Anlage 1 - Technisch-organisatorische Maßnahmen (TOM), der simple system GmbH

Art. 32 DSGVO, Version 1.0

Inhaltsverzeichnis

Änderungshistorie

Version	Datum	Bearbeiter	Änderung
1.0	21.12.2017	DSB	Erstmalige Erstellung

1. Einleitung und Rahmenbedingungen

Die folgenden Festlegungen repräsentieren das Datenschutzkonzept simple system GmbH & Co. KG (nachfolgend simple system).

simple system legt damit die Standards fest, nach denen die Standorte alle Formen von papiergebundenen und elektronischen Informationen während der Verarbeitung, vom Dateneingang bis zur Vernichtung der Daten, behandeln, schützen und nach der Erbringung der Dienstleistung gemäß der jeweils vereinbarten Anforderung des Kunden vernichten.

Es werden in einzelnen Teilbereichen die entsprechenden Maßnahmen beschrieben, die simple system durchführt, um einen unzulässigen Umgang mit personenbezogenen Daten und Dokumenten sowie eine unzulässige Verwendung von personenbezogenen Daten gemäß der jeweils gültigen Datenschutzgesetze zu verhindern und eine entsprechende IT-Sicherheit zu gewährleisten.

1.1. Anwendungsbereich

Die folgenden Festlegungen werden für die gesamte Verarbeitung und somit für alle von simple system übernommenen Aufträge und Aufgaben eingehalten.

Da aufgrund verschiedenster Auftragsspezifikationen davon auszugehen ist, dass verschiedene Aufträge mit höheren oder niedrigeren Datenschutzstandards verarbeitet werden müssen, ist der Anwendungsbereich der in diesem Dokument definierten Standards durch entsprechende Einzelvereinbarungen mit den Auftraggebern einzuschränken oder zu erweitern. Dies kann insbesondere dann der Fall sein, wenn Subunternehmer an der Leistungserbringung beteiligt sind.

Weiterhin können die Sicherheitsanforderungen auf Wunsch eines Auftraggebers, erhöht werden, soweit dies in einem Dokument zur entsprechenden Auftragsdokumentation schriftlich vereinbart wird.

1.2. Verantwortlichkeiten Gesamtverantwortung

1.2.1.1. Gesamtverantwortung

Die Gesamtverantwortung, insbesondere für die Festlegung der Anforderungen sowie Inhalte und Ziele des Datenschutzkonzepts einschließlich der fortlaufenden Prüfungen und Verbesserung der Regelungen, übernimmt der Datenschutzkoordinator von simple system. Dieser steht überwachend und beratend der Datenschutzbeauftragte zur Seite.

1.2.1.2. Überwachung und Durchführung

Für die Überwachung der Durchführung ist externer Datenschutzbeauftragter bestellt, der die Aufgaben gemäß den gesetzlichen Bestimmungen der jeweils gültigen Datenschutzgesetze wahrnimmt. Als Datenschutzbeauftragter ist bestellt:

Firma	Anschrift	Kontakt
MKM Datenschutz GmbH	Äußere Sulzbacher Straße 124a 90491 Nürnberg	+49 911 66 95 77 55

Der Datenschutzkoordinator der simple system unterstützt den Datenschutzbeauftragten bei der Erfüllung seiner Aufgaben.

2. Technische und organisatorische Maßnahmen

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

2.1.1. Zutrittskontrolle

Das Ziel einer Zutrittskontrolle ist es, Unbefugten den Zutritt (z.B. zu Datenverarbeitungsanlagen) zu verwehren, mit denen personenbezogene Daten verarbeitet oder genutzt werden. Der Begriff des Zutritts ist dabei räumlich zu verstehen.

Den Zutritt zu unserem Firmengebäude stellen wir durch folgenden Maßnahmen sicher:

- Protokollierte Vergabe von Zutrittsberechtigungen
- Entzug der Zutrittsberechtigung nach Ausscheiden
- Türsicherungen (elektrische Türöffner) mit Chipkarte

2.1.2. Zugangskontrolle

Das Ziel einer Zugangskontrolle ist es, mit Hilfe geeigneter Maßnahmen zu verhindern, dass Unbefugte Datenverarbeitungsanlagen und -systeme, mit denen personenbezogene Daten verarbeitet oder genutzt werden, eindringen oder nutzen können.

