Anlage 2: technisch organisatorische Maßnahmen
zwischen dem Auftraggeber und Fa. Dunkelberg Systemhaus GmbH

Auftragnehmer (Auftragsverarbeiter):

Firma
Dunkelberg Systemhaus GmbH

Sägewerkstr. 9

75181 Pforzheim

Verantwortlicher: Jens Dunkelberg

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)

- **Zutrittskontrolle**
  Kein unbefugter Zutritt zu Datenverarbeitungsanlage:
  + Alarmanlage
  + Automatisches Zugangskontrollsystem
  + Chipkarten-/Transponder-Schließsystem
  + Manuelles Schließsystem
  + Videoüberwachung der Zugänge
  + Sicherheitsschlösser
  + Schlüsselregelung (Schlüsselausgabe etc.)
  + Personenkontrolle beim Pförtner / Empfang
  + Sorgfältige Auswahl von Reinigungspersonal
- **Zugangskontrolle**
  Keine unbefugte Systembenutzung:
  + Zuordnung von Benutzerrechten
  + Erstellen von Benutzerprofilen
  + Passwortvergabe
  + Authentifikation mit Benutzername / Passwort
  + Zuordnung von Benutzerprofilen zu IT-Systemen
  + Einsatz von VPN-Technologie
  + Einsatz von Intrusion-Detection-Systemen
  + Verschlüsselung von Smartphone-Inhalten ist noch nicht eingerichtet.
  + Einsatz von zentraler Smartphone-Administrations-Software (z.B. zum externen Löschen von Daten)
  + Einsatz von Anti-Viren-Software
  + Verschlüsselung von Datenträgern in Laptops / Notebooks
  + Einsatz einer Hardware-Firewall
  + Einsatz einer Software-Firewall
- **Zugriffskontrolle**
  Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems:
  + Erstellen eines Berechtigungskonzepts
  + Verwaltung der Rechte durch Systemadministrator
  + Anzahl der Administratoren auf das „Notwendigste“ reduziert
  + Passwortrichtlinie inkl. Passwortlänge, Passwortwechsel ist noch nicht eingerichtet.
  + Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von

Daten

+ Sichere Aufbewahrung von Datenträgern
+ physische Löschung von Datenträgern vor Wiederverwendung
+ ordnungsgemäße Vernichtung von Datenträgern (DIN 66399)
+ Einsatz von Aktenvernichtern bzw. Dienstleistern (nach Möglichkeit mit Datenschutz-Gütesiegel)
+ Protokollierung der Vernichtung ist noch nicht eingerichtet.
+ Verschlüsselung von Datenträgern

– **Trennungskontrolle**
Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden

+ physikalisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern
+ Logische Mandantentrennung (softwareseitig)
+ Erstellung eines Berechtigungskonzepts
+ Festlegung von Datenbankrechten
+ Trennung von Produktiv- und Testsystem

– **Pseudonymisierung** (Art. 32 Abs. 1 lit. a DS-GVO; Art. 25 Abs. 1 DS-GVO)
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;

+ Verwendung von Testdatensätzen, die pseudonymisiert werden

1. Integrität (Art. 32 Abs. 1 lit. b DS-GVO)

– **Weitergabekontrolle**
Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport:

+ Einrichtungen von Standleitungen bzw. VPN-Tunneln
+ Beim physischen Transport: sorgfältige Auswahl von Transportpersonal und Fahrzeugen

– **Eingabekontrolle**
Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind:

+ Protokollierung der Eingabe, Änderung und Löschung von Daten
+ Erstellen einer Übersicht, aus der sich ergibt, mit welchen Applikationen welche Daten eingegeben, geändert und gelöscht werden können (internes Verfahrensverzeichnis)
+ 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

2. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO)

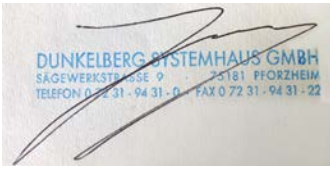
– **Verfügbarkeitskontrolle**
Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust:

+ Unterbrechungsfreie Stromversorgung (USV)
+ Klimaanlage in Serverräumen
+ Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen
+ Schutzsteckdosenleisten in Serverräumen
+ Feuerlöschgeräte in Serverräumen nicht vorhanden, Überwachung auf Einbruch und Brand vorhanden.
+ Erstellen eines Backup- & Recoverykonzepts

  + Testen von Datenwiederherstellung
  + Erstellen eines Notfallplans
  + Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort
- **Rasche Wiederherstellbarkeit** (Art. 32 Abs. 1 lit. c DS-GVO);
  + Wiederherstellung von Systemen, Netzen, Daten
  + Notfallmanagement
  + Ausweichalternativen in externe Rechenzentren, wird aktuell noch nicht genutzt.

3. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO)

- Datenschutz-Management gemäß VdS 10010 ist in der Zertifizierungsphase
- Incident-Response-Management (bedingt)
- Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO);
- Auftragskontrolle
  Keine Auftragsdatenverarbeitung im Sinne von Art. 28 DS-GVO ohne entsprechende Weisung des Auftraggebers:
  + Eindeutige Vertragsgestaltung
  + formalisiertes Auftragsmanagement
  + strenge Auswahl des Dienstleisters
  + Vorabüberzeugungspflicht
  + Nachkontrollen...



Jens Dunkelberg
Fernmeldeanlagenelektronikermeister
Geschäftsführer