Vertrag zur Auftragsverarbeitung gem. Art. 28 DSGVO

Vereinbarung

zwischen dem

beauftragenden Hausarzt gemäß Teilnahmeerklärung

- Verantwortlicher -

und

HÄVG AG/ Mediverbund als Managementgesellschaft

- Auftragsverarbeiter –

1. Rechtsgrundlage, Art und Zweck der Verarbeitung

1.1 Der Auftragsverarbeiter verarbeitet im Rahmen der elektronischen Arztvernetzung Daten, unter anderem auch Gesundheitsdaten, für den Verantwortlichen. Rechtsgrundlage der Verarbeitung ist Art. 6 Abs. 1 lit. b, Art. 9 Abs. 2 lit. h DSGVO in Verbindung mit § 22 BDSG-neu.

1.2 Die Art und der Zweck der Verarbeitung erfolgt zur Erfüllung des in Anhang 14 der Anlage 12 „Elektronische Arztvernetzung“ des HZV-Vertrags geregelten Vertragsinhaltes.

1.3 Der Verantwortliche bleibt im Rahmen des Auftrags für die Einhaltung der gesetzlichen Bestimmungen der Datenschutzgesetze, für die Wahrung der ärztlichen Schweigepflicht und insbesondere für die Rechtmäßigkeit der Datenweitergabe an den Auftragsverarbeiter sowie für die Rechtmäßigkeit der Datenverarbeitung verantwortlich.

2. Gegenstand und Umfang der Datenverarbeitung

2.1. Für die Durchführung der elektronischen Arztvernetzung werden folgende Daten vom Verantwortlichen an den Auftragsverarbeiter übermittelt:

- Versichertenstammdaten
- Die von dem Verantwortlichen für einen konkreten Behandlungszusammenhang als erforderlich angesehene Anamnesedaten, Befunddaten, Diagnosedaten, Medikationsdaten sowie Therapiedaten
- Absender- und Empfängerinformationen

2.2. Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:

- HZV-Versicherte
- Ärzte

2.3. Der Auftragsverarbeiter übernimmt hierbei ab dem Punkt der Datenannahme die technischen Verarbeitungsvorgänge, die Bereitstellung von Speicherkapazität, Rechenleistung, die hierfür erforderliche Infrastruktur und die Systembetreuung.

3. Weisungsrechte des Verantwortlichen

3.1 Der Auftragsverarbeiter verpflichtet sich, die Verarbeitung der Daten ausschließlich im Rahmen dieses Auftrags oder nach Weisungen des Verantwortlichen durchzuführen.

3.2 Der Auftragsverarbeiter hat die Weisungen des Verantwortlichen hinreichend zu dokumentieren.

3.3 Der Auftragsverarbeiter hat den Verantwortliche darauf hinzuweisen, wenn er der Ansicht ist, die Weisung verstoße gegen Datenschutzvorschriften. Der Auftragsverarbeiter ist berechtigt, die Weisung solange auszusetzen, bis sie durch den Verantwortliche geändert oder bestätigt wurde.

4. Kontrollrechte des Verantwortlichen

4.1. Zur Ausübung seines Kontrollrechtes wird der Datenschutzbeauftragte des Auftragsverarbeiters für den Verantwortlichen regelmäßig anhand vorgelegter Zertifikate, Berichte oder beantworteter Checklisten die Einhaltung der datenschutz- und IT-sicherheitsrechtlichen Maßnahmen bewerten und entsprechende Kontrollen im Rahmen des Auftragsverhältnisses gem. Art. 28 DSGVO für den Verantwortlichen übernehmen. Das Ergebnis der Bewertung wird in einem "Statusbericht zu Datenschutz, Datensicherheit und IT-Sicherheit" dokumentiert. Dieser Statusbericht ist auf Wunsch des Verantwortlichen einsehbar.

4.2. Der Auftragsverarbeiter verpflichtet sich, dem Datenschutzbeauftragten auf Anforderung die erforderlichen Auskünfte für den Verantwortlichen zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.

4.3. Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann erfolgen durch

- die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DSGVO;
- die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DS-GVO;
- aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-

Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren);
- eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz).

