vitagroup
VITASYSTEMS GMBH

ANLAGE 3 TECHNISCHE UND ORGANISATORISCHE MAßNAHMEN (TOM)

BASIS

für die

vitasystems GmbH,
Gottlieb-Daimler-Straße 8, 68165 Mannheim

- nachfolgend „Auftragnehmer“ genannt -

Historie

Dokument-ID	Datum und Revision der Freigabe	Autor(en): Name und Funktion	Änderung
TOM-VSYSTEM-001	2020-08-07-1.1	Ingo Klöckl, Datenschutzkoordinator	Erstversion
TOM-VSYSTEM-001	2021-06-30-1.2	Ingo Klöckl, Datenschutzkoordinator	Struktur vereinheitlicht

TOM-VSYSTEM-001	2021-07-20-1.3	Ingo Klöckl, Datenschutzkoordinator	Aktualisierung nach Überprüfung mit CIT und ITO
TOM-VSYSTEM-001	2021-10-09-1.4	Ingo Klöckl, Datenschutzkoordinator	Umbenennung _DS_ nach _PIM_
TOM-VSYSTEM-001	2021-10-20-2.0	Ingo Klöckl, Datenschutzkoordinator	Einarbeitung Feedback DSB
TOM-VSYSTEM-001	2022-11-16-2.1	Ingo Klöckl, Datenschutzkoordinator	Ergänzung Mobile Office

Inhaltsverzeichnis

A. Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO) 4

A.1. Zutrittskontrolle 4

A.2. Zugangskontrolle 6

A.3. Zugriffskontrolle 6

A.4. Trennungskontrolle 7

B. Integrität (Art. 32 Abs. 1 lit. b DS-GVO) 7

B.1. Eingabekontrolle/Plausibilitätskontrolle/Transaktionskontrolle 7

B.2. Weitergabekontrolle/Übermittlungskontrolle 8

B.3. Auftragskontrolle/Vertragskonformitätskontrolle 8

C. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO) 8

C.1. Verfügbarkeitskontrolle 8

C.2. Wiederherstellungskontrolle 9

D. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung (Art. 32 Abs. 1 lit. d; Art. 25 Abs. 1 DS-GVO) 9

D.1. Datenschutzmanagement (Art. 25 Abs. 2 DS-GVO) 9

D.2. Incident-Response-Management 10

D.3. Datenschutzfreundliche Voreinstellungen 10

D.4. Auftragskontrolle (Art. 28 DS-GVO) 10

E. Besondere Maßnahmen für Mobile Office (Sicherheitsperimeter P4) 11

1 Technische und organisatorische Maßnahmen (TOM)

Die technischen und organisatorischen Maßnahmen gemäß Art. 24, 32 DS-GVO zur allgemeinen Sicherheit beinhalten die im Folgenden genannten Maßnahmen.

Alle hier aufgeführten Maßnahmen werden im Rahmen der allgemeinen Datenverarbeitungskonformität umgesetzt. Werden im Rahmen einer Datenverarbeitungstätigkeit besondere Risiken erkannt, die mit den Maßnahmen zur allgemeinen Sicherheit nicht hinreichend behandelt werden, werden zusätzliche technische oder organisatorische Maßnahmen umgesetzt, die zusätzlich zu den hier aufgeführten Maßnahmen gelten.

(Anm. Die Angabe der Sicherheitsperimeter stellt die Verknüpfung mit den Definitionen der Sicherheitsbereiche der ISO 27001 dar.)

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

A.1. Zutrittskontrolle

1.1.1 Standort Mannheim GDS8_EG (Sicherheitsperimeter P2)

Prinzipiell erfolgt die Datenverarbeitung in den Räumlichkeiten des Rechenzentrums (Sicherheitsperimeter P1) und nicht in den Büroräumen der vitasystems GmbH. Eine Verarbeitung von Daten des Auftraggebers am Standort kann im Einzelfall aber nicht ausgeschlossen werden und muss ggf. mit weitergehenden, verarbeitungsspezifischen Maßnahmen abgesichert werden.