Um den Zugang zu unserem Netzwerk zu schützen, haben wir folgende Maßnahmen getroffen:

- Benutzerverwaltung zur Anmeldung
- Individueller Benutzername und Passwort
- Segmentierung von Netzwerken nach Schutzbedürftigkeit
- Einsatz von Virenscanner und Firewall
- Einsatz sicherer Übertragungstechnik (VPN)
- Passwortregelung (Anzahl Zeichen, Sonderzeichen, Historie, keine Zeichenfolgen)

2.1.3. Zugriffskontrolle

Das Ziel einer Zugriffskontrolle ist es zu gewährleisten, dass ausschließlich die zur Benutzung der Datenverarbeitungssysteme Berechtigen auf die ihrer Zugriffsberechtigung unterliegenden personenbezogene Daten zugreifen können und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, vervielfältigt, verändert oder entfernt werden können.

Um unerlaubte Tätigkeiten innerhalb der Systeme von simple system außerhalb der eingeräumten Berechtigungen zu verhindern, haben wir folgende Maßnahmen getroffen:

- Rechtevergabe nach Rollen / Organisationseinheiten
- Verwaltung der Zugriffsrechte durch Administrator
- Datenschutzkonforme Entsorgung von Datenträgen und Papier
- Mobile Datenträger enthalten keine personenbezogenen Daten

2.1.4. Trennungskontrolle

Das Ziel des Trennungsgebots ist es zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten ebenfalls getrennt voneinander verarbeitet werden.

Um sicherzustellen, dass zu unterschiedlichen Zwecken erhobene Daten getrennt voneinander verarbeitet werden, haben wir die folgenden Maßnahmen getroffen:

- Funktionstrennung durch mandantenfähige Systeme
- Erstellung Berechtigungskonzept und Vergabe nach Rollen
- Datentrennung durch Netzsegmentierung
- Trennung von Entwicklungs-, Test- und Produktivsystemen

2.1.5. Pseudonymisierung (Art. 32 Abs. 1 lit. a DS-GVO; Art. 25 Abs. 1 DS-GVO)

Die 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

- Pseudonymisierung mittels einer eindeutigen Identifikationsnummer (ID). Diese ID wird im System bei der Erstellung von Protokollierungen verwendet.

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

2.2.1. Weitergabekontrolle

Das Ziel einer Weitergabekontrolle ist es zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, vervielfältigt, verändert oder entfernt werden können und dass überprüft sowie festgestellt werden kann, an welchen Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zu Datenübertragung vorgesehen ist.

Folgende Maßnahmen haben wir im Bezug auf die Weitergabe von personenbezogenen Daten getroffen:

- Sichere Aufstellung von Servern und SAN (Sicherheitsbereich) / NAS
- Unternehmenseigene Domain zur E-Mail-Kommunikation (intern)
- Weitergabe an Dritte nur nach Prüfung der Rechtsgrundlage
- Schriftliche Festlegung der Weitergabe in Drittländer
- Sichere Übertragung von Datenlieferungen (SFTP, VPN)

- Beschränkung des zur Übermittlung befugten Personenkreises

2.2.2. Eingabekontrolle

Das Ziel einer Eingabekontrolle ist es, dass nachträglich festgestellt werden kann, ob und von wem personenbezogene Daten in die Systeme und Anlagen zur Datenverarbeitung eingegeben, verändert oder entfernt worden sind.

Die Nachvollziehbarkeit innerhalb der Datenverwaltung stellen wir wie folgt sicher:

- Protokollierung der Eingabe personenbezogener Daten
- Zweckfestlegung der Protokolldaten

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

2.3.1. Verfügbarkeitskontrolle

Das Ziel der Verfügbarkeitskontrolle ist es zu gewährleisten, dass personenbezogene Daten gegen die Zerstörung oder Verlust physisch sowie auch logisch geschützt sind.

Da die Daten ausschließlich in den Räumlichkeiten unserer externen Rechenzentren verarbeitet werden, verweisen wir hinsichtlich der Verfügbarkeit der Daten auf die **Anlage 1.A** zu dieser Vereinbarung.

2.4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO)

2.4.1. Allgemein

Allgemeine Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

- Datenschutz-Management
- Incident-Response-Management
- Regelmäßige Prüfungen durch den Datenschutzbeauftragten

2.4.2. Auftragskontrolle

Das Ziel einer Auftragskontrolle im Sinne von Art. 28 DS-GVO ist es zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend des Auftrags und den Weisungen des Auftragsgebers verarbeitet werden können.

