IT für Gesundheit und Soziales

Datenschutz und Datensicherheit in der RZV Rechenzentrum Volmarstein GmbH - RZV Datenschutzkonzept-TOM - Umsetzung technischer und organisatorischer Maßnahmen (TOM) gemäß Art. 32 DS-GVO, § 27 DSG-EKD, § 26 KDG und § 64 BDSG

Inhalt

1 Vorbemerkungen

Diese applikationssystemunabhängige Darstellung über Datenschutz und Datensicherheit in der RZV Rechenzentrum Volmarstein GmbH (im Folgenden „die RZV“) wurde für Kunden und Interessenten der RZV herausgegeben und beschreibt, welche technischen und organisatorische Maßnahmen gemäß Art. 32 Datenschutz-Grundverordnung der Europäischen Union (DS-GVO), § 27 Kirchengesetz über den Datenschutz der Evangelischen Kirche in Deutschland (DSG-EKD), § 26 Gesetz über den Kirchlichen Datenschutz (KDG) und § 64 Bundesdatenschutzgesetz (BDSG) die RZV als Auftragsverarbeiter gemäß Art. 28 Absatz 1 DS-GVO durchführt, um ein angemessenes Schutzniveau bei der Verarbeitung personenbezogener Daten zu gewährleisten. Zum Zweck der einfacheren Lesbarkeit wird im Folgenden nur auf die DS-GVO referenziert.

In der vorliegenden Darstellung ist der Kunde oder Interessent stets Verantwortlicher im Sinne von Art. 4 DS-GVO, er wird im Folgenden "Auftraggeber" genannt.

Die Verteilung der Verantwortlichkeit für die Einhaltung der genannten Vorschriften richtet sich nach dem Umfang der zwischen der RZV und dem Auftraggeber vereinbarten Auftragsverarbeitung. Die Bandbreite der von der RZV angebotenen Services reicht dabei von unterstützenden Dienstleistungen für den auftraggeberseitigen Betrieb der dezentral autonom betriebenen Auftraggebersysteme über das „Hosting“, bis hin zum kompletten Outsourcing in den zentralen Betrieb der RZV. Beim kompletten Outsourcing von Applikationssystemen in den zentralen Betrieb der RZV werden die Applikationssysteme in den beiden Rechenzentren der RZV mit zentralen Rechner- und Speichersystemen betrieben. Bei diesem zentralen Betrieb der Systeme greifen die Auftraggeber über gesicherte Verbindungen im Rahmen zweckgebundener Berechtigungskonzepte auf die zentralen Ressourcen zu.

Bei der Aufzählung und Beschreibung der einzelnen Maßnahmen musste dem Spannungsfeld zwischen der detaillierten Preisgabe von Sicherheitsfunktionalitäten und der Verschwiegenheitsverpflichtung zu eben genau diesen Sicherheitsfunktionalitäten Rechnung getragen werden. Weitergehende Informationen müssen den folgenden Kontrollrechten des Auftraggebers vorbehalten bleiben:

- Berücksichtigung datenschutzspezifischer Zertifizierungen oder Datenschutzsiegel und -prüfzeichen der RZV,
- Einholung konkreter schriftlicher Selbstauskünfte bei der RZV,
- Vorlage von Testaten über die RZV durch Sachverständige oder
- Ausübung von Überprüfungs- und Inspektionsrechten gemäß Art. 28 Absatz 3 Buchstabe h DS-GVO.

2 Sicherheit der Verarbeitung gemäß Art. 32 DS-GVO

2.1 Pseudonymisierung und Verschlüsselung personenbezogener Daten (Art. 32 Absatz 1 Buchstabe a und Art. 25 Absatz 1 DS-GVO)

Alle Datenleitungen zwischen der RZV und ihren Auftraggebern und ihren Partnern sind auftragsgemäß verschlüsselt.

Alle gespeicherten Daten im zentralen Betrieb der RZV sind grundsätzlich verschlüsselt gespeichert. Das bedeutet, dass diese Daten nur über die zugehörigen Applikationen mit entsprechenden Zugriffsrechten gelesen werden können.

Darüber hinaus ist organisatorisch sichergestellt, dass bei Zugriffen mit externen Tools oder Hilfsprogrammen eine geeignete Dokumentation durch die jeweiligen Bearbeiter erstellt wird.