Unbefugten wird der Zutritt zu Datenverarbeitungsanlagen durch die folgenden Maßnahmen verwehrt:

Zutrittskontrollsystem:

- Zugang zu den Betriebsräumen über persönliche Chipkarte für alle Mitarbeiter am Standort; Chipverwaltung
- Zutritt für Dritte nur in Begleitung eines Mitarbeiters

1.1.2 Standort Mannheim AA54_1OG (Sicherheitsperimeter P2)

Prinzipiell erfolgt die Datenverarbeitung in den Räumlichkeiten des Rechenzentrums (Sicherheitsperimeter P1) und nicht in den Büroräumen der vitasystems GmbH. Eine Verarbeitung von Daten des Auftraggebers am Standort kann im Einzelfall aber nicht

ausgeschlossen werden und muss ggf. mit weitergehenden, verarbeitungsspezifischen Maßnahmen abgesichert werden.

Unbefugten wird der Zutritt zu Datenverarbeitungsanlagen durch die folgenden Maßnahmen verwehrt:

Zutrittskontrollsystem:

- Zugang zu den Betriebsräumen über persönliche nummerierte Chipkarte für alle Mitarbeiter des Standorts, weitere Mitarbeiter der vitagroup Unternehmensgruppe ausnahmsweise nach Befugnis; Chipverwaltung/dokumentierte Ausgabe der Chips
- Zutritt für Dritte nur in Begleitung eines Mitarbeiters

1.1.3 Standort Braunschweig (Sicherheitsperimeter P2)

Prinzipiell erfolgt die Datenverarbeitung in den Räumlichkeiten des Rechenzentrums (Sicherheitsperimeter P1) und nicht in den Büroräumen der vitasystems GmbH. Eine Verarbeitung von Daten des Auftraggebers am Standort kann im Einzelfall aber nicht ausgeschlossen werden und muss ggf. mit weitergehenden, verarbeitungsspezifischen Maßnahmen abgesichert werden.

Unbefugten wird der Zutritt zu Datenverarbeitungsanlagen durch die folgenden Maßnahmen verwehrt:

Zutrittskontrollsystem:

- Zugang zu den Betriebsräumen über Schlüssel für alle Mitarbeiter des Standorts; Schlüsselverwaltung
- Zutritt für Dritte nur in Begleitung eines Mitarbeiters; Besucherregelung
- Regelung zum Verschließen von Bürotrakts

1.1.4 Standort Chemnitz (Sicherheitsperimeter P2 und P2c)

Unbefugten wird der Zutritt zu Datenverarbeitungsanlagen durch die folgenden Maßnahmen verwehrt:

Zutrittskontrollsystem:

- Zugang zu den Betriebsräumen über persönliche nummerierte Chipkarten für alle Mitarbeiter des Standorts; Chipkartenverwaltung
- Zutritt für Dritte nur in Begleitung eines Mitarbeiters; Besucherregelung; Besucherprotokollierung und -ausweis; Unterzeichnung Datenschutzerklärung

A.2. Zugangskontrolle

Durch die folgenden Maßnahmen wird verhindert, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können:

- Zugang zu IT-Systemen nur nach Eingabe einer persönlichen Benutzerkennung mit Passwort
- Zugang zu administrativen Systemkomponenten nur über bestimmte Mitarbeiter, Accounts und bestimmte IP-Ebenen
- Zugang zu Produktivsystemen nur über bestimmte Mitarbeiter, Accounts und bestimmte IP-Ebenen
- Für alle Mitarbeiter verbindliche Passwortregeln sind in den Datenschutzrichtlinien vorgegeben
- Gruppenpassworte nur für Service-Accounts
- Passwortwechsel nach BSI-Empfehlungen, nach Bekanntwerden oder Vorfällen
- Passworthistorie zum Sperren bereits verwendeter Passworte
- Sichere Aufbewahrung von kryptographischen Schlüsseln
- Automatische Sperrung der Arbeitsplatz-Rechner (Pausenschaltung)
- Einrichtung eines (1) Benutzerstammdatensatzes pro User
- Einsatz von Anti-Viren-Software