- Vertragliche Regelungen gemäß § 11 BDSG (Auftragsdatenverarbeitung)
- Unteraufträge nur bei gleichwertigem Schutzniveau
- Prüfung und Dokumentation beim Auftragnehmer getroffener Maßnahmen
- Verpflichtung der Mitarbeiter von Auftragnehmern auf das Datengeheimnis

3. Begleitende Dokumente zu den technisch-organisatorischen Maßnahmen

Die Verarbeitung der personenbezogenen Daten erfolgt auf Servern in von simple system beauftragten Rechenzentren. simple system hat alle erforderlichen datenschutzrechtlichen Verträge

mit den Rechenzentrumsbetreibern abgeschlossen. In Anlage 1. A sind die technischen und organisatorischen Maßnahmen der Rechenzentren beschrieben.

4. Weitere Maßnahmen

Sämtliche Beschäftigten von simple system, die personenbezogene Daten verarbeiten, sind in Schriftform zur Wahrung der Vertraulichkeit verpflichtet. Die Beschäftigten werden durch den Datenschutzbeauftragten regelmäßig im Umgang mit personenbezogenen Daten geschult.

5. Schlussbestimmung

Der Datenschutz unterliegt bei simple system einem kontinuierlichen Verbesserungsprozess und wird an die jeweiligen aktuellen und gültigen Datenschutzbestimmungen angepasst. Eine Aktualisierung des Dokuments findet fortlaufend statt.

Anlage 1. A - Technische und organisatorische Maßnahmen des Rechenzentrumsdienstleisters

Technische und organisatorische Maßnahmen des Rechenzentrumsdienstleisters - SpaceNet AG

1. Zutrittskontrolle

- elektronisches Zutrittskontrollsystem mit Protokollierung
- dokumentierte Schlüsselvergabe an Mitarbeiter
- Richtlinien zur Begleitung von Gästen im Gebäude
- 24/7 personelle Besetzung der Rechenzentren
- Videoüberwachung an den Ein- und Ausgängen
- Türsicherungen (elektrische Türöffner, usw.) mit Chipkarte bzw. Fingerabdruckscanner
- Zutritt nur nach Anmeldung mit Besucherkontrolle, Begleitung und Einweisung
- Videoüberwachung aller RZ-Zugangsbereiche und Räume
- Alarmanlage für Außensicherung (Türen, Fensteröffnungskontakte)

2. Zugangskontrolle

- Zugang ist passwortgeschützt, Zugriff besteht nur für Mitarbeiter des Auftragnehmers und ggf. des Auftraggebers
- Passwörter, die der Auftragnehmer dem Auftraggeber mitteilt werden mit einem Passwortgenerator erstellt
- Zentrale und geschützte Kennwortverwaltung
- Kennwortrichtlinie

3. Zugriffskontrolle

- Durch regelmäßige Sicherheitsupdates und Backups (nach dem jeweiligen Stand der Technik) stellt der Auftragnehmer sicher, dass unberechtigte Zugriffe verhindert werden
- Revisionssicheres, verbindliches Berechtigungsvergabeverfahren für Mitarbeiter des Auftragnehmers

- Für übertragene Daten/Software/Applikationen ist einzig der Auftraggeber in Bezug auf Sicherheit und Updates zuständig
- Bedarfsorientierte Ausgestaltung eines Berechtigungskonzeptes und der Zugriffsrechte gemeinsam mit dem Auftraggeber sowie deren Überwachung und Protokollierung
- Protokollierung von Jobs via Ticketsystem
- Automatische Erzeugung von Protokolldateien, wo technisch möglich und sinnvoll, sowie Auswertung dieser Logs im Verdachtsfall. Zyklische automatische Löschung durch Rotation
- Authentifizierungsrichtlinie
- Ansprechpartner und ihre Berechtigung sind individuell hinterlegt

4. Weitergabekontrolle

- Alle Mitarbeiter sind auf das Datengeheimnis nach § 5 BDSG verpflichtet
- Datenschutzgerechte Löschung der Daten nach Auftragsbeendigung gem. Ziffer 10 der Vereinbarung
- Möglichkeiten zur verschlüsselten Datenübertragung werden im Umfang der Leistungsbeschreibung des Hauptauftrages zur Verfügung gestellt
- Trennung von Netzen, insbesondere zwischen Internet (Außenwelt) und Innennetz. Umsetzung von Multi-Tier-Architekturen mit abgestuften Sicherheitsbereichen und Schutzmechanismen (z.B. Firewalls, Intrusion Detection Systems, o.a.) sind möglich
- Verschlüsselungen und Tunnelverbindungen (SSL, VPN)
- Protokollierung von Übertragungsvorgängen

5. Eingabekontrolle

- Die Daten werden vom Auftraggeber selbst eingegeben bzw. erfasst.
- Protokollierung externer Zugriffe
- Nachweis der Beauftragung und erfolgter Abarbeitung im Ticketsystem