2.2 Vertraulichkeit der Systeme und Dienste (Art. 32 Absatz 1 Buchstabe b DS-GVO)

2.2.1 Zutrittssicherheit in der RZV GmbH

Durch wirksame Zutrittskontrollsysteme und eine dezidierte Schließregelung ist sichergestellt, dass Unberechtigten der Zutritt zu Datenverarbeitungsanlagen, mit denen Informationen verarbeitet und genutzt werden und zu Sicherheitszonen, in denen Dokumente mit vertraulich zu behandelnden Informationen vorhanden sind, verwehrt wird. Die personenbezogenen Zutrittsberechtigungen werden über ein formulargestütztes Berechtigungsverfahren erteilt. Über die Zutrittskontrollsysteme und die Schließregelung wird mit der Ausgabe

von Transpondern und/oder Schlüsseln umgesetzt, welche Personen welche Sicherheitszonen laut Berechtigungen betreten dürfen.

Darüber hinaus sind die Räumlichkeiten der RZV in verschiedene Informationssicherheitszonen unterteilt. Die Zutrittsregelung sowie Besucherbetreuung wird für jedes Gebäude gemäß den Vorgaben für die Informationssicherheitszonen geregelt. Je nach Sicherheitszone kommen dabei auch Einbruchmeldeanlagen und Videoüberwachungssysteme zum Einsatz.

2.2.2 Zugangssicherheit in der RZV GmbH

Für den Zugang ins LAN der RZV werden grundsätzlich alle Arbeitsplatzrechner und Drucker einer Switch-Authentifizierung unterworfen und den betrieblichen Anforderungen entsprechend autorisiert. Die personenbezogenen Berechtigungen werden über ein formulargestütztes Berechtigungsverfahren vergeben

Der Zugang wird nur nach entsprechender Active-Directory Authentifizierung gestattet. Die zur Authentifizierung und zum Schutz genutzten Passwörter müssen immer aus einer Kombination von mindestens 10 Zeichen bestehen und mindestens drei der folgenden vier Zeichengruppen enthalten: Großbuchstaben (A bis Z), Kleinbuchstaben (a bis Z), Ziffern (0 bis 9) und nicht alphabetische Zeichen (z. B. !, $, #, %). Passwörter werden spätestens nach 40 Tagen Gültigkeit geändert. Zur Absicherung der Daten der Anwenderinnen und Anwender sind gemäß Empfehlung des Herstellers Microsoft maximal 10 Fehlversuche möglich, bis eine vorübergehende Sperrung des Benutzerkontos automatisch vorgenommen wird.

Die Passwortregeln in den Applikationssystemen werden soweit technisch möglich entsprechend des Auftraggeberauftrages konfiguriert. Alle Mitarbeiterinnen und Mitarbeiter sind verpflichtet, ihre Passwörter und ihnen bekannte Passwörter auf Auftraggebersystemen für den Zugang zu Datenverarbeitungsanlagen jeder Art vertraulich zu behandeln und nicht an unberechtigte Dritte zur Kenntnis zu geben.

Die Verwaltung von **Authentisierungsinformation (Login-Daten)** von Benutzern erfolgt über die entsprechenden Funktionalitäten für die verschiedenen Systeme.

Während der Betriebsbereitschaft eines Arbeitsplatzrechners sind Mitarbeiterinnen und Mitarbeiter zur Beaufsichtigung ihres Systems verpflichtet.

Die Arbeitsplatzrechner sind zentral so eingestellt, dass der Bildschirm nach 10 Minuten ungenutzter Zeit gesperrt wird und nur mit Hilfe des Passworts wieder aktiviert werden kann. Darüber hinaus sind die Mitarbeiterinnen und Mitarbeiter verpflichtet, die Bildschirmsperrung beim Verlassen des Arbeitsplatzes zu aktivieren.

2.2.3 Zugriffssicherheit in der RZV GmbH

Über ein formulargestütztes Berechtigungsverfahren ist organisatorisch sichergestellt, dass die Anzahl von Mitarbeiterinnen und Mitarbeitern mit Zugriffsrechten auf Produktivdaten oder Kopien von Produktivdaten der Auftraggeber sowie der eigenen Systeme auf ein Mindestmaß beschränkt ist. Dabei wird gewährleistet, dass ausschließlich berechtigte Mitarbeiterinnen und Mitarbeiter der RZV und ihrer Auftragsverarbeiter die Möglichkeit haben, Daten einzusehen, soweit dies im Rahmen ihrer Aufgabenerfüllung erforderlich ist. Die applikationsbezogenen Rollen- und Berechtigungssystematiken sind in den einzelnen Dokumentationen der Applikationen beschrieben. Berechtigungskonzepte und bedarfsgerechte Zugriffsrechte werden entsprechend der Weisungen durch den Auftraggeber umgesetzt.