4.4. Für weitergehende Ermöglichung von Kontrollen durch den Verantwortlichen kann der Auftragsverarbeiter einen Vergütungsanspruch geltend machen.

5. Personal

5.1. Der Auftragsverarbeiter setzt nur Personal zur Auftragserledigung ein, welches schriftlich auf den Datenschutz, die Vertraulichkeit und die ärztliche Schweigepflicht nach § 203 StGB verpflichtet wurde. Er hat sein Personal dabei auf die besondere Sensibilität der Daten des Verantwortlichen, vorliegend Gesundheitsdaten, hinzuweisen.

5.2. Der von dem Auftragsverarbeiter benannte Datenschutzbeauftragte ergibt sich aus ANLAGE 16 des HZV-Vertrags. Bei Änderungen des Datenschutzbeauftragten ist der Verantwortliche unverzüglich zu informieren.

6. Unterauftragsverhältnisse

6.1. Als Unterauftragsverhältnisse sind Dienstleistungen zu verstehen, die sich auf die Hauptleistung des Vertrages beziehen. Nicht umfasst sind Nebenleistungen wie z.B. Telekommunikationsleistungen, Post/ Transportleistungen.

6.2. Der Auftragsverarbeiter ist verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Verantwortlichen, seines Personals und insbesondere seiner Versicherten auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen abzuschließen sowie Vorkehrungen zu treffen und Kontrollmaßnahmen zu ergreifen.

6.3. Der Auftragsverarbeiter darf Unterauftragnehmer (weitere Auftragsverarbeiter) im Rahmen der rechtlichen Auflagen und Rahmenbedingungen beauftragen.

6.4. Der Verantwortliche stimmt der Beauftragung der nachfolgend genannten Unterauftragnehmer bereits jetzt zu unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2 bis 4 DS-GVO.:

Gesellschaft für IT-Vernetzung (GefIT) mbH
Kölner Str. 18
70376 Stuttgart

Sowie als weiterer Unterauftragsverarbeiter für die GefIT die

x-tention Informationstechnologie GmbH
Bürgermeister-Wegele-Straße 12
86167 Augsburg

6.5. Die Weitergabe von personenbezogenen Daten des Verantwortlichen an den Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet.

6.6. Eine weitere Auslagerung durch den Unterauftragnehmer bedarf der ausdrücklichen Zustimmung des Hauptauftragnehmers (mind. Textform); sämtliche vertraglichen Regelungen in der Vertragskette sind auch dem weiteren Unterauftragnehmer aufzuerlegen.

7. Technische und organisatorische Maßnahmen

Der Auftragsverarbeiter hat die Sicherheit gem. Art. 32 DSGVO herzustellen und zu garantieren. Hierzu trifft er Maßnahmen, die dem Stand der Technik entsprechen. Die technischen und organisatorischen Maßnahmen können dabei stets angepasst werden, um den Schutz auch bei sich verändernden Rahmenbedingungen weiter gewährleisten zu können. Einzelheiten zu den Maßnahmen finden sich im **Anhang** dieses Vertrages. Die technischen und organisatorischen Maßnahmen erfüllen insbesondere auch die besonderen Anforderungen für den Schutz von Gesundheitsdaten gem. § 22 Abs. 2 BDSG-neu.

8. Unterstützung des Verantwortlichen

8.1 Der Auftragsverarbeiter hat den Verantwortlichen bei der Umsetzung der Betroffenenrechte nach Art. 15 ff. DSG-VO zu unterstützen.

8.2 Der Auftraggeber hat ferner den Verantwortlichen, soweit ihm möglich ist, bei seinen Pflichten gem. Art. 32, 36 DSGVO zu unterstützen.

9. Beendigung und Löschung

9.1. Dieser Auftrag endet mit Ablauf des zugrundeliegenden Hauptvertrages bzw. der zugrundeliegenden vertraglichen Regelung.

9.2. Nach Abschluss der vertraglich vereinbarten Arbeiten– spätestens mit Beendigung der Leistungsvereinbarung – hat der Auftragsverarbeiter sämtliche in seinen Besitz gelangte Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, datenschutzgerecht zu vernichten, sofern keine Aufbewahrungspflichten des Auftragsverarbeiters entgegenstehen. Das Protokoll der Löschung ist auf Anforderung vorzulegen.

