d.vinci

d.vinci HR-Systems, Nagelsweg 37-39, 20097 Hamburg

Technisch-organisatorische Maßnahmen (TOM) nach Art. 32 DSGVO

Gültig ab	30.10.2024
Eigentümer	Informationssicherheitsbeauftragter
Klassifizierung	öffentlich

d.vinci betreibt und administriert Systeme für ihre Kunden im Rechenzentrum pop-interactive in Hamburg. d.vinci ist zertifiziert nach ISO/IEC 27001, und die Zertifizierung schließt die Leistungen des Rechenzentrums mit ein. Dieses Dokument beschreibt die technisch-organisatorischen Maßnahmen zum Schutz der personenbezogenen Daten in diesen Systemen.

Zur Einordnung der technisch-organisatorischen Maßnahmen ist von Bedeutung, dass die Systeme nicht in einer klassischen Cloud betrieben werden, sondern es sich um eine SaaS-Lösung handelt, die allein von d.vinci administriert und betrieben wird. Das Personal des Rechenzentrums hat weder Zutritt noch Zugang zu den Systemen. d.vinci nutzt lediglich die Infrastruktur des Rechenzentrums (Löschanlage, Brandschutz, Notstromversorgung usw.).

Soweit sich die hier aufgeführten Maßnahmen zwischen dem Rechenzentrum und den Büroräumen d.vincis unterscheiden, sind sie mit einem „RZ“ (Rechenzentrum) bzw. „N37“ (Büroräume) versehen.

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

a) Zutrittskontrolle: Maßnahmen zur Verhinderung des Zutritts Unbefugter zu den Datenverarbeitungsanlagen

- RZ: Solides Gebäude mit Stahltüren, fensterloser Serverraum in einem oberen Stockwerk
- Alarmanlage
- RZ: Backups in separatem, verschlossenem Brandschutzbereich
- Zutrittsregelung/Schlüsselverwaltung mit Dokumentation der Schlüsselvergabe
- N37: Zutritt mittels Transponder statt mechanischer Schlüssel
- RZ: Vergabe und Entzug von Zutrittsrechten nach dem Need-to-know-Prinzip einschl. Dokumentation
- RZ: Protokollierung der Zutritte
- RZ: Besucherregelung (Zutritt nur für bestimmte Personen, Ausweispflicht, usw.)
- RZ: Videoüberwachung
- N37: Besucherregelung (Dokumentation von Besuchszeiten, Begleitung von Besuchern usw.)

b) Zugangskontrolle: Maßnahmen zur Verhinderung des Zugangs Unbefugter zu den Datenverarbeitungsanlagen

- RZ: „data at rest“-Verschlüsselung
- N37: Verschlüsselung der Festplatten der Clients
- Etablierte Patchmanagementprozesse
- Deaktivierung nicht benötigter Dienste und Funktionen
- Zugang zum Unternehmensnetzwerk von außen via VPN
- Persönlicher User-Login am d.vinci-System
- Verfahren zu Vergabe und Entzug von Benutzerberechtigungen auf Basis eines Rollenkonzepts
- Genehmigungsverfahren bei Änderungen an Berechtigungen
- Regelmäßige Überprüfung der Benutzerkonten
- Automatische Sperrung des Benutzerkontos nach 5 gescheiterten Anmeldeversuchen
- Vorgabe für Kennwörter gemäß Richtlinie
- Mindestens 25 Zeichen lange und zufällig generierte Kennwörter für Service-Accounts
- Zugangsprotokollierung und -auswertung (SIEM)
- Administration via VPN-Tunnel
- Teilweise Mehr-Faktor-Authentifizierung basierend auf der Klassifizierung von Informationen
- N37: Automatische Sperrung der Clients bei Nichtverwendung
- Redundante Firewalls

c) Zugriffskontrolle: Maßnahmen zur Verhinderung des Zugriffs Unbefugter auf personenbezogene Daten

- Konfigurierbare Rollen und Rechte in der Anwendung (z. B. Personalreferenten und Fachbereiche)
- Etabliertes Rollen- und Rechtekonzept für d.vinci-Mitarbeiter
- Änderung von Zugriffsrechten nach dem Need-to-know-Prinzip einschl. Dokumentation
- Regelmäßige Überprüfung der Benutzerkonten einschl. Zugriffsberechtigungen
- Protokollierung von Zugriffen und administrativen Tätigkeiten
- Verschlüsselte Kommunikationswege
- Segmentierte Netzwerke
- Dediziertes Netzwerk für die Kundensysteme
- Möglichst restriktive Firewallregeln
- Toolbasiertes Schwachstellenmanagement
- Dedizierte Backup-Hardware und dediziertes Backup-Netzwerk
- Verschlüsselte Übertragung von Datensicherungen
- Abschluss von Verträgen zur Auftragsdatenverarbeitung mit Dienstleistern für die Instandhaltung von Datenverarbeitungsanlagen
- N37: Sperrung der USB-Ports der Clients
- Akten- und Datenträgervernichtung gemäß DIN 66399

d) Trennungskontrolle: Maßnahmen zur getrennten Verarbeitung personenbezogener Daten, die zu unterschiedlichen Zwecken erhoben wurden

- Speichern der Daten in nach Kunden getrennten Datenbanken
- Trennung von Entwicklungs-, Test und Produktionsumgebung mit jeweils eigenem Datenbestand
- Verwendung generischer Testdaten; keine Produktivdaten in Entwicklungs- und Testsystemen
- Einsatz gesonderter Systeme je nach Zweck der Datenerhebung
- Zugriffsberechtigungen nach funktioneller Zuständigkeit

e) Pseudonymisierung (Art. 32 Abs. 1 lit. a DS-GVO; Art. 25 Abs. 1 DS-GVO): Maßnahmen zur 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.

