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

1. 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 Pseudonymisierung:

Innerhalb der Plattform wird auf Datensätze von Personen lediglich mit Referenzen gearbeitet. So wird sichergestellt, dass es innerhalb der Plattform ausschließlich einen Ort gibt, in dem personenbezogene Daten vorliegen. Diese Vorgabe ist software-architektonisch beschrieben und dokumentiert. Im Rahmen der Entwicklung wird die Vorgabe durch Reviews von Codes sowie von technischer Planung vorab der Entwicklung geprüft und sichergestellt. So kann gewährleistet werden, dass:

- Die Daten sensibel verwendet werden. Daten zur Person werden nur zur Verfügung gestellt, wenn die benötigte Funktionalität dies voraussetzt.
- Die Daten schnell und sicher anonymisiert werden können. Das Überschreiben der personenbezogenen Daten hat einen sofortigen und globalen Effekt.

2. 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:

- SSL-Verschlüsselung
- Verschlüsselung aller Datenleitungen:
    1. HTTPS/WSS
    2. TCP/IP Sockets
- Verschlüsselte VPN-Verbindung auf Server
- TLS Verschlüsselung über TLS 1.2 Protokoll

3. Maßnahmen zur Sicherung der Vertraulichkeit

3.1. 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:

- Verschluss von Clients in Schränken nach Dienstschluss
- Zutritt des Gebäudes nur über Chipkarten
- Mieterbezogene Chipkartenverwaltung

- Organisationsanweisung zur Ausgabe von Chipkarten

Serverstandort (durch Subdienstleister):

- Gesicherte Fenster (z.B. vergittert, Sicherheitsglas)
- Mit Schloss gesicherte Räume (z.B. Zahlenschloss, Schlüssel, Biometrieschloß, Transponder)
- Gelände durch Zaun mit Bewegungsmeldesystem geschützt
- Dokumentiertes Zutritts-ID-System
- 24/7 Wachpersonal vor Ort

3.2. Zugangskontrolle

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

Beschreibung des Zugangskontrollsystems:

- Personalisierte Nutzer-Accounts
- Revisionssicheres, verbindliches Verfahren zur Rücksetzung „vergessener“ Passwörter vorhanden
- Revisionssicheres, verbindliches Verfahren zur Vergabe von Berechtigungen vorhanden
- Richtlinie zum sicheren, ordnungsgemäßen Umgang mit Passworten
- Automatische, passwortgeschützte Bildschirm- und Rechnersperre
- Serversysteme nur mit Konsolenpasswort oder über passwortgeschützte, verschlüsselte Verbindung administrierbar
- Clientsysteme nur nach mindestens passwortgestützter lokaler bzw. zentraler Authentifizierung nutzbar
- Automatisierte Standardroutinen für regelmäßige Aktualisierung von Schutzsoftware (z. B. Virenscanner)
- Drucker nur für berechtigte Personen im Netzwerk zugänglich

3.3. 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 Berechtigungskonzept
- Dokumentation der Berechtigungen
- Streng reglementierter Datenbankzugriff
- Direkter Server-Zugriff auf CTO und DevOps beschränkt
- Nur IT- und datenschutzrechtlich geschultes Personal hat Zugriff auf Kundendaten
- Revisionssicheres, verbindliches Verfahren zur Wiederherstellung von Daten aus Backup
- Trennung von Berechtigungsbewilligung (organisatorisch) durch HR und CEO und Berechtigungsvergabe (technisch) durch CTO oder System Administrator

3.4. 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:

- Trennung von Entwicklungs-, Test- und Produktivsystemen
- Verarbeitung von personenbezogenen Daten im Auftrag lediglich im Rechenzentrum durch gesicherten Zugriff von Clients am Bürostandort über verschlüsselte Verbindungen
- Die Daten des Auftraggebers und anderer Kunden/Mandanten werden bei einem Dienstleister auf logisch getrennten Systemen verarbeitet.
- Es existiert ein Berechtigungskonzept, das der getrennten Verarbeitung von Daten des Auftraggebers von Daten anderer Kunden/Mandanten Rechnung trägt.

4. Maßnahmen zur Sicherung der Integrität

4.1. Datenintegrität

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

Beschreibung der Datenintegrität:

- Redundante Speicher-Systeme und Datenbanken
- Regelmäßige Backups der Speicher-Systeme und Datenbanken
- Deployment neuer Releases und Patches mit Release-/Patch Management
- Funktionstest bei Installation und Releases/Patches durch Qualitätssicherung
- Logging sowohl der Geschäftsprozesse sowie des Release-/Patch Managements
- Regelmäßige Prüfung und Aktualisierung der Versionen von verwendeten Systemen entlang klar definierter Migrationspfade

4.2. 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 von Transaktionen von Datensätzen
- Kontrollprozesse, die das manuelle Übertragen von Daten verhindern (Übertragungen finden nur automatisiert statt)
- Klare Sicherheits-Architektur und Kontroll-Gateways, die sicherstellen, dass Daten nur in klar definierten, authentifizierten und autorisierten Richtungen mit verschlüsselten Transportwegen übertragen werden