9.3. Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragsverarbeiter entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren.

9.4. Sollte die Teilnahme des Verantwortlichen am zugrundeliegenden Hauptvertrag oder an der zugrundliegenden vertraglichen Regelung enden, gleich aus welchem Grund, verbleiben sämtliche in den Besitz des Auftragsverarbeiters gelangten Unterlagen, erstellten Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen für weitere 6 Monate im Besitz des Auftragsverarbeiters.

9.5. Sollte in der in 9.4 genannten Frist keine Abholung der Daten durch einen anderen berechtigten Verantwortlichen erfolgen, werden die Daten datenschutzgerecht gelöscht, sofern keine Aufbewahrungspflichten des Auftragsverarbeiters entgegenstehen.

Anhang – Technisch-organisatorische Maßnahmen

I. Zugangskontrolle

1. Zutrittskontrollrichtlinie

Es existiert eine Zugriffs- und Zutrittskontrollrichtlinie, in der folgende Themenbereiche geregelt sind:
- Benutzerverwaltung
- Verwaltung von Sonderrechten
- Sicherheitsbereiche
- Physische Zutrittskontrollen

- Sicherung von Büros, Räumen und Einrichtungen

2. Regelung für Besucher und Fremdpersonal

   Eine Regelung für Fremdpersonal und Besucher ist vorhanden. Besucher des Bürogebäudes müssen sich beim Empfang von x-tention anmelden. Anschließend werden diese dort von einem Mitarbeiter abgeholt und während des gesamten Aufenthalts begleitet. Sollte der Zutritt von Externen im Rechenzentrum (z. B. zu Wartungszwecken) notwendig sein, gilt auch dort die Begleitpflicht. Zusätzlich muss der Zutritt in das Rechenzentrum in einem Formular protokolliert und die Nutzungsrichtlinie für Rechenzentrumszutritt für Servicetechniker von Drittfirmen unterzeichnet werden.

3. Zentrales Zutrittskontrollsystem

   Das Bürogebäude und die Rechenzentren sind durch geeignete Maßnahmen zutrittsgeschützt. Dies ist unter anderem durch ein zentrales Zutrittskontrollsystem, welches die Zutrittsberechtigungen zu den einzelnen Räumen (Büros, Rechenzentrum, Technikräume etc.) steuert, sichergestellt. Die Vergabe der Zutrittsberechtigungen erfolgt nach dem Least-Privilege-Prinzip, dessen Einhaltung durch regelmäßige Audits kontrolliert und sichergestellt wird.

4. Chip-Karten und Mitarbeiterausweis

   Als Zutrittsmedium werden Chip-Karten verwendet, welche auch gleichzeitig als personalisierter Mitarbeiterausweis mit aufgedrucktem Lichtbild und Namen zu tragen sind. Durch die Kombination von Mitarbeiterausweis und Zutrittsmedium ist eine geregelte Aus- bzw. Rückgabe sichergestellt und Zutrittsberechtigungen können mittels dem zentralen Zutrittskontrollsystem gezielt vergeben, entzogen und kontrolliert werden.

5. Türen, Schlösser und Vereinzelungsschleusen

   Die Türen und Schlösser sind den unterschiedlichen Schutzbedürfnissen der Räume angepasst. Jedenfalls werden entsprechend stabile Türen und Verankerungen sowie sichere Schlösser verwendet. Gegebenenfalls können Türen zusätzlich durch ein manuelles Schließsystem versperrt werden. Bei den Vor- bzw. Technikräumen der Rechenzentren kommen Motorschlösser zum Einsatz. Der Zutritt zum Rechenzentrum selbst ist zusätzlich durch eine Vereinzelungsschleuse reglementiert. Sofern Fenster in sensiblen Bereichen vorhanden sind, werden diese durch Gitter geschützt.

6. Videoüberwachung

   Sensible Bereiche, wie z. B. die Rechenzentren von x-tention oder die Zutrittsbereiche zum Bürogebäude, sind zusätzlich durch eine Videoüberwachungsanlage geschützt.