- Pseudonymisierungsverfahren werden nicht eingesetzt, stattdessen Verfahren zur sicheren Verschlüsselung und Anonymisierung

2. Integrität (Art. 32 Abs. 1 lit. b DSGVO)

a) Weitergabekontrolle: Maßnahmen, um sicherzustellen, dass personenbezogene Daten bei der Übertragung oder Speicherung auf Datenträgern nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können und überprüft werden kann, welche Personen oder Stellen personenbezogene Daten erhalten haben.

- Verschlüsselter Datentransport mit TLS mind. Version 1.2
- Administration der Infrastruktur durch einen VPN-Tunnel
- Irreversible Vernichtung von Datenträgern nach DIN 66399
- Verschlüsselung der Client-Festplatten
- Regelung zur eingeschränkten Nutzung mobiler Speichermedien
- Verschlüsselung von Offsite-Backups
- Protokollierung der Anmeldungen am d.vinci-System

b) Eingabekontrolle: Maßnahmen, um die Möglichkeit der Prüfung sicherzustellen, wer personenbezogene Daten zu welcher Zeit in Datenverarbeitungsanlagen verarbeitet hat.

- Befristete Protokollierung der IP-Adressen bei Abgabe von Bewerbungen
- Im d.vinci-System einsehbares Audit-Log zu administrativen Änderungen
- Rechte- und Rollenkonzept

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)

Verfügbarkeitskontrolle und Belastbarkeitskontrolle: Maßnahmen zum Schutz personenbezogener Daten vor zufälliger Zerstörung oder Verlust, sowie zur ständigen Verfügbarkeit der Daten für den Auftraggeber

- Tägliche Datensicherungen in einen unabhängigen Brandschutzbereich
- Auslagerung verschlüsselter Backups an einen geographisch entfernten Ort
- Regelmäßige Tests der Wiederherstellung aus Backups
- Regelmäßige Disaster-Recovery-Übungen
- Betrieb in einem professionellen Rechenzentrum: baulicher Brandschutz, Brandfrüherkennung, Gas-Löschanlage, USV, Videoüberwachung, Hochwasserschutz, redundante Klimatisierung, redundante Internetanbindung
- Etabliertes Notfallmanagement zur umgehenden Behandlung und Aufarbeitung akuter Störungen
- Vordefinierte Maßnahmen für beschriebene Notfallszenarien
- Etabliertes Risikomanagement
- Redundante Netzwerkkomponenten
- Betrieb der virtuellen Maschinen im hochverfügbaren Cluster
- Redundante Dienste
- Bedarfsgerechtes Einspielen von Sicherheits-Updates
- Überprüfen aller eingehenden Dateien auf Viren
- Monitoring der Verfügbarkeit relevanter Dienste und Ressourcen
- Einsatz ausschließlich aktueller Hardware mit Herstellersupport

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

a) Datenschutzmanagement: Maßnahmen zur Gewährleistung einer den datenschutzrechtlichen Grundanforderungen genügende Organisation

- Etabliertes Datenschutzmanagementsystem
- Bestellung eines externen betrieblichen Datenschutzbeauftragten
- Etablierte Rolle eines internen Datenschutzberaters
- Vertraulichkeitsverpflichtung der Mitarbeiter
- Jährliche Neuverpflichtung der Mitarbeiter auf Vertraulichkeit und relevante Datenschutzrichtlinien
- Jährliche Schulungen der Mitarbeiter zum Datenschutz
- Datenschutzschulungen für neue Mitarbeiter
- Führen eines Verzeichnisses von Verarbeitungstätigkeiten
- Jährliches Audit der technisch organisatorischen Maßnahmen durch den betrieblichen Datenschutzbeauftragten
- Audit technisch organisatorischer Maßnahmen im Rahmen der ISO 27001-Zertifizierung

b) Incident-Response-Management: Maßnahmen zum Auslösen von Meldeprozessen im Falle von Datenschutzverstößen

- Etablierter Prozess zur Meldung von Datenschutzverletzungen an Aufsichtsbehörden und Betroffene

c) Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO): Maßnahmen zur Sicherstellung, dass nur die notwendigen personenbezogenen Daten verarbeitet werden und die Menge der erhobenen Daten minimiert wird.

- Privacy by Design: Integration des Datenschutzes in die Entwicklung der Software schon zum Zeitpunkt der Anforderungserhebung
- Opt-In statt Opt-out, wo immer sinnvoll möglich
- Begrenzung der Menge der gesammelten personenbezogenen Daten auf das Notwendige
- Transparenz darüber, welche Daten gesammelt werden, wie sie verwendet werden und mit wem sie geteilt werden
- Automatische Datenlöschung nach einem vom Kunden einstellbaren Zeitraum

d) Auftragskontrolle: Maßnahmen zur Gewährleistung, dass personenbezogene Daten nur entsprechend der Weisungen verarbeitet werden können.

- Vereinbarung zur Auftragsverarbeitung mit Regelungen zu den Rechten und Pflichten des Auftragnehmers und Auftraggebers
- Festlegen von Weisungsberechtigten auf Seiten des Auftraggebers und Weisungsempfängern auf Seiten des Auftragnehmers
- Möglichkeit des Zutritts, der Auskunft und der Kontrolle für den Auftragnehmer, etwa durch Pentests oder Audits
- Dokumentation weisungsgebundener Auftragsdurchführung
- Einweisung aller zugriffsberechtigten Mitarbeiter des Auftragnehmers
- Verpflichtung der d.vinci-Mitarbeiter auf Vertraulichkeit