2.2.4 Verarbeitungstrennung

Alle Applikationssysteme sind so gestaltet, dass zu unterschiedlichen Zwecken erhobene Daten auch getrennt voneinander verarbeitet werden können. Insbesondere sind die implementierten Verarbeitungsroutinen so aufgebaut, dass sie nicht ohne weiteres eine Verknüpfung von Daten zulassen, welche eine nicht erlaubte Datensammlung über einzelne Personen ermöglicht.

2.3 Integrität der Systeme und Dienste (Art. 32 Absatz 1 Buchstabe b DS-GVO)

2.3.1 Weitergabekontrolle

2.3.1.1 Weitergabekontrolle in der RZV GmbH bei externer Kommunikation

Die Weitergabekontrolle gewährleistet, dass personenbezogene Daten bei der Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durchgeführt wird.

Ein Datenaustausch von Arbeitsplatzrechnern und Servern sowie sonstigen Geräten, die in das LAN der RZV eingebunden sind, mit anderen Computern oder Geräten erfolgt ausschließlich über die Netzwerkinfrastruktur der RZV.

Ein Austausch von personenbezogenen Daten zwischen einem privaten und einem zur dienstlichen Nutzung bereitgestellten Arbeitsplatzrechner ist verboten.

2.3.1.2 Kommunikation mit Auftraggebern

Die Weitergabekontrolle wird auftragsgemäß durch verschlüsselte VPN-Verbindungen oder aber durch point-to-point-Verbindungen auf „Layer 2 – Ebene“ zwischen den Auftraggebern und der RZV sichergestellt.

Mit point-to-point Verbindung ist eine logische Leitung gemeint, die zwei Endpunkte auf physikalischer Basis miteinander verbindet (MAC-Adresse und IP-Adresse) die exakt nur von zwei Teilnehmern genutzt werden kann: Dem einzelnen Auftraggeber und der RZV. Andere Teilnehmer können weder diese Leitung noch die physikalischen Endpunkte nutzen oder sehen. Die Datenleitungen zwischen den Standorten der Auftraggeber und der RZV sind aus diesem Grund nicht verschlüsselt.

Darüber hinaus stellt die RZV technisch und organisatorisch in ihrer Kommunikation mit ihren Kunden sicher, dass personenbezogene Daten bei der Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübermittlung vorgesehen ist. Gleiches gilt für den Versand von physischen Dokumenten.

2.3.1.3 E-Mail

Jede ein- oder ausgehende E-Mail wird in der Firewall auf Viren untersucht. Darüber hinaus sind Dateitypen festgelegt, die als Anhang eingehender oder ausgehender E-Mails automatisch blockiert werden. Hierbei handelt es sich um Anhänge mit aktiven, ausführbaren Inhalten. Einer versehentlichen oder ungewollten Übertragung von ausführbaren Programmen jeder Art ist auf diese Weise wirkungsvoll begegnet.

Weiterhin sind alle Mitarbeiterinnen und Mitarbeiter verpflichtet, den Versand von Informationen mit personenbezogenem Inhalt per E-Mail über ein gesichertes Verfahren zu organisieren.

2.3.1.4 Fernbetreuung, Fernwartung, Remote Control

Grundsätzlich ist es Dritten, betriebsfremden Mitarbeitenden oder Beauftragten von externen Dienstleistern oder Lieferanten nur gestattet, während einer Online-Verbindung auf technische Geräte, Betriebssysteme oder Applikationen zuzugreifen, wenn diese gesetzlich oder vertraglich zur Einhaltung der einschlägigen Datenschutzgesetze in der jeweils gültigen Fassung verpflichtet sind. Darin enthalten ist insbesondere die Pflicht, Mitarbeiterinnen und Mitarbeiter bei der Aufnahme ihrer Tätigkeit gemäß einer gesonderten Erklärung zur Vertraulichkeit im Sinne von Art. 28 Absatz 3 Buchstabe b DS-GVO und zur Einhaltung einschlägiger Datenschutzvorschriften, insbesondere DS-GVO, zu verpflichten und darauf hinzuweisen, dass diese Verschwiegenheitspflicht auch nach Beendigung ihrer Tätigkeit fortbesteht.

Die Installation von Software zur Durchführung von Fernwartungssitzungen erfolgt nur durch Mitarbeiterinnen und Mitarbeiter des Systembetriebes oder in ihrem Beisein. Es werden marktübliche und bekannte Verfahren zur Fernwartung verwendet.

2.3.1.5 Internet

Im LAN der RZV werden eigene, öffentliche Webserver ausschließlich in einer gesonderten DMZ betrieben.

Der Zugriff auf das Internet von den Arbeitsplätzen im LAN der RZV erfolgt grundsätzlich über die Firewall, so dass hier eine wirksame Kontrolle gegen aktive Inhalte gegeben ist.

