrelevanten Einstellungen der Benutzer.