6. Auftragskontrolle

- Unsere Mitarbeiter werden in regelmäßigen Abständen im Datenschutzrecht unterwiesen auch im Hinblick auf das Weisungsrecht des Auftraggebers
- Der Auftragnehmer hat einen betrieblichen Datenschutzbeauftragten bestellt und sorgt durch die Datenschutzorganisation für dessen angemessene und effektive Einbindung in die relevanten betriebliche Prozesse

7. Verfügbarkeitskontrolle

- Backup- und Recovery-Konzept mit täglicher Sicherung der Daten je nach gebuchten Leistungen des Hauptauftrages
- Einsatz von Festplattenspiegelung
- Einsatz unterbrechungsfreier Stromversorgung
- Einsatz von Portreglementierungen
- Vermeidung von Single-Point-of-Failures als Grundgedanke aller Infrastruktur im Rechenzentrumsbetrieb, d.h. Sicherstellen von Verfügbarkeit durch Redundanz von Systemen und Komponenten
- Vermeidung von Single-Point-of-Failures in Auftraggebersystemen je nach gebuchten Leistungen des Hauptauftrages
- Redundante Stromversorgung (Hauptversorgung, Trafo, Unterbrechungsfreie Stromversorgung durch USV, Notstromgeneratoren auf Basis von Dieselmotoren im Außenbereich)
- Datensicherung, d.h. Backup, auch Shared Backup ist räumlich getrennt buchbar
- Verwendung von Firewalls und Load Balancern zur Zugangs- und Content-Filterung und horizontalen Lastverteilung auch bei Shared Services buchbar
- Klimaversorgung
- 7x24h Monitoring aller Systeme der Rechenzentrumsinfrastruktur.
- Notfallpläne (BCM) gemäß ISO 27001-Standart für den Rechenzentrumsbetrieb

Technische und organisatorische Maßnahmen des Rechenzentrumsdienstleisters - Noris Networks

1) Zutrittskontrolle

Die schützenswerten Daten werden in den noris network Rechenzentren verarbeitet.

Vermeidung von Lagehinweisen auf schützenswerte Gebäudeteile

Die Rechenzentren sind als schützenswerte Gebäudeteile zu sehen. An den Standorten ist die genaue Lage der Rechenzentrumsfläche bzw. der dazugehörigen Technikräume nicht ersichtlich.

Geschlossene Fenster und Türen

Die Rechenzentren haben keine Fenster; Türen schließen selbsttätig.
In der Deutschherrnstraße in Nürnberg ist zum Rechenzentrum NBG3 die Außentür (am Perimeter) des Rechenzentrums (zur Schleuse) tagsüber zugänglich, es ist jedoch absolut nicht ersichtlich, dass es sich um ein Rechenzentrum handelt (durch allgemeine Merkmale), die äußere Schleusentür ist dann bereits wieder verriegelt; erst in der Schleuse ist eine Identifikation als Rechenzentrum offensichtlich. Ebensowenig ist das Deutschherrnkarree als Ganzes vom äußeren Erscheinungsbild nicht als Rechenzentrumsstandort ersichtlich, jedoch sind hier viele verschiedene Rechenzentren untergebracht.

In der Seidlstraße in München ist zum Rechenzentrum MUC6 die Außentür (am Perimeter) bzw. die Tiefgarage tagsüber zugänglich, es ist jedoch absolut nicht ersichtlich, dass es sich um ein Rechenzentrum handelt (durch allgemeine Merkmale), die äußere Etagentür zum Pförtnerdienst ist dann bereits wieder verriegelt; erst im Innenbereich ist eine Identifikation als Rechenzentrum offensichtlich.

Aufzeichnungen

Die Türzutrittskontrollprotokolle werden gesichtet, stichprobenartig überprüft und archiviert.

Büroräumlichkeiten

Zutrittskontrollsysteme an den Eingängen. Keine exponierte Erdgeschosslage (mit Ausnahme der Geschäftsstelle in der Deutschherrnstraße in Nürnberg, wo kurze Laufwege zu den beiden Rechenzentren NBG3 und NBG4 maßgeblich sind). Mitarbeiter sind angewiesen, Fenster und Türen außerhalb der Bürozeiten geschlossen bzw. verschlossen zu halten. Der Sicherheitsdienst überprüft darüberhinaus außerhalb der Bürozeiten, dass Fenster und Türen geschlossen sind.

Gefahrenmeldeanlage

Die Gefahrenmeldeanlage für Brand- und Alarmdetektion ist durchgängig über das noris-network-Monitoring realisiert.