4.3. 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:

- Verwendung von TLS sowohl innerhalb öffentlicher als auch privater Netze
- Regelmäßiges Patching der verwendeten kryptographischen Verfahren
- Administrativer System-Zugriff ausschließlich über getrennte Netze und gesonderte Tunnelverbindungen mit passwortgeschützten private/public RSA-Keys
- Regelmäßige Rotation der Zugriffsschlüssel
- Klares Berechtigungskonzept sowohl für administrativen Systemzugriff als auch administrativen Applikationszugriff
- Umfassende und separierte Protokollierungsverfahren für System- und Applikationszugriff

4.4. 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:

- Sämtliche System- und Programmeingaben werden geloggt
- Netzzugriffe werden geloggt
- Logfile Management
- Protokollierung der Administrationstätigkeiten (Anlegen von Benutzern, Ändern von Benutzerrechten etc.)
- Erstellen von Änderungsbelegen zu den Vorgängen: Erstellung von kritischen Berechtigungen, sämtliche Löschung, Änderung von Daten, sämtliche Arbeiten am Source Code.

5. Maßnahmen zur Sicherung der Verfügbarkeit und Belastbarkeit

5.1. Verfügbarkeitskontrolle

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

Beschreibung des Verfügbarkeitskontrollsystems:

- Unterbrechungsfreie Stromversorgung am Serverstandort
- Archivierungskonzept
- Feueralarmsystem (Büro- und Serverstandort)
- Feuerlöschsystem (Serverstandort)
- Klimaanlage (Serverstandort)
- Vollständiges Backup- und Recoverykonzept mit täglicher Sicherung und katastrophensicherer Aufbewahrung der Datenträger
- Notfall- und Wiederanlaufverfahren mit regelmäßiger Erprobung
- Sachkundiger Einsatz von Schutzprogrammen (Virenscanner, Firewalls, Verschlüsselungsprogramme, SPAM-Filter) und schriftliche Konzeption ihres Einsatzes (Virenschutzkonzept usw.)
- Einsatz von Festplattenspiegelung
- Verfügbarkeit eines Ausweichrechenzentrums

- Vorhalten von einsatzbereiter Zwillingssysteme
- Brandmeldeanlage
- Alarmanlage
- Notfallplan

5.2. 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 Datensicherungs- und Datenbanksysteme sowohl in Hardware als auch in Software
- Summenprüfung zwecks Integritätssicherung der Datensicherungsverfahren
- Regelmäßige Tests der Wiederherstellbarkeit sowohl von Daten und Systemen als auch Services

5.3. 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 InstantMessaging-Benachrichtigungen
- Recovery-Prozesse sind Tool- und Codegestützt. Diese unterliegen damit aller Qualitätssicherungen wie Code-Review Prozesse, Versionssicherheit und Dokumentation
- Notfallpläne mit Verantwortlichkeiten
- Klar definierte Zeitfenster für Wartungen sowie im Rahmen des Release-/Patch Managements
- Regelmäßige Tests

6. Maßnahmen zur regelmäßigen Evaluation der Sicherheit der Datenverarbeitung

6.1. Überprüfungsverfahren

Maßnahmen, die die datenschutzkonforme und sichere Verarbeitung sicherstellen.

Beschreibung der Überprüfungsverfahren:

- Prüfung auf datenschutzkonforme und sichere Verarbeitung ist Bestandteil der Planungsprozesse, denen Implementierungen vorausgehen (Security by Design)
- Regelmäßige Prüfung und Dokumentation der Daten, Systeme und Services hinsichtlich des Bedarfs an Vertraulichkeit, Integrität und Verfügbarkeit
- Regelmäßige externe Prüfung durch Kunden
- Geschultes Personal sowie regelmäßige interne und sicherheitsbezogene Hackathons
- OLAs beinhalten Durchführung von Kontrollen
- Regelmäßige interne Revision sämtlicher datenschutzrelevanter Aspekte durch Datenschutzbeauftragten

- Regelmäßige Überprüfung der Zertifizierung aller Subdienstleister
- Formalisierte Prozesse für Datenschutzvorfälle
- Wesentliche Weisungen des Auftraggebers werden dokumentiert

6.2. 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:

- Datenschutzgerechte Verträge nach Art. 28 DSGVO
- Auftragsdatenverarbeitungsmanagement
- Vertraglich fixierte Ansprechpartner
- Nur von weisungsberechtigten Personen des Auftraggebers werden Weisungen entgegengenommen.
- Zu allen Aktivitäten sind Aufträge des Auftraggebers vorhanden.
- Es kommen nur Subunternehmer zum Einsatz, die von Auftraggeber freigegeben sind.
- Es ist sichergestellt, dass datenschutzrechtliche Regelungen auch an Subunternehmer weitergegeben und von diesen eingehalten werden.
- Eingeschaltete Subunternehmer werden vom Auftragnehmer regelmäßig kontrolliert.