II. Datenträgerkontrolle

1. Regelungen zur sicheren Verwendung von mobilen IT-Geräten und Datenträgern

   Für mobile IT-Geräte und Datenträger ist durch Nutzungsrichtlinien definiert, dass diese sicher zu verwahren sind (z. B. bei Dienstreisen).

2. Festplatten- und Datenträgerverschlüsselung

   Festplatten von Notebooks sowie Datenspeicher von Smartphones sind durchgängig mittels kryptographischer Verfahren gemäß dem Stand der Technik verschlüsselt und somit im Falle des Diebstahls oder Verlustes vor unberechtigtem Zugriff geschützt. Bei der Verwendung von mobilen Datenträgern (z. B. USB-Sticks) wird durch die Datenklassifizierungsrichtlinie vorgegeben, dass diese im Fall der Speicherung von definierten Datenklassen zu verschlüsseln sind.

3. Mobile Device Management

   Smartphones und Tablets sind in ein Mobile-Device-Management-System eingebunden, welches das Fernlöschen sowie die technische Durchsetzung zur Einhaltung definierter Sicherheitsvorgaben ermöglicht.

4. Vernichtung von ausgedruckten Dokumenten und Datenträgern

   Für nicht mehr benötigte ausgedruckte Dokumente und Datenträger in Disc-Form (CDs, DVDs) stehen mehrere Aktenvernichter (Shredder) zur Verfügung, deren Verwendung durch die entsprechende Datenklassifizierung vorgegeben ist. Nicht mehr benötigte Hardware-Komponenten (z. B. Festplatten) werden physisch sicher vernichtet.

III. Speicherkontrolle

1. Datenklassifizierung

   Es existiert eine schriftliche und verpflichtende Vorgabe, wie Daten zu klassifizieren und zu behandeln sind (Zugriff, Weitergabe, Verwahrung etc.). Diese gilt sowohl für Informationen in elektronischer als auch physischer Form (z.B. Papier).

2. Automatische Bildschirmsperre

   Nach einer Inaktivität von 15 Minuten werden alle Systeme automatisch gesperrt. Mitarbeiter sind zudem organisatorisch verpflichtet, den Bildschirm manuell zu sperren, sobald sich dieser außerhalb des eigenen Sichtfeldes befindet.

3. Virenschutz

   Auf allen Client- und Server-Systemen von x-tention ist eine Virenschutzsoftware im Einsatz. Die Aktualisierung der Virensignaturen wird mehrmals pro Tag durch ein zentrales Management-System sichergestellt. Zusätzlich kommt eine Zwei-Hersteller-Strategie zur Anwendung. Als erweiterter Schutz ist auf allen Clients Application Whitelisting aktiviert, um die Ausführung unbekannter bzw. ungewollter Software (z. B. Viren, Ransomware etc.) technisch zu unterbinden.

4. Einsatz von Firewalls

   Eine Perimeter- sowie eine zusätzliche interne Campus-Firewall regeln den Zugriff auf die unterschiedlichen Netzbereiche. Sämtliche Firewall-Freischaltungen werden über einen eigenen Change Request im Service Management Tool abgewickelt. Firewall-Freischaltungen im internen Netz werden durch den Teamleiter Netzwerk geprüft und freigegeben, Firewall-Freischaltungen von/in die DMZ oder von/in das Internet müssen zusätzlich vom CISO geprüft und freigegeben werden.

   Zusätzlich werden auch noch folgende Funktionen durch die Perimeter-Firewall umgesetzt:

   - Inspektion von verschlüsselten Verbindungen (z. B. HTTPS)
   - Intrusion Detection bzw. Intrusion Prevention System
   - Scannen nach Schadsoftware
   - AntiBot-Feature
   - Content-Filter
   - Application-Control-Mechanismus

5. Trennung von Test- und Produktivdaten

   Systeme, welche Test- bzw. Produktivdaten verarbeiten, werden getrennt voneinander betrieben.

6. Trennung von Kunden

   Jeder Kunde von x-tention wird sowohl netzwerktechnisch als auch applikativ getrennt von anderen Kunden betrieben. Für Kunden werden eigene AD-Domänen und somit auch eigene User mit unterschiedlichen Berechtigungen betrieben. Über Rollen im Unternehmen ist klar definiert, welche Rolle über welche Rechte, Pflichten und Verantwortlichkeiten verfügt.