Hierfür ist ein stiller Alarm mit verschiedenen Alarmmeldelinien und direkter Koppelung an das noris-network-Monitoring-System und die daran angeschlossene 24-h-Rufbereitschaft durch noris-Mitarbeiter realisiert. Diese alarmieren entsprechend Notfallplan die Polizeibehörden.

In den Rechenzentren ist eine Rauchdetektion direkt an das noris-network-Monitoring und die daran angeschlossene 24-h-Rufbereitschaft durch noris-Mitarbeiter gekoppelt. Die Bearbeitung findet entsprechend der Einträge im Notfallplan statt.
An den Standorten Deutschherrnstraße in Nürnberg, Seidlstraße in München und Elisabeth-Selbert-Straße in München, in Kürze auch in der Thomas-Mann-Straße in Nürnberg, wird darüber hinaus Feueralarm über BMZ (Brand-Melde-Zentrale) automatisch an die jeweilige Berufsfeuerwehr gemeldet. Die Grundlage bilden entsprechende Branddetektoren und Feuermelder.

Im Rechenzentrum NBG3 in der Deutschherrnstraße sind Wasserdetektionsbänder mit Meldestrecke an das noris-network-Monitoring-System und die daran angeschlossene 24-h-Rufbereitschaft durch noris-Mitarbeiter gekoppelt. Die Bearbeitung findet entsprechend Notfallplan statt.

Videoüberwachung

Die Rechenzentren sind jeweils in der Schleuse und in den Rechenzentren videoüberwacht. Optional können über weitere Kameras einzelne Schrankreihen überwacht werden. Identifizierung zu Überwachungszwecken, Erkennung und Lokalisierung von Gefahren bzw. Schadensverhütung und Alarmierung wird über Sichtprüfung und in Stichproben vom zentralen Operatingplatz in Nürnberg aus für die Rechenzentren durchgeführt.

Eine Stichprobe der digitalisierten Bewegungsbilder im Rechenzentrum kann durchgeführt und mit den archivierten Daten (Zutrittskontrollprotokolle) abgeglichen werden, um eine Kontrolle über die Zutritte hinsichtlich Legitimität der stattgefundenen Handlungen zu erhalten.

Perimeterschutz

An den Standorten Deutschherrnstraße/Thomas-Mann-Straße in Nürnberg und am Standort Elisabeth-Selbert-Straße in München ist das Areal jeweils mit Pförtnerkabine und Schranken an den Zufahrten ausgestattet, um hier eine ordnende oder abschreckende Wirkung zu erreichen. In der Kilianstraße in Nürnberg ist das Gebäude als Gebäude ohne Publikumsverkehr zu werten und demnach von außen verschlossen zu halten. Weitere Perimeterschutzmaßnahmen werden derzeit nicht realisiert.

Schlüsselverwaltung / Ausweisverwaltung

Diese obliegt der Personalverwaltung, die hier die entsprechenden Prozesse, insbesondere in Bezug auf Entzug der Berechtigungen von Mitarbeitern nach Verlassen der Firma berücksichtigt.

Beaufsichtigung oder Begleitung von Fremdpersonen

Bei Zutritt externer Dienstleister gelten die entsprechenden Schutzbestimmungen von noris network (spezielle Prozessdefinitionen beim Zutritt zum Rechenzentrum: Umfang, Zeitpunkt, Firmenname, Name mit Unterschrift, spezifische Zutrittskontrollkarte, Begleitung eines Mitarbeiters, Kameraüberwachung etc.), die Dokumentation im „Ticket“ im Ergebnis rundet die Tätigkeit ab.

Maßnahmen von Fremdpersonen werden jeweils im Beisein eines noris-network-Mitarbeiters durchgeführt, in Ausnahmefällen auch durch entsprechende Einweisungen der Arbeitskräfte und entsprechender Überwachung durch geeignete Maßnahmen (insbesondere Videoüber-wachung), Nachweis des Zutritts und Verlassen des Rechenzentrums über Archivierung des Zugangskontrollsystems.

Zutritt der Rechenzentrumsbereiche zu Geschäftszeiten

Der Zugang zu den Rechenzentren ist nicht für den Publikumsverkehr vorgesehen. Nur die Systemverantwortlichen haben Zutritt zu den Systemen. Die Schlüsselgewalt besitzen nur der IT-Sicherheitsbeauftragte, der IT-Leiter und der Rechenzentrumsbetriebsleiter.
Alle anderen Berechtigten sind auf entsprechende Zugangskarten bzw. die Eingabe eines Systemcodes angewiesen, im Rechenzentrum Thomas-Mann-Straße in Nürnberg wird künftig auch eine Biometriefunktion implementiert werden.

