Technische und organisatorische Maßnahmen nach Art. 32 DSGVO

Der Auftragnehmer trifft nachfolgende technische und organisatorische Maßnahmen zur Datensicherheit im Sinne des Art. 32 DSGVO.

1. Vertraulichkeit

Zutrittskontrolle

Die Räumlichkeiten des Auftragsverarbeiters in der Christian-Pless-Str. 11-13 in 63069 Offenbach am Main befinden sich in einem ausschließlich geschäftlich genutzten Hinterhaus in den Etagen OG 2.

Die Räumlichkeiten der Geschäftsstelle in der Rehlingstr. 6d in 79100 Freiburg im Breisgau befinden sich in einem ausschließlich geschäftlich genutzten Bürogebäude in den Etagen OG 6.

Sämtliche Zugänge sind ausreichend gegen den unbefugten Zutritt abgesichert, das bedeutet, dass:

- Jedwede Außentüren mit einem manuellen und technischen Schließsystem versehen und grundsätzlich verschlossen sind;
- die den Mitarbeitern zur Verfügung gestellten Schlüssel personengebunden registriert sowie die Schlüsselausgabe quittiert wird;
- Besucher nur in Begleitung eines Mitarbeiters sich in den Räumlichkeiten bewegen können;
- Personal von Dritten, insbesondere für Reinigungs- und Wartungsaufgaben sorgfältig ausgewählt wird;
- es Festlegungen zur Zugangsberechtigung und Besucherregelung gibt.

Im Rahmen des Rechenzentrumsbetriebes wird darauf geachtet, dass:

- der Zutritt zum Rechenzentrum nur autorisierten Personen gestattet ist;
- der Zutritt durch ein materielles (RFID-Chip) und ein geistigen (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 Version sichergestellt. Die Daten werden bei einem Sicherheitsdienst hinterlegt (Whitelist), so wird gewährleistet, dass nur berechtigte Personen das Rechenzentrum betreten können;
- der Zutritt zu den einzelnen Kundenschränken oder -flächen ausschließlich durch den Kunden und durch das zuständige Personal möglich ist;
- die Zutrittskontrollsysteme sowie die Alarmanlagen über USV und Netzersatzanlage gegen Stromausfall gesichert sind;
- das Rechenzentrum, insbesondere der Zutritt zu Sicherheitsbereichen mit Videoüberwachung ausgestattet ist;
- das Rechenzentrum regelmäßig innerhalb vorgegebener Zeitfenster durch einen Wachdienst begangen wird. Die zu überprüfenden Punkte, welche der Wachdienst in den Rechenzentren

zu kontrollieren hat, sind festgelegt. Auffälligkeiten werden berichtet. Die vorgegebenen Laufwege des Wachdienstpersonals werden protokolliert.

Zugangskontrolle

Es erfolgt insbesondere eine authentifizierte Benutzeridentifikation, insbesondere dadurch, dass:

- alle technischen Systeme (zentral und dezentral), Hardware und Software Firewall geschützt sind;
- der vorhandene Virenschutz (Anti-Virensoftware) gepflegt und aktualisiert wird;
- der Zugang zu Serverräumen nur einer begrenzten Anzahl von Personen gestattet wird (restricted area);
- Mitarbeiter ausschließlich mit den personalisiert angelegten Benutzerprofilen arbeiten, welche die Eingabe eines spätestens aller drei Monate zu ändernden und mindestens 8 Stellen umfassenden alphanumerischen Passwort erfordern;
- Bildschirme automatisiert spätestens nach 5 Minuten sowie Zugänge bei mehr als fünf Fehlversuchen für 30 Minuten gesperrt werden;
- VPN-Technologie (SSL/TLS) eingesetzt wird;
- mobile Datenträger (Laptops) gesondert verschlüsselt sind.

Zugriffskontrolle

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

- die Zugriffsrechte (sowohl für Anwender, wie auch für Administratoren) sich an den aufgabenbedingten und datenschutzrechtlichen Erfordernissen orientieren;
- der Zugriff auf Anwendungen (Eingabe, Veränderung und Löschung) protokolliert wird und ausgewertet werden kann (mindestens für 14 Tage);
- Schutz gegen unberechtigte interne und externe Zugriffe durch Verschlüsselung und Firewalls bestehen (siehe Zugangskontrolle).

Trennung

Die getrennte Datenverarbeitung wird gewährleistet durch:

- fehlende Möglichkeit eines physikalischen Zugriffs durch dedizierten Rechte und Pflichten;
- klare Trennung und Nachvollziehbarkeit von Kundenzugriffen (logische Trennung durch individuellen Benutzungsprofil mit Passwortschutz);
- getrennte Verarbeitung zweckgebundener Daten.

