Technische und organisatorische Maßnahmen

der

Carl Zeiss Meditec Vertriebsgesellschaft mbH

Rudolf-Eber-Straße 11
73447 Oberkochen

Als nicht-öffentliche Stelle, die im Auftrag personenbezogene Daten erhebt, verarbeitet oder nutzt, müssen wir technische und organisatorische Maßnahmen treffen, die erforderlich sind, um die Ausführung der Datenschutzvorschriften zu gewährleisten. Insbesondere sind Vertraulichkeit, Integrität, Verfügbarkeit und Systembelastbarkeit im Zusammenhang mit der Datenverarbeitung sicherzustellen.

Die folgenden technischen und organisatorischen Maßnahmen[1] sind dazu in unserem Unternehmen umgesetzt (zutreffendes ist angekreuzt):

1. Vertraulichkeit

a) Zutrittskontrolle/Gebäudeabsicherung

Kein unbefugter Zutritt zu Datenverarbeitungsanlagen, z.B.: Magnet- oder Chipkarten, Schlüssel, elektrische Türöffner, Werkschutz bzw. Pförtner, Alarmanlagen, Videoanlagen.

- ☒ Alarmanlage
- ☒ Automatisches Zutrittskontrollsystem
- ☒ Schließsystem mit Codesperre
- ☒ Lichtschranken / Bewegungsmelder
- ☒ Schlüsselregelung (Schlüsselausgabe etc.)
- ☒ Protokollierung der Besucher
- ☒ Einsatz von sorgfältig ausgewähltem Wachpersonal
- ☒ Absicherung von Gebäudeschächten
- ☒ Chipkarten-/Transponder-Schließsystem
- ☒ Manuelles Schließsystem
- ☒ Videoüberwachung der Zugänge
- ☒ Sicherheitsschlösser
- ☒ Personenkontrolle beim Pförtner/ Empfang
- ☒ Sorgfältige Auswahl von Reinigungspersonal
- ☒ Tragepflicht von Berechtigungsausweisen

[1] Aus den Angaben muss ein angemessenes Sicherheitsniveau ableitbar sein. In jedem Abschnitt sind dazu getroffene Maßnahmen anzugeben.

b) Zugangskontrolle/Absicherung Systemzugang

Keine unbefugte Systembenutzung, z.B.: (sichere) Kennwörter, automatische Sperrmechanismen, Zwei-Faktor-Authentifizierung, Verschlüsselung von Datenträgern.

- ☒ Zuordnung von Benutzerrechten
- ☒ Einsatz von individuellen Benutzernamen
- ☒ Vorgaben für sichere Passwörter
- ☒ Authentifikation mit biometrischen Verfahren
- ☒ Authentifikation mit Benutzername/ Passwort
- ☒ Zuordnung von Benutzerprofilen zu IT-Systemen
- ☒ Gehäuseverriegelung am Server
  Server stehen in abgeriegelten Räumen
- ☒ Einsatz von VPN-Technologie (Fernzugriff)
- ☒ Sperren von externen Schnittstellen (USB etc.)
- ☒ Verschlüsselung von mobilen Datenträgern
- ☒ Einsatz von Intrusion-Detection-Systemen (Malware Stationen im Eingangsbereich)
- ☒ Einsatz von zentraler Smartphone-Administrations-Software (z.B. zum Fern-Löschen)
- ☒ Verschlüsselung von Smartphone-Inhalten, wenn entsprechende App heruntergeladen wurde
- ☒ Sichere Passwörter für Smartphones
- ☒ Verschlüsselung von Datenträgern in Laptops

c) Zugriffskontrolle/Sicherstellung von Zugriffsberechtigungen

Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems, z.B.: Berechtigungskonzepte und bedarfsgerechte Zugriffsrechte, Protokollierung von Zugriffen.

- ☒ Erstellen eines Berechtigungskonzepts
- ☒ Verwaltung der Rechte durch Systemadministrator
- ☒ Anzahl der Administratoren auf das „Notwendigste“ reduziert
- ☒ Passwortrichtlinie inkl. Passwortlänge, Passwortwechsel
- ☒ Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten
- ☒ Ordnungsgemäße Vernichtung von Papier (Einsatz von Aktenvernichtern bzw. Dienstleistern)
- ☒ Physische Löschung von Datenträgern vor Wiederverwendung
- ☒ Ordnungsgemäße Vernichtung von Datenträgern (DIN 66399)
- ☒ Sichere Aufbewahrung von Datenträgern
- ☒ Protokollierung der Vernichtung
- ☒ Verschlüsselung von Datenträgern
- ☒ Einsatz von Anti-Viren-Software
- ☒ Einsatz einer Hardware-Firewall
- ☒ Einsatz einer Software-Firewall

d) Trennungskontrolle/Maßnahmen zur Zwecktrennung von Daten

Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden, z.B. Mandantenfähigkeit, Sandboxing, physikalisch oder virtuell getrennte Systeme.

- ☒ Physikalisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern
- ☒ Logische Mandantentrennung (softwareseitig)
- ☒ Erstellung eines Berechtigungskonzepts
- ☒ Verschlüsselung von Datensätzen, die zu demselben Zweck verarbeitet werden
- ☒ Trennung von Produktiv- und Testsystem

2. Integrität

a) Weitergabekontrolle/Sicherheit beim Datentransfer

Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport.