Der Zutritt wird zeitlich auf die regulären Geschäftszeiten der noris network AG beschränkt.
Weiterhin findet zu Bürozeiten eine stichprobenartige Sichtung der Überwachungskameras am zentralen noris-network-Leitstand in Nürnberg statt.

Besonderes Verfahren außerhalb Geschäftszeiten

Zu Geschäftszeiten ist davon auszugehen, dass berechtigtes Bedienungspersonal sich regelmäßig in den Rechenzentrumsbereichen aufhält.

Außerhalb dieser Zeiten ist ein Vier-Augen-Prinzip für den Zutritt zu den Rechenzentren erforderlich (mindestens telefonische Kontaktaufnahme, Fernbedienung des jeweiligen Tür-öffnungssystems durch das 24-h-Betreitschafts-Bedienerpersonal, unter ggf. gleichzeitiger Sichtung per Videokontrolleinrichtung).

Wenn nach vereinbarter Verweildauer kein Lebenszeichen vom Berechtigten zu vernehmen ist, erkundigt sich der Mitarbeiter des Bedienerpersonals über den Verweilort des Berech-tigten, um hier Gefahr für Leib und Leben auszuschließen. Der Berechtigte gibt andernfalls einen abschließenden Rapport, nachdem das Rechenzentrum verlassen wurde.

Die beim Sicherheitsdienst hinterlegte Zugangskarte/Schlüssel darf nicht eingesetzt werden, außer für Notfälle (insbesondere für den akuten Brandeinsatz der Feuerwehr nach auto-matischer Auslösung einer Brandmeldung für das Rechenzentrum im zentralen Feuermelde-Systems).

Kontrolle des Rechenzentrums-Zutritts

Der Zutritt zu den Rechenzentren über Zugangskarten wird protokolliert, und durch den Rechenzentrumsbetriebsleiter archiviert.
Das automatische Kontrollsystem lässt vollautomatisch nur den Zutritt für die berechtigten Zugangskartenbesitzer zu.

Die Videokontrolleinrichtungen erfassen systematisch alle Zutritts-Schleusen und wichtigen Systemkomponenten. Diese werden stichprobenartig in Hinblick auf Verdachtsmomente ausgewertet.

Kontrollgänge

In den Rechenzentren finden regelmäßige Kontrollgänge statt. Diese finden ferner auch im Rahmen des Brandschutzes statt, siehe auch Punkt 7.

Es finden für die Rechenzentren tägliche, wöchentliche und monatliche Kontrollgänge nach Checkliste statt. Die Ergebnisprotokolle der Begehungen sind in Papierform beim Rechenzentrumsbetriebsleiter einzusehen.

Umgang mit und Sicherheit von Datenträgern

Mobile Datenträger wie Bänder, Platten und Kassetten werden bei Bedarf nur in abgesperrten Schutzbereichen (insbesondere Safe) gelagert.

Gedruckte Aufzeichnungen sind, soweit diese als streng vertraulich gekennzeichnet sind, ebenfalls im Safe gelagert. Der jeweilige Safe ist nur für einen definierten Personenkreis zugänglich, der Zugriff auf diese Dokumente haben muss.

Schutzzonen

Innerhalb des Rechenzentrums sind getrennte Bereiche für Carrier (Datenleitungen), Stromversorgung (Stromunterverteilung) und Racks (absperrbare Racks), bzw. bei einzelnen Kundenprojekten dedizierte Cages (abgegrenzte Käfigbereiche auf der IT-Fläche) aufgebaut, für die nur ein eingeschränkter Personenkreis Zutritt erhält, und bei denen es eine abgesicherte Zutrittsmöglichkeit (zusätzlicher Alarmkreis in der Alarmanlage) gibt.

Notausgänge

Die Rechenzentren besitzen Notausgänge nach Brandschutzverordnung; dabei wird sichergestellt, dass Alarm ausgelöst wird, wenn die nur von innen durchführbare Panikfunktion einer Tür betätigt wird.

2) Zugangskontrolle

Für sämtliche schützenswürdigen Systeme der Datenverarbeitung, d. h. auch für die dazugehörigen Testsysteme, wird eine Benutzerverwaltung durchgeführt.

Die Benutzerverwaltung wird grundsätzlich personenbezogen durchgeführt.

Grundlage der Passwort-Policy sind die allgemeinen Vorgaben zum Aufbau von Kennwörtern (wie Mindestlänge, Kennwortkomplexität). Diese können bei Bedarf durch eine systemspezifische Policy auf den konkreten Schutzbedarf angepasst werden.