2.3.1.6 Teleworking

Für alle Arbeitsplätze (stationär oder mobil), die außerhalb des LANs der RZV zu Zwecken des Teleworkings eingesetzt werden, gelten immer auch alle IT-Vorschriften analog zu den Bestimmungen für Arbeitsplätze im LAN der RZV. Darüber hinaus sind alle diese Zugriffe einer doppelten Authentifizierung unterworfen.

2.3.1.7 Mobile Arbeitsplätze (Notebooks) und sonstige mobile Endgeräte (Smartphones etc.)

Es kommen nur von der RZV bereitgestellte mobile Arbeitsplätze und sonstige mobile Endgeräte zum Einsatz. Die Zugriffe dieser Geräte auf zentrale Verfahren der RZV sind ebenfalls einer doppelten Authentifizierung unterworfen.

Mobile Arbeitsplätze werden außerhalb des RZV-Netzwerkes immer mit einer aktiven Firewall betrieben, die einen direkten Internetzugriff, unter Umgehung der Firewall des LAN der RZV, unterbindet. Die Deaktivierung von Firewallfunktionen und die Deaktivierung von sonstiger Software zum Schutz vor Schadsoftware sind nur den Administratoren der RZV gestattet.

Mobile Arbeitsplätze müssen darüber hinaus regelmäßig (mindestens alle 14 Tage, bei längerer Abwesenheit sofort nach Rückkehr) im LAN der RZV betrieben werden, damit aktuelle Sicherheitspatche und Virenpattern geladen werden.

2.3.2 Eingabekontrolle in der RZV GmbH

Alle Zugriffe auf Applikationssysteme durch Mitarbeiterinnen und Mitarbeiter der RZV werden mit benutzerbezogenen Accounts durchgeführt. Dabei werden Ereignisprotokolle, die Benutzertätigkeiten aufzeichnen, erzeugt, aufbewahrt und anlassbezogen überprüft. Protokollierungseinrichtungen und Protokollinformation sind vor Manipulation und unbefugtem Zugriff geschützt.

Sowohl im fachlichen als auch im technischen Support existieren keine Gruppenaccounts.

Den Auftraggebern wird empfohlen, ebenfalls nach diesem Grundsatz zu verfahren.

Für von der RZV beauftragte Dritte gilt derselbe Grundsatz.

Beim Zugriff auf die Datenbanken über die implementierten und freigegebenen Funktionen der einzelnen Softwaremodule ist die Nachvollziehbarkeit der vorgenommenen Eingaben durch entsprechende Kontroll- und Dokumentationsfunktionen als Bestandteil der Funktionen und der Datenbanken sichergestellt. Bei Eingaben, die durch externe Tools oder Hilfsprogramme vorgenommen werden und die der datenschutzrechtlichen Eingabekontrolle unterliegen, wird eine geeignete Dokumentation durch die jeweiligen Bearbeiter sichergestellt.

Zur Sicherstellung der Qualität und der Belastbarkeit der Protokollierungsdaten, werden die Uhren aller relevanten informationsverarbeitenden Systeme innerhalb der RZV über die zentrale Firewall synchronisiert.

2.4 Dauerhafte Verfügbarkeit und Belastbarkeit der zentralen, RZV-eigenen Systeme und Dienste (Art. 32 Absatz 1 Buchstabe b DS-GVO)

2.4.1 Verfügbarkeit der zentralen, RZV-eigenen Systeme

Beide Rechenzentren der RZV GmbH sind durch die TÜV Informationstechnik GmbH mit dem hohen Gütesiegel (Trusted Site Infrastructure TSI, Level 3 erweitert sowie Level 2 erweitert) für hohen Schutzbedarf sowie erweiterten Schutzbedarf zertifiziert.

Das Kriterienwerk **Trusted Site Infrastructure (TSI)** ist ein etabliertes und anerkanntes Verfahren zur Prüfung und Zertifizierung der physischen Sicherheit und Verfügbarkeit von Rechenzentren.

Der zugrundeliegende Kriterienkatalog TSI.STANDARD orientiert sich an den Maßnahmenempfehlungen der Grundschutz-Kataloge des Bundesamtes für Sicherheit in der Informationstechnik (BSI) und berücksichtigt die einschlägigen EN-und DIN-Normen, insbesondere die DIN EN 50600, aber auch, VDE-Vorschriften und VdS-Publikationen.

Mit der anspruchsvollen Zertifizierung ist der Nachweis erbracht, dass die geprüfte Infrastruktur den strengen Anforderungen genügt und eine sehr hohe System- und Datenverfügbarkeit sichergestellt ist (kein „single point of failure“).