- ☒ Einrichtung von Standleitungen bzw. VPN-Tunneln
- ☒ Erstellen einer Übersicht von regelmäßigen Abruf- und Übermittlungsvorgängen
- ☒ E-Mail-Verschlüsselung
- Beim physischen Transport: sichere Transportbehälter/-verpackungen
- ☒ Dokumentation der Empfänger von Daten und Zeitspannen der geplanten Überlassung bzw. vereinbarter Löschfristen
- ☒ Verschlüsselung externer Datenträger bei Weitergabe (CDs, USB-Sticks etc.)
- ☒ Beim physischen Transport: sorgfältige Auswahl von Transportpersonal und Fahrzeugen
- ☒
- ☒ Verschlüsselte Datenübermittlung (z.B. via https oder SFTP)

b) Eingabekontrolle

Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind, z.B.: Protokollierung, Dokumentenmanagement;

- ☒ Erstellen einer Übersicht, aus der sich ergibt, mit welchen Applikationen welche Daten eingegeben, geändert und gelöscht werden können
- ☒ 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
- ☒ Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen worden sind
- ☒ Protokollierung der Eingabe, Änderung und Löschung von Daten

3. Verfügbarkeit und Belastbarkeit

a) Verfügbarkeitskontrolle/Schutz von Daten vor zufälliger Zerstörung und Verlust

- ☒ Unterbrechungsfreie Stromversorgung (USV)
- ☒ Klimaanlage in Serverräumen
- ☒ Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen
- ☒ Schutzsteckdosenleisten in Serverräumen
- ☒ Feuer- und Rauchmeldeanlagen
- ☒ Feuerlöschgeräte in Serverräumen
- ☒ Alarmmeldung bei unberechtigten Zutritten zu Serverräumen
- ☒ Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort
- ☒ Erstellen eines Backup- und Recoverykonzepts
- ☒ Erstellen eines Notfallplans
- ☒ Serverräume über der Wassergrenze (nur in Hochwassergebieten relevant)
- ☒ Serverräume nicht unter sanitären Anlagen
- ☒ Regelmäßige Sicherung von Systemzuständen
- ☒ Regelmäßige Sicherung von Dateibeständen
- ☒ Regelmäßige Sicherung von Datenbanken

b) Rasche Wiederherstellbarkeit

- ☒ Wiederherstellung nach Backup- und Recoverykonzept
- ☒ Kontrolle eines Notfallplans
- ☒ Testen von Datenwiederherstellung

4.) Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

a) Datenschutz-Management

- ☒ Die Grundsätze zum Datenschutz (Erhebung, Verarbeitung oder Nutzung personenbezogener Daten) sind in einer unternehmensinternen Richtlinie festgelegt.
- ☒ Der DSB ist bei der Datenschutzfolgeabschätzung eingebunden
- ☒ Es ist ein Datenschutzbeauftragter schriftlich benannt
- ☒ Der DSB ist im Organigramm eingebunden
- ☒ Verpflichtung der Mitarbeiter auf das Datengeheimnis / zum Umgang mit personenbezogenen Daten
- ☒ Schulung von Mitarbeitern
- ☒ Verpflichtung der Mitarbeiter auf das Fernmeldegeheimnis
- ☒ Einführung eines Kontrollsystems, das den unberechtigten Zugriff auf personenbezogene Daten aufdeckt

☒ Die interne Verarbeitungsübersicht der Verarbeitungsprozesse ist vorhanden

b) Störungsfallmanagement

Prozess der Reaktion auf erkannte oder vermutete Sicherheitsvorfälle bzw. Störungen in IT-Bereichen sowie hierzu vorbereitende Maßnahmen und Prozesse.

☒ Erstellung eines Plans zum Umgang bei Störfällen

☒ Sicherheitsteam ist benannt und geschult

☒ Team mit realitätsnahen Übungen getestet

c) Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen

☒ Beachtung privacy by Design/Datenschutz durch Technikgestaltung

☒ Beachtung privacy by Default/Datenschutz durch datenschutzfreundliche Voreinstellung

☒ Auswahl datenschutzfreundlicher Technologie bei der Beschaffung

d) Auftragskontrolle/Einbindung von Unter-Auftragsverarbeitern

Keine Auftragsdatenverarbeitung ohne entsprechende Weisung des Auftraggebers, z.B.: Eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement, strenge Auswahl des Dienstleisters, Vorabüberzeugungspflicht, Nachkontrollen.

☒ Auswahl der (Unter-)Auftragsverarbeiter unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit)

☒ Vorherige Prüfung und Dokumentation der beim Auftragsverarbeiter getroffenen Sicherheitsmaßnahmen

☒ Schriftlich dokumentierte Weisungen an den Auftragsverarbeiter (z.B. durch Auftragsdatenverarbeitungsvertrag)

☒ Verpflichtung der Mitarbeiter des Auftragsverarbeiters auf das Datengeheimnis/ Vertraulichkeit

☒ Auftragsverarbeiter hat Datenschutzbeauftragten bestellt (wenn erforderlich)

☒ Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags

☒ Wirksame Kontrollrechte gegenüber dem Auftragsverarbeiter vereinbart

☒ Laufende Überprüfung des Auftragsverarbeiters und seiner Tätigkeiten

Oberkochen, 01. Juni 2024

Arne Schmid
Geschäftsführer

i.V. Felix Mayer
Leiter Qualitätsmanagement