Darüber hinaus werden im Rahmen der Systemhärtung - in Abstimmung mit dem Kunden - Einschränkungen oder Sperrungen von Gast- und/oder Administrator-Zugriffen durchgeführt, die Sperrung von Benutzer- oder Administrator-Passwörtern nach mehreren ungültigen Fehlversuchen veranlasst, und bei Bedarf eine Passwort-Historie mit einem Verbot der Mehrfachänderung bzw. Wiederholung von Passwörtern innerhalb einer vordefinierten Zeitspanne, vereinbart.

Die Speicherung der Zugriffe (und –versuche) wird im Systemlog durchgeführt.

Für Sitzungen gibt es ein definiertes Timeout.

Clean-Desk-Policy

In regelmäßigen Security-Awareness-Trainings wird allen Mitarbeitern das Bewusstsein einer sorgsamen Absicherung ihres Arbeitsumfeldes aufgefrischt. Die Eingabe eines Passwortes muss unbeobachtet erfolgen, geschäftliche Passwörter dürfen nicht außerhalb (z. B. privat zuhause) verwendet werden. Die Vertraulichkeit muss gewährleistet sein. Passwörter dürfen vom Anwender nicht hinterlegt werden (weder schriftlich noch elektronisch), Ausnahme ist das Notfallpasswort im Safe.

Bei Bedarf kommen weitere Systemzugangs-Einschränkungen zum Einsatz, die der Auftraggeber mit dem Auftragnehmer je nach Art der zu schützenden Daten den konkreten organisatorischen Datenverarbeitungsprozess abstimmt, wie etwa: Nutzung von Benutzer-Zertifikaten oder One-Time-Passwort-Verfahren anstelle von Passwörtern.

3) Zugriffskontrolle

noris network setzt nach Anforderung des Auftraggebers Sicherheitsgateways (Firewalls) bzw. Bei Bedarf geeignete Zusatzlösungen wie Applikations-Firewalls, Next Generation Firewalls u. ä. ein, die ihrerseits eine Intrusion-Prevention oder Intrusion-Detection (z. B. nach Portscans u. ä.) durchführen können.

noris network realisiert für den Kunden bei Bedarf einen Virenscan. Die Virenscanner-Patterns werden in regelmäßigen Abständen (ca. jede halbe Stunde) – soweit verfügbar - vom Hersteller abgerufen. Dieser Vorgang wird automatisiert überwacht. Die Annahme von Viren und anderen Bedrohungen (wie z. B. DUL) wird bereits im Vorfeld unterbunden.

noris network hat geordnete Verfahren und Abläufe für Security-Patches und gemeldete Schwachstellen, und bewerkstelligt darüber hinaus eine automatisierte Eskalation von Sicherheitsmeldungen des DFN-CERT.

Sicherheitsüberprüfungen, wie etwa Vulnerability-Scans mit anschließender Bewertung werden bei Bedarf regelmäßig durchgeführt.

4) Weitergabekontrolle

Mobile Datenträger wie Bänder, Platten und Kassetten werden bei entsprechendem Schutz-bedarf im Safe gelagert.

Auf mobilen Devices (USB-Sticks, DVDs) müssen alle schützenswürdigen Daten nach aktuellen kryptographischen Standards verschlüsselt abgelegt sein.

Alte oder defekte Devices werden mittels professioneller Datenträgerentsorgung vernichtet.

Entsprechend mit geheim oder vertraulich klassifizierte Dokumente befinden sich in besonders geschützten Serversystemen oder Dateisystemen, über die ein Zugriff von Außenstehenden erschwert oder verhindert werden kann, um damit vor unberechtigter Offenlegung oder Missbrauch zu schützen. Tape-Libraries und Plattensysteme werden in entsprechenden Schutzbereichen (Racks oder Cages) untergestellt.

Datenkommunikation

Schützenswürdige Daten werden bevorzugt über Datenleitungen statt mittels physikalischem Transport übertragen, um das Risiko von Verlust oder einen Daten-Diebstahl über diese traditionellen Transportwege ausschließen zu können. Dabei kommt über öffentliche Kommunikationskanäle (wie Internet-Datenverkehr) eine verschlüsselte Datenübertragung zum Einsatz (z. B. per SSL, IPsec, SSL-VPN).

E-Mail-Sicherheit

Grundsatz für die E-Mail-Sicherheit bedeutet bei noris network: die Verwendung von Verschlüsselung, wo diese möglich ist (insbesondere TLS-Verschlüsselung). Die Mitarbeiter werden regelmäßig hinsichtlich der Gefahren in Bezug auf Viren bzw. Malware sensibilisiert. Über Viren-/Malware- und Spam-Filter-Schutzmaßnahmen werden die E-Mail-Sicherheitsrisiken systematisch reduziert.