2.4.2 Organisation und Kompetenzen

Die Einrichtungen der Informations- und Kommunikationstechnik im LAN der RZV sind grundsätzlich so gestaltet, dass sie den Anforderungen des Datenschutzes und einem an die Empfehlungen des BSI anzulehnenden Standards der Datensicherheit gerecht werden. Insbesondere zielen die Datensicherheit und der Datenschutz darauf ab, die Integrität der Daten zu gewährleisten, die Authentizität aller weiterzuleitenden Informationen sicherzustellen und jederzeit über die verwendeten Datenspeichersysteme und die dazu benötigten Dienstleistungen und Funktionen verfügen zu können. Zur Erreichung dieser Ziele werden an den entsprechenden Stellen der RZV die notwendigen Kontrollen eingehalten. Die laufende Überwachung von Risiken und Störungen in der RZV sind elementarer Bestandteil des Risikomanagements des Unternehmens.

Für alle Fragen der IT-Sicherheit und IT-Verfügbarkeit ist ein abgestuftes Entscheidungsverfahren eingerichtet. Die damit verbundene Verantwortlichkeit erstreckt sich bis zu den von der RZV bereitgestellten Kommunikationseinrichtungen der Auftraggeber, über die eine Anbindung an das LAN der RZV erfolgt.

In der RZV ist ein IS-Management-Team gemäß BSI-IT-Grundschutz benannt. Das Team ist für die Regelung sämtlicher übergreifender Belange der Informationssicherheit zuständig und koordiniert, berät und kontrolliert die zugehörigen Analysen, Konzepte und Richtlinien. Diesem Team gehört auch ein ausdrücklich benannter, externer Informationssicherheitsbeauftragter an.

Darüber hinaus hat die RZV einen Datenschutzbeauftragten gemäß Art. 37 DS-GVO bestellt. Er wirkt insbesondere auf die Einhaltung aller Gesetze und anderer Vorschriften zum Datenschutz hin. Die Kontaktdaten sind im Internet-Portal des RZV dokumentiert und werden dort aktualisiert. Zusätzlich sind die Kontaktdaten des DSB der zuständigen Aufsichtsbehörde gemeldet worden.

2.4.3 Softwarestandards

Einzusetzende Applikationssoftware wird auf aktuellen Betriebssystemplattformen und Datenbanksystemen betrieben.

Die von Betriebssystem- und Datenbankherstellern angebotenen Sicherheitsupdates für Server und Einrichtungen der Kommunikationstechnik werden in regelmäßigen Abständen schnellstmöglich implementiert.

2.4.4 Hardwarestandards

Für zentral im Rechenzentrum betriebene RZV-eigene Server sind die folgenden Standards eingeführt und werden im laufenden Betrieb aufrechterhalten:

- *Hochverfügbare Rechnerleistung basierend auf multiprozessorfähigen Systemen*
- *Redundante Systeme in beiden Rechenzentren zur Sicherstellung der Geschäftskontinuität sowie Servicekontinuität und Verfügbarkeit*
- *Fehlertoleranter Plattenspeicher*
- *Remotespiegelung der bereitgestellten Daten durch beide Rechenzentren*
- *Online erweiterbare Plattenspeicherkapazität*
- *Online Ersatzlaufwerke*
- *Laufende Überwachung der Systeme*
- *Direkte Störungsübermittlung an Monitoringsysteme*
- *Remotespiegelung aller Datensicherungen*

Für diese Systeme wird ein Wiederanlaufplan vorgehalten, der geeignet ist, flexibel Handlungsanweisungen für verschiedene Formen von Bedrohungen und Beeinträchtigungen der Verfügbarkeit und Sicherheit der RZV zu generieren.

2.4.5 Datensicherung

Die Sicherung der Daten der zentralen Systeme findet in regelmäßigen Abständen bedienerlos über automatisierte Verfahren statt. Die Nachvollziehbarkeit der durchgeführten Sicherungen ist durch geeignete Dokumentationen oder Systemprotokolle jederzeit gewährleistet. Darüber hinaus gelten ergänzende Vorgaben einer gesonderten „Datensicherungsrichtlinie“.

2.4.6 Betriebsdokumentation von Softwaresystemen, Rechner- und Netzwerkinfrastruktur

Der jeweilige Istzustand von Softwaresystemen, Rechner- und Netzwerkinfrastruktur ist zu jeder Zeit ausreichend dokumentiert, so dass ihn ein geeigneter sachverständiger Dritter in akzeptabler Zeit nachvollziehen kann.

2.4.7 Kommunikationsinfrastruktur

Die eingesetzten Netzwerkprotokolle sorgen für eine reibungslose und sichere Kommunikation auf Basis der Vernetzung mit Auftraggebern der RZV und entsprechen den aktuellen, freigegebenen Technologien.