7. Schwachstellen- und Patch-Management

   Es ist ein durchgängiges Schwachstellen- und Patch-Management etabliert sowie ein Schwachstellen- und Patch-Management-Verantwortlicher definiert. Schwachstellen werden regelmäßig über unterschiedliche Kanäle identifiziert. Anschließend werden diese bewertet und angemessene Maßnahmen ergriffen. Sicherheitsrelevante Updates werden vor der Installation getestet und nach definierter Wartezeit auf den Systemen freigegeben und eingespielt.

8. Penetration Tests

   In regelmäßigen Abständen (monatlich) werden alle von extern erreichbaren Systeme hinsichtlich Schwachstellen durch einen automatisierten Penetration Test überprüft. Abweichungen fließen in das Schwachstellen-Management ein und werden dort angemessen behandelt.

IV. Benutzerkontrolle

1. Authentifizierung intern und extern

   Die Authentifizierung von Mitarbeitern bei Systemen im internen Netz erfolgt mittels personalisiertem Benutzerkonto (AD-Account, Benutzername/Passwort). Bei der Verbindung von Extern auf Systeme des Unternehmens (z. B. beim Herstellen einer VPN-Verbindung über das Internet) wird zusätzlich ein zweiter Faktor für die Authentifizierung verwendet.

2. Umgang mit Passwörtern

   Sämtliche Regelungen zum Umgang mit Passwörtern sind sowohl in der Nutzungsrichtlinie für EDV-Systeme und Daten sowie in einer eigenen Kennwortrichtlinie geregelt. Die Vorgaben an die Passwort-Sicherheit entsprechen dem Stand der Technik (Mindestlänge von zehn Zeichen, aktivierte Komplexität, Änderung spätestens nach 90 Tagen usw.). Passwörter dürfen nicht weitergegeben werden und werden in einem unternehmensweiten Passwort-Manager mit personalisierten AD-Zugängen verwaltet.

V. Zugriffskontrolle

1. Segmentierung des Netzwerks

   Das Netzwerk ist in zahlreiche virtuell und physisch getrennte Netzabschnitte (z. B. VLANs) segmentiert. Die Zugriffe auf diese Netzsegmente werden durch Firewalls reglementiert.

2. Berechtigungskonzept

   Ein detailliertes und dokumentiertes Berechtigungskonzept liegt vor. Jeder Mitarbeiter erhält nur jene Rechte, die er für seine tägliche Arbeit zwingend benötigt (Umsetzung des Least-Privilege-Prinzips). Jeder Mitarbeiter arbeitet standardmäßig mit reduzierten Rechten. Zusätzlich können administrative User beantragt werden, welche – je nach Notwendigkeit – erweiterte Rechte zugewiesen bekommen. Das Berechtigungskonzept orientiert sich auf Basis von Rollen.

   Der CISO kontrolliert regelmäßig die Berechtigungen und schränkt diese bei Bedarf ein. Zusätzlich ist ein AD-Manager-Prinzip implementiert, wobei bei jeder AD-Gruppe ein AD-Manager hinterlegt ist. Dieser muss jede Veränderung in seiner AD-Gruppe schriftlich freigeben und regelmäßig die Rechte der ihm zugewiesenen AD-Gruppen überprüfen. Für hoch privilegierte Berechtigungen (z.B. Domain Admins) ist eine Monitoring-Überwachung implementiert. Finden Veränderungen statt, wird der CISO automatisch darüber informiert. Veränderungen für hoch privilegierte Berechtigungen gibt ausschließlich der CISO schriftlich frei.

VI. Übertragungskontrolle

1. Genehmigung von Datenübertragungen

   Es ist geregelt, dass keine personenbezogenen Daten das Unternehmen ohne schriftliche Genehmigung des CISOs verlassen dürfen.

