Technische und organisatorische Maßnahmen

Vertraulichkeit

(Art. 32 Abs. 1 lit. b EU-DSGVO)

- Es gilt grundsätzlich das “Need to Know”-Prinzip. Das heißt, nur Personen, die zur Erfüllung ihrer Aufgaben einen bestimmten Zugriff oder bestimmte Informationen benötigen, erhalten diesen auch.

- Datenträgerkontrollen
    - Es wird eine Inventarliste mit allen relevanten Datenträgern geführt
    - Regelmäßige Kontrolle, ob personenbezogene Datenspeicherung notwendig
    - ist (Umfang und Zweck)
    - Ordnungsgemäße Vernichtung/Löschung von Daten/Datenträgern/Papier:
        - Physische Löschung von Datenträgern vor Wiederverwendung
        - Ordnungsgemäße Vernichtung von Papier (DIN 66399): Sicherheitsstufe P-4

- Angemessene Benutzerverwaltung
    - eindeutige Benutzerkennung
    - Zuordnung von Benutzerrechten
    - Erstellen von Benutzerprofilen
    - Initialpasswort mit Änderungspflicht oder selbstständige Festlegung bei der Erstellung
    - Schulung zu Passwörtern
    - Authentifikation mit Benutzername / Passwort
    - Zuordnung von Benutzerprofilen zu IT-Systeme
    - Verwaltung der Rechte durch Systemadministrator
    - Anzahl der Administratoren auf das „Notwendigste“ reduziert
    - Unterscheidung von Benutzern im “öffentlichen” und “privaten” Netzwerk

- Benutzer Kontrollmaßnahmen
    - Nur autorisierte Personen und Geräte erhalten Zugriff
    - Anwender müssen sich für Netzwerkanmeldungen authentifizieren (Zwei-Faktor-Authentifizierung für Zugang zum “privaten” Netzwerk für Administratoren sowie bei bestimmten Applikationen)
    - Einsatz einer Software-Firewall
    - Regelmäßige Kontrolle der Firewall-Einstellungen
    - Benutzerkonten von ausgeschiedenen Mitarbeitern werden unverzüglich gesperrt

    - Nutzung von privaten Mobilgeräten (u. a. Laptops, Tablet-PCs, Smartphones), z. B. im Rahmen einer Bring-Your-Own-Device-Regelung erlaubt

- Personenbezogene Daten werden im Falle einer Weitergabe, wenn möglich, pseudonymisiert und in jedem Falle verschlüsselt übertragen (Art. 32 Abs. 1 lit. a EU-DSGVO).

Integrität

(Art. 32 Abs. 1 lit. b EU-DSGVO)

- Mobile Mitarbeiter, die UMTS oder WLAN-Hotspots nutzen, sind angewiesen, die Firewall der mobilen Computer umzustellen, damit sie für Fremdgeräte nicht mehr erreichbar sind. Grundsätzlich sind alle Mitarbeiter dazu angewiesen, öffentliche Netzwerke nur in Ausnahmefällen zu verwenden.

- Der Datentransfer per FTP wird in Hinsicht auf personenbezogene Daten nicht verwendet, weil das Passwort im Klartext übertragen wird.

- Der Datentransfer per HTTP wird in Hinsicht auf personenbezogene Daten nicht verwendet, weil die Daten unverschlüsselt übertragen werden.

- Durch die Vergabe von Berechtigungen zur Eingabe, Änderung und Löschung von personenbezogenen Daten auf Basis eines Berechtigungskonzepts kann eine unbefugte Verarbeitung personenbezogener Daten größtenteils ausgeschlossen werden.

- Auswahl von Subauftragnehmern unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit)

Verfügbarkeit

(Art. 32 Abs. 1 lit. b EU-DSGVO)

- Zum Einsatz kommt eine Multi-Server-Architektur zur Gewährleistung der Verfügbarkeit aller Funktionen auch bei Teilausfällen und Wartungsarbeiten

- Ein Backup- und Recoverykonzept finden Anwendung
    - Sicherung auf externen, physisch getrennten Servern
    - Sicherung von Datenbanken und Fileservern

- Notfallpläne existieren und werden einmal jährlich geprobt

- Maßnahmen im Rechenzentrum sind bei der netcup GmbH erhältlich

Belastbarkeit

(Art. 32 Abs. 1 lit. b EU-DSGVO)

- Maßnahmen, die Belastbarkeit sicherstellen sollen:
    - Möglichkeit der Zuschaltung weiterer Server innerhalb weniger Minuten bei erhöhten Aufkommen von Anfragen
    - Ausreichende Dimensionierung der Storage-Systeme
    - Ausreichende Dimensionierung der Arbeitsspeicher
    - Monitoring der Systeme
    - Monitoring des Netzwerks
    - Ausfallraten-Statistik
    - Verfügbarkeitsstatistik

Verarbeitung auf Dauer

(Art. 32 Abs. 1 lit. b EU-DSGVO)

- Stetiges Monitoring der Systeme
- Monitoring des Netzwerks
- Changemanagement: Updates und Änderungen werden vor Veröffentlichung ausgiebig getestet

Wiederherstellbarkeit

(Art. 32 Abs. 1 lit. c EU-DSGVO)

- Just-in-time Benachrichtigungen bei etwaigen Fehlern und Ausfällen (z.B. EMail, SMS, Anruf)
- Vorhandensein von Ausweichrechenzentren

Regelmäßige Evaluation

(Art. 32 Abs. 1 lit. d EU-DSGVO)

- Auswertung von Vorfällen
- Auswertung und Umsetzung von Verbesserungsvorschlägen und stetige Weiterentwicklung nach dem Stand der Technik