Informationsdienste, Benutzer und Informationssysteme werden in VLANs gruppenweise voneinander getrennt gehalten.

Das gesamte unternehmensweite Netzwerk (LAN/WAN) wird laufend hinsichtlich Funktionsfähigkeit und Performance überwacht. Dabei wird eine von Auftraggeberverträgen vorgegebene Verfügbarkeits- und Durchsatzquote zugrunde gelegt.

2.4.8 Firewall

Das LAN der RZV wird dreistufig, unter anderem, durch eine vom BSI zertifizierte Firewall gegen unerlaubte Zugriffe von außen geschützt (Paketfilter, Application Level Gateway, Paketfilter). Dabei übernimmt das Application Level Gateway zusätzlich zur inhaltsbezogenen Filterung auch Intrusion-Detection-Funktionalitäten. Aus Gründen der Verfügbarkeit ist die Firewall als Cluster ausgebildet und auf zwei Standorte verteilt.

Zum Schutz der Applikationen und Daten gegen Viren und andere Angriffe von Dritten werden zwei Virenscanner von unterschiedlichen Herstellern eingesetzt. Dabei übernimmt ein Virenscanner die Kontrolle des WAN-Eingangs während ein zweiter die Arbeitsplatzrechner schützt. Alle Virenbeschreibungsdateien werden mehrfach täglich auf Aktualität überprüft und ggf. erneuert.

Der Zugriff auf als unsicher eingestufte Internetseiten wird über eine von den Firewallherstellern bereitgestellte Blacklist verhindert. Darüber hinaus werden die Datenströme der Protokolle http, https und FTP im Rahmen ihrer Möglichkeiten auf Schadsoftware überprüft.

Die Firewallsysteme werden durch zwei Personen verwaltet und administriert, die fachlich in der Lage sind, sich vollumfänglich zu vertreten.

2.5 Rasche Wiederherstellung nach Zwischenfällen (Art. 32 Absatz 1 Buchstabe c DS-GVO): Notfall/Krisenmanagement

2.5.1 Störungen und Notfall/Krise

Eine Störung ist eine Situation, in der Systeme, Gebäude, Räumlichkeiten oder Ressourcen nicht wie vorgesehen zur Verfügung stehen oder funktionieren. Im Vergleich zu einem Notfall, sind die dadurch möglicherweise entstehenden Schäden eher als „gering“ einzustufen. Störungen (Incidents) werden durch die im allgemeinen Tagesgeschäft integrierte Störungsbehebung, im Rahmen des Prozesses "Management der Störungen (Incidents) und Serviceanfragen (Service Requests)", bearbeitet. Die Behebung einer Störung ist nicht Gegenstand des Notfall-/Krisenmanagements und wird aus diesem Grund hier nicht näher betrachtet. Eine schwerwiegende Störung (Major Incident) kann sich jedoch zu einem Notfall ausweiten und ist deshalb besonders zu beobachten.

Ein(e) Notfall/Krise ist ein Schadensereignis, bei dem die Verfügbarkeit unternehmenswichtiger Systeme oder Services innerhalb einer geforderten Zeit durch die im allgemeinen Tagesgeschäft integrierte Störungsbehebung nicht wiederhergestellt werden kann. Die Festlegung, dass ein Notfall eingetreten ist kann unmittelbar erfolgen oder zu einem späteren Zeitpunkt, wenn eine Störung zu einem Notfall eskaliert. Die Entscheidungskompetenz, dass ein Notfall eingetreten ist, liegt bei den Mitgliedern des Krisenstabs.

2.5.2 Notfall-/Krisenprozess - Alarmierung und Eskalation

Wird in der RZV ein Notfall erkannt oder tritt eine schwerwiegende Störung (Major Incident) auf, wird zunächst das RZV-Operating oder außerhalb der üblichen Bürozeiten die technische Rufbereitschaft unter der Rufnummer 02335/638-888 informiert. Dieses entscheidet, ob es eigenständig in der Lage ist die Störungsbeseitigung abzuwickeln, oder ob ggf. der „Second Level Support“ gerufen werden muss. Sollte sich nach einer ersten Analyse herausstellen, dass die Störungsbeseitigung nicht innerhalb von 2 Stunden abgeschlossen werden kann, so ist durch das RZV-Operating der Krisenstab gemäß festgelegter Meldewege zu informieren. Dieser beschließt und überwacht die weitere Vorgehensweise und entscheidet, ob ein Notfall/Krise vorliegt. Sollte ein(e) Notfall/Krise vorliegen, sind die zuständigen Notfallteams einzuberufen. Gleichzeitig sind ggf. Vorgaben durch die Geschäftsführung und den Krisenstab zu erstellen, welche Informationen an die Auftraggeber und möglicherweise auch an die Presse durch den Krisenstab und die Notfallteams zu übermitteln sind.