A.3. Zugriffskontrolle

Durch die folgenden Maßnahmen wird gewährleistet, dass die Benutzung eines Datenverarbeitungssystems ausschließlich durch Berechtigte erfolgt, die nur im Rahmen ihrer Zugriffsberechtigung auf Daten zugreifen können:

- Bedarfsorientierte Ausgestaltung des Berechtigungskonzepts und der Zugriffsrechte, betrachtete Ebenen: Datenfelder, Anwendungsprogramme, Betriebssystem, Server/IT-System
- Differenzierte Berechtigungen (über Profile bzw. Rollen) je nach Arbeitsaufgaben an Mitarbeiter; Genehmigung der Zugriffsberechtigungen und Dokumentation

- Automatische Prüfung der Berechtigungen über ein Benutzerverwaltungssystem
- Minimale Anzahl von Administratoren
- Bei Datenträgern Verschlüsselung und kontrollierte Vernichtung
- Durchführung einer genehmigten Konfigurationsänderung nur durch festgelegten Bereich

A.4. Trennungskontrolle

Durch die folgenden Maßnahmen wird gewährleistet, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können:

- Trennung von Produktiv-, Test- und Entwicklungsumgebungen auf Netzwerkebene sowie auf Basis unabhängiger VMs unter VMware ESXi
- Einsatz mandantenfähiger Systeme auf Plattform- und Anwendungsebene, soweit möglich

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

B.1. Eingabekontrolle/Plausibilitätskontrolle/Transaktionskontrolle

Durch die folgenden Maßnahmen wird gewährleistet, dass nachträglich geprüft werden kann, ob und von wem personenbezogene Daten eingegeben, verändert oder entfernt (gelöscht) worden sind:

- Alle Eingaben, Änderungen und Löschungen personenbezogener Daten werden, soweit technisch möglich, in dem verwendeten Datenbanksystem mit Uhrzeit- und Benutzerstempel protokolliert und dokumentiert
- Definition klarer Löschfristen für alle Kategorien personenbezogener Daten und Regelungen zur Zuständigkeit der erforderlichen Datenlöschungen gemäß Richtlinien des Datenschutz-Managementsystems
- Regelung von Aufbewahrungsfristen für alle erzeugten Protokolle
- Schutz der Protokolldatenbestände gegen unbefugte Zugriffe

B.2. Weitergabekontrolle/Übermittlungskontrolle

Durch die folgenden Maßnahmen wird gewährleistet, dass personenbezogene Daten bei Transport, Übertragung und Übermittlung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können:

- Einsatz von Datenverschlüsselung (SSL/TLS, VPN) beim Transport
- Ein administrativer Zugriff auf Serversysteme erfolgt grundsätzlich über verschlüsselte Verbindungen (Tunnelverbindung: VPN = Virtual Private Network oder SSL/TLS)
- Sendungsverfolgung des Paket-Dienstleisters beim Versand von Datenträgern.
- Vernichtung von Datenträgern durch zertifizierte Entsorger (Datenträgertonne) und mehrfaches Überschreiben nach sicherem Verfahren

B.3. Auftragskontrolle/Vertragskonformitätskontrolle

Durch die folgenden Maßnahmen wird gewährleistet, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können:

- Eindeutige Vertragsgestaltung entsprechend den Vorgaben von Art. 26, 28 DS-GVO zwischen Auftraggeber und Auftragnehmer
- Regelmäßige Kontrolle der ordnungsgemäßen Vertragsausführung

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

C.1. Verfügbarkeitskontrolle

Die folgenden Maßnahmen erlauben eine Kontrolle der Verfügbarkeit der zur Verarbeitung von personenbezogenen Daten eingesetzten Systeme:

- Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust
  - Unterbrechungsfreie Stromversorgung (USV)
  - Einsatz von Virenschutz und Firewall sowie regelmäßige Aktualisierung
- Systemhärtung

  - Verteilung von System- und Softwareupdates

- Patch Management mit Einsatz eines Werkzeugs zum Software- und Anforderungsmanagement

- Maßnahmen zur Datensicherung (physikalisch/logisch)

  - Backup- und Recovery-Konzept

- ISO 27001-konformer Schutz zur Erhaltung der physischen Sicherheit der eingesetzten Serverräume (Sicherheitsperimeter P1, über Rechenzentrums-Dienstleister)

C.2. Wiederherstellungskontrolle

Die folgenden Maßnahmen werden umgesetzt, so dass eine rasche Wiederherstellbarkeit der Verfügbarkeit personenbezogener Daten gewährleistet ist:

- Maßnahmen zur Datensicherung (physikalisch/logisch)

  - Backup- und Recovery-Konzept

D. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung (Art. 32 Abs. 1 lit. d; Art. 25 Abs. 1 DS-GVO)

D.1. Datenschutzmanagement (Art. 25 Abs. 2 DS-GVO)

Durch die folgenden Maßnahmen wird gewährleistet, dass Prozesse im Rahmen eines Datenschutzmanagements in den Datenschutzrichtlinien verbindlich geregelt und implementiert sind.

- Zentrale Dokumentation aller betrieblichen Verfahrensweisen und Regelungen zum Datenschutz im Datenschutz-Managementsystem

– Ein Datenschutzbeauftragter ist bestellt, der bei der Planung, Umsetzung, Evaluierung und Anpassung der erforderlichen Maßnahmen im Bereich von Datenschutz beteiligt ist

D.2. Incident-Response-Management

Durch die folgenden Maßnahmen wird gewährleistet, dass Datenschutzvorfälle rechtzeitig erkannt und entsprechend den Vorgaben von Art. 33, 34 DS-GVO behandelt werden:

– Dokumentierter Prozess zur Erkennung, Meldung und Bearbeitung von Sicherheitsvorfällen und Datenpannen

– Einbindung des Datenschutzbeauftragten in Sicherheitsvorfälle und Datenpannen

D.3. Datenschutzfreundliche Voreinstellungen

Durch die folgenden Maßnahmen wird gewährleistet, dass nur die notwendigen Daten erhoben und verarbeitet werden:

– Konzeption und Ausführung der Verarbeitungstätigkeit gemäß Vorgaben des Datenschutz-Managementsystems

D.4. Auftragskontrolle (Art. 28 DS-GVO)

Durch die folgenden Maßnahmen wird eine Auftragskontrolle als **Verantwortlicher** gewährleistet:

– Siehe Maßnahmen aus Abschn. B.3

Durch die folgenden Maßnahmen wird eine Auftragskontrolle als **Auftragsverarbeiter** gewährleistet:

– Siehe Maßnahmen aus Abschn. B.3

– Erstellung von TOMs

– Eintrag ins Verzeichnis der Verarbeitungstätigkeiten

E. Besondere Maßnahmen für Mobile Office (Sicherheitsperimeter P4)

Die Sicherheit von Daten im Mobile Office wird durch die „Ergänzungsvereinbarung zum Arbeitsvertrag Mobile Office“ geregelt. Sie legt u. a. Maßnahmen fest zu:

- Einsatz von Arbeitsmitteln
- Umgang mit Daten und Unterlagen im Mobile Office
- Zusätzliche Maßnahmen im Mobile Office zum Schutz von Daten und Betriebsgeheimnissen
- Sicherheitsmaßnahmen bei der Übertragung von Daten und beim Transport von Unterlagen
- Umgang mit Daten und Arbeitsmitteln bei Beendigung des Mobile Office