5) Eingabekontrolle

Der Auftraggeber stimmt mit dem Auftragnehmer je nach Art der zu schützenden Daten den konkreten organisatorischen Datenverarbeitungsprozess ab. noris network kann hierfür bei Bedarf die notwendigen technischen Einrichtungen zur Protokollierung und Archivierung zur Verfügung stellen.

Die entsprechend mit den datenschutzrechtlichen Systemen betrauten Personen besitzen ein besonderes Vertrauensverhältnis und sind namentlich benannt. Die Aktivitäten für die Systemadministration (mit Zeitpunkt der Aktivität und Angabe der ausführenden Person) werden aufgezeichnet.

Flankierend dazu werden alle mit der Betriebsführung betrauten Mitarbeiter auf das Datengeheimnis (nach § 5 BDSG) verpflichtet und in regelmäßigen Abständen Veran-staltungen und Fortbildungen zum Thema Datensicherheit durchgeführt.

Die Grundlage für die Maßgaben zur Eingabekontrolle stellt eine effektive Zugangskontrolle nach Punkt 2) dar.

6) Auftragskontrolle

Der Auftraggeber stimmt mit dem Auftragnehmer je nach Art der zu schützenden Daten den konkreten organisatorischen Datenverarbeitungsprozess ab. Bei Bedarf wird die Betriebs-führung (Operating) nach Betriebshandbuch und alle Änderungen mittels definiertem „Change“-Verfahren durchgeführt, um eine adäquate Auftragskontrolle durch den Auftrag-geber sicherzustellen. Ein Change-Prozess nach ITIL stellt sicher, dass eine Freigabe durch den Kunden erfolgt und bei Bedarf ein mehrstufiger Change in Testumgebung und Produktionsumgebung durchgeführt werden kann.

Flankierend dazu werden alle mit der Betriebsführung betrauten Mitarbeiter auf das Datengeheimnis (nach § 5 BDSG) verpflichtet und in regelmäßigen Abständen Veran-staltungen und Fortbildungen zum Thema Datensicherheit durchgeführt.

7) Verfügbarkeitskontrolle

Um die Erfordernis der Rückspielung eines Backups im Vorfeld freizuhalten, betreibt die noris network AG ihre Rechenzentren nach Hochverfügbarkeitsstandards, d. h. das Risiko, dass Daten durch Gefährdungslagen wie Wasserschäden, Blitzschlag, Stromausfall oder dem Ausfall einer Klimaanlage beeinträchtigt werden, ist durch Maßgaben für ein sicheres Rechenzentrum mit erhöhtem Schutzbedarf nach BSI Grundschutz sehr klein gehalten.

Backup

noris network erstellt nach Anforderung des Auftraggebers regelmäßige Backups der be-treffenden Systeme im Rahmen nach definiertem Backup-Verfahren und dazugehörigem Recovery-Prozess. Backups werden nach Anforderung des Auftraggebers in unterschiedlichen Brandschutzabschnitten durchgeführt. Die Backup-Medien verbleiben je nach Anforderung des Kunden im Backup-System an diesem anderen Standort, oder nach Anforderung des Kunden auch per Lagerung als Backup-Medium in einem Safe. Die Frequenz und Aufbewahrungsdauer des Backups kann der Auftraggeber – entsprechend dessen Erfordernissen – bei Bedarf individuell vorgeben.

8) Trennungsgebot

noris network führt eine Netzwerktrennung zur Trennung von Kundensetups, je nach Bedarf des Auftraggebers und nach Angemessenheit des angestrebten Schutzzwecks auch innerhalb von Kundensetups in verschiedenen Zonen (z. B. Produktions- und Testumgebung) durch, die ggf. durch individuelle Zugangsberechtigungen voneinander getrennt werden.

Anlage 2: Eingesetzte Unterauftragnehmer

Unterauftragnehmer	Tätigkeit
SpaceNet AG	Betreiber Rechenzentrum
Noris Networks AG	Betreiber Rechenzentrum
Entwickler, Wartungstechniker	Zur Implementierung von neuen Funktionen und zur Wartung der vorhandenen Funktionen setzt simple system externe Techniker ein. Die Techniker verarbeiten keine personenbezogenen Daten des Auftraggebers, ein Zugriff auf Auftraggeber-Daten kann jedoch nicht mit Sicherheit ausgeschlossen werden.