Nach Wiederherstellung der Funktionsfähigkeit wird dokumentiert, welche Ursachen für das Ereignis verantwortlich waren und ob Maßnahmen einzuleiten sind, die eine Wiederholung verhindern oder die Wahrscheinlichkeit einer Wiederholung reduzieren.

2.5.3 Notfall-/Wiederanlaufpläne, Wiederanlaufziele

Für den Fall, dass ein Notfall eingetreten ist, gibt es für die wichtigsten Notfallszenarien Notfall-/Wiederanlaufpläne, die die Sicherstellung der Leistungserbringung der RZV Services im Notfall/Krisenfall gewährleisten.

Zielvorgabe dabei ist, dass der Betrieb der zentralen Produktionssysteme und die Leistungserbringung der RZV Services nicht länger als gemäß SLA's zulässig oder falls keine SLA's explizit definiert sind 24 Stunden zusammenhängend unterbrochen ist.

Zur Sicherstellung, dass dieses Ziel auf der Basis der hier beschriebenen Szenarien erreicht werden kann, sind regelmäßige Tests zwingend notwendig. Hierfür stellen die Auftraggeber der RZV ggf. die benötigten Zeitfenster für Tests zur Verfügung, um die in den jeweiligen Notfall-/Wiederanlaufplänen beschriebenen Notfallszenarien auf Belastbarkeit zu überprüfen, und nehmen, wenn nötig, ihrerseits die Funktionsfähigkeit durch geeignete Testmaßnahmen ab. Die Testergebnisse werden dokumentiert.

2.6 Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen (Art. 32 Absatz 1 Buchstabe d DS-GVO)

2.6.1 Datenschutz-Management

Datenschutz und Informationssicherheit haben für die RZV als IT-Dienstleister im Gesundheitswesen eine exponierte Bedeutung. Alle technischen und organisatorischen Maßnahmen und datenschutzrelevanten Regelungen sind deshalb fest im unternehmensweit geltenden, integrierten Managementsystem der RZV verankert. Dieses ist insbesondere an § 28 der DS-GVO (Datenschutz-Grundverordnung der Europäischen Union), den international anerkannten Normen ISO/IEC 20000-1 (Servicemanagement) und ISO/IEC 27001 (Informationssicherheitsmanagement) sowie den Anforderungen des TÜViT-Prüfkataloges Trusted Site Infrastructure (TSI) ausgerichtet.

2.6.2 Regelmäßig überprüfte Qualität und Sicherheit

Zur Unterstreichung der Professionalität und IT-Kompetenz bei der Erbringung ihrer Dienstleistungen lässt die RZV ihr Managementsystem regelmäßig durch eine akkreditierte Zertifizierungsgesellschaft nach den folgenden international anerkannten Standards zertifizieren und jährlich wiederbegutachten:

- ISO/IEC 20000 (Servicemanagement)
- ISO/IEC 27001 (Informationssicherheitsmanagement)

Ergänzend zu den jährlich wiederkehrenden Wirksamkeitsüberprüfungen im Rahmen der ISO/IEC-Zertifizierungen wird das Management von Informationssicherheit und Datenschutz in der RZV regelmäßig von zwei weiteren neutralen externen Institutionen begutachtet durch:

- die TÜV Informationstechnik GmbH zur regelmäßigen (alle zwei Jahre) Überprüfung der IT-Infrastruktur der beiden Rechenzentren der RZV hinsichtlich der Anforderungen des TÜViT-Prüfkataloges Trusted Site Infrastructure (TSI),
- dem gemäß Art. 37 DS-GVO extern benannten RZV Datenschutzbeauftragten zur kontinuierlichen Aufgabenwahrnehmung gemäß Art. 39 DS-GVO.

2.6.3 Wirksamkeit Notfall-/Krisenmanagement

Jeweils im ersten Quartal eines Jahres wird in der Geschäftsleitungssitzung durch die Geschäftsführung und den verantwortlichen Führungskräften festgelegt, welche Notfallszenarien der verfügbaren Notfall-/Wiederanlaufpläne oder welche Notfall-/Krisenprozesse im Rahmen der Tests auf Funktionsfähigkeit und Belastbarkeit überprüft werden sollen. Die Organisation, Moderation und Ergebnisdokumentation dieses Tests wird vom RZV Service-Kontinuitäts- und Verfügbarkeitsbeauftragten durchgeführt. Alle notwendigen Maßnahmen werden protokolliert. Die Ergebnisdokumentation wird spätestens im vierten Quartal, wiederum in der Geschäftsleitungssitzung vorgestellt.