2. Verträge zur Auftragsdatenverarbeitung

   Wird von x-tention ein Auftragnehmer in Anspruch genommen, der Daten des Unternehmens verarbeitet, geschieht dies nur nach sorgfältiger Auswahl und unter entsprechenden vertraglichen Vereinbarungen, die mindestens die gemäß Art. 28 und 29 DSGVO geforderten Punkte beinhalten (ADV-Verträge).

   - Definition des Gegenstands und der Dauer des Auftrags
   - Definition von Art, Umfang und Zweck der Datenanwendung
   - Sicherstellung, dass auch der Auftragnehmer entsprechende technische und organisatorische Maßnahmen zur Informations- und Datensicherheit getroffen hat (gem. Art. 32 DSGVO)
   - Definition des Kontroll- bzw. Audit-Rechts durch x-tention
   - Verpflichtung der Mitarbeiter des Auftragnehmers auf das Datengeheimnis
   - Vorgehen bei Hinzuziehen eines zusätzlichen Sub-Auftragnehmers
   - Vorgehen bei Beendigung des Vertrags bzw. Auftragsverhältnis (Rückgabe bzw. Löschung der Daten)
   - Vertragsstrafen im Falle eines Verstoßes

VII. Eingabekontrolle

1. Personalisierte Konten

   Sämtliche AD-Konten sind personalisiert. Auch administrative AD-Konten sind personalisiert und haben nur jene Rechte, die unbedingt für die Aufgabenerfüllung notwendig sind (siehe Berechtigungskonzept).

2. Logging und Session Monitoring

   Auf allen Servern ist das Mitprotokollieren von Zugriffen (Logging bzw. Security Log) aktiviert. Dadurch können durchgeführte Aktivitäten überprüft werden. Je nach Bedarf sind Systeme zusätzlich mit einem Session Monitoring ausgestattet, welches alle durchgeführten Aktivitäten sowohl per Video als auch textbasiert aufzeichnet. Ausgewählte Systeme verfügen zusätzlich über revisionssichere Audit-Logs (z.B. Passwort Manager, Firewall, Service Management Tool usw.)

3. Synchronisierung der Systemzeiten

   Alle Systeme sind mit einem standardisierten Zeitsynchronitätsdienst (NTP) zwecks Sicherstellung von Verfügbarkeits- und Integritätskriterien verbunden, sodass diese zeitsynchron sind.

VIII. Transportkontrolle

1. Verschlüsselung bei Datenübertragungen

   Genehmigte Datenübertragungen werden ausschließlich verschlüsselt gemäß dem Stand der Technik durchgeführt. Eine Weitergabe von Daten in anonymisierter oder pseudonymisierter Form wird jedoch präferiert.

2. Gesicherte Verbindungen von Extern

   Wird eine Verbindung von Extern (z. B. über das Internet) benötigt, wird diese über einen VPN-Tunnel realisiert. Dadurch werden die Vertraulichkeit und Integrität der übertragenen Daten sichergestellt.

3. Geregelter Zugriff von Dritten

   Sämtliche Zugriffe von Dritten (z. B. Fernwartungsfirmen, Hersteller) sind mittels Fernwartungsverträgen

gemäß den gesetzlichen Bestimmungen geregelt. Über einen Sideletter zum jeweiligen Rahmenvertrag sind detaillierte Bestimmungen geregelt (z. B. auf welche Systeme wird zugegriffen, welcher User greift zu, wird ein Session Monitoring eingesetzt usw.).

4. Einsatz von digitalen Signaturen

   Ein definierter Personenkreis von x-tention setzt fortgeschrittene bzw. qualifizierte Zertifikate ein, um Dokumente und E-Mails zu signieren (Integritäts- bzw. Authentizitätsschutz). Zusätzlich ist es dadurch möglich, E-Mails zu verschlüsseln (Vertraulichkeitsschutz).

IX. Wiederherstellung

1. Backup- und Recovery-Konzept inkl. Auslagerungsstrategie

   Es existiert ein umfassendes Backup- und Recovery-Konzept, welches auf Basis der jeweiligen Datenarten (z. B. Fileserver-Daten, Datenbank-Daten usw.) über mehrere Stufen die Datenverfügbarkeit gewährleistet. Zusätzlich zu einem Disk-basierten Backup-System werden für Disaster-Fälle Backup-Bänder ausgelagert und an einem separaten Standort in einem Band-Safe gelagert. Die Backup-Protokolle werden täglich gesichtet und auf Erfolg überprüft. Mittels regelmäßigen Recovery-Tests wird die ordnungsgemäße Funktion der Datensicherungen getestet und dokumentiert.