Pseudonymisierung & Verschlüsselung

Die Übermittlung von personenbezogenen Daten erfolgt verschlüsselt. Eine Pseudonymisierung erfolgt nicht, wo eine Löschung aus gesetzlichen oder anderen

Gründen nicht möglich ist, erfolgt eine Anonymisierung. Verschlüsselungsverfahren und Passwortvergabe erfolgen nach dem Stand der Technik.

2. Integrität

Eingabekontrolle

Die Kontrolle von Eingaben, erfolgt durch:

- Protokollierung und Nachvollziehbarkeit von Eingaben, Änderungen und Löschung von Daten (durch Logfiles);
- die Zugriffsrechte orientieren sich (sowohl für Anwender, wie auch für Administratoren) an den aufgabenbedingten und datenschutzrechtlichen Erfordernissen.

Weitergabekontrolle

Die Aspekte der Weitergabe personenbezogener Daten wird hierdurch umgesetzt, dass:

- VPN-Technologie (SSL/TLS) zur Datenkommunikation eingesetzt wird;
- E-Mail-Nachrichten bzw. sonstige Informationen grundsätzlich verschlüsselt bzw. anonymisiert versendet werden können;
- beim physischen Transport, geeignete Transportpersonen sorgfältig ausgewählt werden.

3. Verfügbarkeit und Belastbarkeit

Zur Durchsetzung der Verfügbarkeit, hat der Auftragsverarbeiter veranlasst, dass:

- eine unterbrechungsfreie Stromversorgung besteht (USV);
- Räumlichkeiten in Brandabschnitten versehen mit einzelnen Brandschutzeinrichtungen (Feuer- und Rauchmeldeanlagen; Feuerlöscher) eingeteilt sind;
- Klimaanlagen vorhanden sind;
- eine Notfallmatrix besteht.

Im Rahmen des Rechenzentrumsbetriebes wird insbesondere darauf geachtet, dass: * die Stromversorgung durch Redundanzen sichergestellt wird (Notstromaggregate sowie USV-Anlagen mit n+1 Redundanz; Überbrückungszeit mindestens 15 min. bis die Notstromaggregate die Stromversorgung wieder sicherstellen - Anlaufzeit inkl. Lastübernahme 1 - 2 min.); * das Rechenzentrum mit einer Raumklimatisierung ausgestattet ist (mittlere Temperatur 22° C +/-4°, redundant ausgelegt (n+1), die installierten Luftfilter entsprechen DIN EN 779 G4); * das Rechenzentrum über baulich getrennte Brandabschnitte verfügt. In den Räumlichkeiten ist eine Brandmeldeanlage und eine Brandfrühersterkennung installiert; * die Hochwasser- und Erdbebenkritikalität DIN-gerecht geprüft wurde.

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

Der Auftragnehmer hat sich den folgenden datenschutzrechtlichen Standards unterworfen:

- Erarbeitung eines IT-Sicherheits- und Datenschutzkonzepts;
- Fertigung von internen Datenschutz- und Sicherheitsrichtlinien (Policies) sowie Arbeitsanweisungen;
- Bestellung eines internen Datenschutzbeauftragten;
- Regelmäßige Kontrolle durch den Datenschutzbeauftragten;
- Regelmäßige Hinweise und Ermahnungen, um das Problembewusstsein zu fördern;
- Regelmäßige Datenschutz-Schulungen der Beschäftigten
- Gelegentliche unvermutete Kontrolle der Einhaltung von Datenschutz- und Datensicherungsmaßnahmen.

Der Auftragnehmer gewährleistet, dass die Leistungserbringung in deutschen Rechenzentren und unter Beachtung des deutschen Datenschutzrechts erfolgt.

Die Leistungen des Auftragnehmers orientieren sich zudem soweit möglich an den Vorgaben der Normen der ISO-27001 Zertifizierung. Der Workflow zur Annäherung und Erfüllung der Normen richtet sich nach dem im ITIL Framework. Zudem verfolgt der Auftragnehmer die Prozesse, um die Anforderungen der ISO 20000 zu erfüllen (Vorbereitung einer Zertifizierung; insbesondere Incident & Service Request Management; Problem Management; Business Relationship Management; Budgeting and Accounting for Services; Service Level Management; Capacity Management; Design and Transition of new or changed Services; Change Management; Release and Deployment; Configuration Management; Information Security Management; Service Continuity and Availability; Supplier Management; Durchführung interner Audits). Der Auftragnehmer hat zudem nach den allgemein anerkannten Regeln von Wissenschaft und Technik die operativen Leistungskomponenten (Storage Systeme/ Infiniband-Switche und Uplink Router/ Switche) doppelt redundant ausgelegt.