2.6.4 Rechte der betroffenen Personen gemäß Kapitel III DS-GVO

Die RZV hat als gegebenenfalls Verantwortlicher für die Verarbeitung geeignete Maßnahmen getroffen, um der betroffenen Person alle Informationen gemäß den Art. 13 und 14 DS-GVO und alle Mitteilungen gemäß den Art. 15 bis 22 und Art. 34 DS-GVO, die sich auf die Verarbeitung beziehen, gemäß Art. 12 DS-GVO zu übermitteln. Ansprechpartner zur Wahrung der Rechte der betroffenen Personen gemäß DS-GVO sind die Geschäftsführer der RZV und der benannte Datenschutzbeauftragte.

2.7 Aufsicht des Verantwortlichen (Art. 29 DS-GVO), Authentizität von Aufträgen und Auftragskontrolle

Die RZV und jede der RZV unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen Daten ausschließlich auf Weisung des Auftraggebers als Verantwortlichem gemäß Art. 4 DS-GVO verarbeiten.

Alle Mitarbeiterinnen und Mitarbeiter sind deshalb verpflichtet, personenbezogene Daten, die im Auftrag ihrer Auftraggeber verarbeitet werden, nur entsprechend der schriftlichen Vereinbarungen mit den jeweiligen Auftraggebern zu verarbeiten.

Für darüberhinausgehende Aufträge erteilen Auftraggeber der RZV eine entsprechende schriftliche Weisung. Diese Weisungen werden ausschließlich schriftlich oder per E-Mail erteilt. Anweisungen per E-Mail werden immer durch entsprechende Verfahren (z.B. durch Auftragsbestätigungen an den Auftraggeber oder über die innerhalb des Systems eingerichteten Kommunikationsmöglichkeiten) authentisiert.

3 Verpflichtung zur Vertraulichkeit (Art. 28 DS-GVO) und auf das Datengeheimnis (§ 26 DSG-EKD bzw. § 5 KDG bzw. § 53 BDSG)

3.1 Verpflichtung von Mitarbeiterinnen und Mitarbeitern zur Vertraulichkeit und auf das Datengeheimnis

Bei der Verarbeitung personenbezogener Daten haben die Mitarbeiterinnen und Mitarbeiter für ihren Verantwortungsbereich und ihren Arbeitsplatz die technisch und organisatorisch erforderlichen Vorkehrungen für die Einhaltung der Datenschutzbestimmungen und -gesetze zu treffen.

Die Mitarbeiterinnen und Mitarbeiter der RZV sind gemäß einer gesonderten Erklärung zur Vertraulichkeit im Sinne von Art. 28 Absatz 3 Buchstabe b DS-GVO, auf das Datengeheimnis gemäß § 26 DSG-EKD bzw. § 5 KDG bzw. § 53 BDSG und zur generellen Einhaltung einschlägiger Datenschutzvorschriften, insbesondere DS-GVO, Kirchengesetz über den Datenschutz der Evangelischen Kirche in Deutschland (DSG-EKD, Gesetz über den Kirchlichen Datenschutz (KDG) und Bundesdatenschutzgesetz (BDSG), verpflichtet und im Rahmen einer gesonderten Schulung in die Bestimmungen der RZV eingewiesen.

Ein Verstoß gegen die Vertraulichkeitspflicht wird arbeits-, dienst- oder disziplinarrechtlich und gegebenenfalls strafrechtlich verfolgt.

3.2 Verpflichtung von Mitarbeiterinnen und Mitarbeitern weiterer Auftragsverarbeiter im Sinne von Art 28 Absatz 4 DS-GVO

Weitere Auftragsverarbeiter, deren Dienste die RZV in Anspruch nimmt, um bestimmte Verarbeitungstätigkeiten mit Zugriffsmöglichkeit auf personenbezogene Daten im Namen des Auftraggebers als Verantwortlichem auszuführen, sind gesetzlich oder vertraglich zur Einhaltung der einschlägigen Datenschutzgesetze in der jeweils gültigen Fassung verpflichtet. Darin enthalten ist insbesondere die Pflicht, Mitarbeiterinnen und Mitarbeiter bei der Aufnahme ihrer Tätigkeit gemäß einer gesonderten Erklärung zur Vertraulichkeit im Sinne von Art. 28 Absatz 3 Buchstabe b DS-GVO, auf das Datengeheimnis und zur Einhaltung einschlägiger Datenschutzvorschriften, insbesondere DS-GVO, zu verpflichten und darauf hinzuweisen, dass diese Verschwiegenheitspflicht auch nach Beendigung ihrer Tätigkeit fortbesteht.