2. Business Continuity Management (BCM)

   Es existiert ein umfassendes Notfallmanagement (BCM) inkl. Wiederanlaufplänen, Übungen und Tests sowie einer Notfallorganisation, wobei das Notfallmanagement in einem 3-stufigen Verfahren aufgebaut ist:

   - Die Basis bildet das BCM (Business Continuity Management) von x-tention (Rechenzentrums-Basisbetrieb). Darin sind Szenarien für den RZ-Ausfall bis hin zum Komplettausfall beschrieben und sowohl präventive als auch reaktive Maßnahmen enthalten.
   - Darauf ist das SCM (Service Continuity Management) von x-tention aufgesetzt, über welches zentrale Basis-Dienste für x-tention und deren Kunden abgebildet sind (z.B. AD).
   - Als dritte Stufe werden die Kernapplikationen in das SCM integriert, wobei diese sowohl für x-tention als auch für Kunden von x-tention definiert sind.

   Disaster-Recovery-Tests der Infrastruktur sind definiert und werden regelmäßig durchgeführt (z.B. Notstrom-Aggregats-Tests, USV-Stresstests, Fail-Over-Tests usw.).

3. Security Incident Management / Data Breach

   Ein Security-Incident-Management- bzw. Data-Breach-Prozess ist etabliert. Der CISO hat im Falle eines Sicherheitsvorfalls spezielle Befugnisse, beruft ein Incident Response Team ein und koordiniert die Behebung. Zu anderen CISOs, Datenschutzbeauftragten, einschlägigen Sicherheitsorganisationen, CERTs und Behörden wird ein enger Kontakt gepflegt.

X. Zuverlässigkeit & Datenintegrität

1. Monitoring mit Alarmierung

   Sämtliche Systeme inkl. Infrastruktur- und Netzwerkkomponenten sind in ein unternehmensweites Monitoring-System eingebunden. Alarmiert wird automatisch per E-Mail und SMS.

2. Redundante Rechenzentren mit entsprechendem physischem Schutz

   x-tention verfügt über zwei redundante Rechenzentren, die gemäß dem Stand der Technik ausgestattet sind. Neben einem umfassenden Zutrittsschutz (siehe Kapitel 3.1) werden nachfolgend wesentliche Komponenten aufgelistet, die einen sicheren Betrieb der Rechenzentrumsinfrastruktur gewährleisten:

   - Örtliche Trennung der Rechenzentren (unterschiedliche Brandabschnitte)
   - Sicherheitszelle (Lampertz-Zelle)
   - Unterbrechungsfreie Stromversorgung (USV-Anlage auf Batterie-Basis für mehrere Stunden) inkl. Überwachung auf Stromausfall
   - Diesel-Notstromaggregat und rotierenden USV-Anlage
   - Brandfrüherkennung (Rauchansaugsystem und Rauchmelder)
   - Automatische Brandlöschanlage (FM 200) und verfügbare Kleinlöschgeräte (TFL CO2)
   - Redundante Klimageräte inkl. Temperatur- und Luftfeuchtigkeitsüberwachung
   - Sumpfbecken und Wasserstandsüberwachung

3. Change Management

   Änderungen an sämtlichen Produktivsystemen werden durch ein verpflichtendes und flächendeckendes Change Management behandelt, freigegeben und nachvollziehbar dokumentiert. Je nach Art, Inhalt und Umfang des Changes wird dieser ggf. durch das CAB (Change Advisory Board – mehrköpfiges Gremium aus unterschiedlichen Fachbereichen inkl. Informationssicherheit) diskutiert und freigegeben. Bei Bedarf erfolgt die Umsetzung des Changes im Vier-Augen-Prinzip. Der gesamte Change-Prozess wird von der Anforderung bis zur abgeschlossenen Umsetzung (inkl. Post Implementation Review) nachvollziehbar in einem Service Management Tool dokumentiert.