Anlage – Technisch-organisatorische Maßnahmen

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

Zutrittskontrolle

☐ Der Zutritt zu den Datenverarbeitungsanlagen / Rechenzentrumen ist nur den Personen gestattet, die hier notwendige Tätigkeiten ausüben. Der Zutritt zu den Datenverarbeitungsanlagen / Rechenzentren wird über ein geeignetes Zutrittskontrollsystem geregelt (z.B.: Magnet- oder Chipkarten, Schlüssel, elektrische Türöffner, Werkschutz bzw. Pförtner, Alarmanlagen, Videoanlagen). Besucher können diese Bereiche nur in Begleitung von Zutrittsberechtigten betreten.

☐ Die o.g. Anlagen sind auch außerhalb der Regelarbeitszeit überwacht.

☐ Die Zutrittsberechtigungen werden nach einem Zutrittsberechtigungskonzept gesteuert.

☐ ……..

☐ ……..

Zugangskontrolle

☐ Der Zugang zu den Anwendungen ist nach Authentifizierung über einen Benutzer-Account mit Passwort möglich

☐ Änderung der Passwörter nach einem festgelegten Intervall vom Anwender gemäß der Passwortrichtlinie

☐ Der Zugang zu den Anwendungen ist über eine benutzerspezifische Zwei-Faktor-Authentifizierung möglich

☐ Der Zugang ist benutzerspezifisch auf jeweils freigeschaltete Instanzen (Mandanten) beschränkt.

☐ Anmeldevorgänge werden protokolliert.

☐ ……..

☐ ……..

Zugriffskontrolle

☐ Die Anwendungen sind so eingerichtet, dass kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems möglich ist

☐ Anwendungszugriffe werden protokolliert

☐ ……..

☐ ……..

Trennungskontrolle

☐ Es wird eine logische Trennung der zu verarbeitenden Daten des Auftraggebers von Daten anderer Auftragnehmer vorgenommen, z.B. über Mandanten

☐ ……..

☐ ……..

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

☐ Die Verarbeitung personenbezogener Daten sind in einer Weise verändert, dass sie ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifisch betroffenen Person zugeordnet werden können.

☐ ……..

☐ ……..

☐ ……..

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

Weitergabekontrolle

Verhinderung von unbefugtem Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport durch:

☐ Verschlüsselung

☐ Virtual Private Networks (VPN)

☐ elektronische Signatur

☐ ……..

☐ ……..

Eingabekontrolle

☐ Protokollierung der Eingabe, Änderung oder Entfernung von personenbezogenen Daten

☐ ……..

☐ ……..

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

Verfügbarkeitskontrolle

Sicherstellung des Schutzes gegen zufällige oder mutwillige Zerstörung oder Verlust durch:

☐ Backup-Strategie (online/offline; on-site/off-site)

☐ USV

☐ Aktuellen Virenschutz über alle Systemen

☐ Firewall

☐ Aktuelles Patchen relevanter Systeme

☐ Organisation von Meldewege

☐ Notfallpläne

☐ Brandfrüherkennung in IT-Räumen

☐ Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DS-GVO)

☐ Nicht zutreffend

☐ ……..

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

☐ Datenschutz-Management

☐ Informations-Sicherheitsmanagement-System (ISMS)

☐ Regelmäßige Auditierung ISMS

☐ Incident-Response-Management

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

☐ Es finden regelmäßige Schulungen zum Datenschutz, IT-Systemen bzw. zur Einhaltung entsprechender Arbeitsanweisungen beim Auftragnehmer statt.

☐ Arbeitsanweisungen

☐ Konzepte

☐ ……..

☐ ……..

☐ ……..

5. Weitere organisatorische Maßnahmen

☐ ……..

☐ ……..

☐ ……..

☐ ……..

☐ ……..

☐ ……..

☐ ……..

☐ ……..

☐ ……..

☐ ……..

☐ ……..