

Datenschutzhandbuch der NOVENTI HealthCare GmbH

Technisch-organisatorische Maßnahmen

1 Maßnahmen zu Gewährleistung der Vertraulichkeit

1.1 Zutrittskontrolle

Zutrittskontrolle	vorhanden
Ein unbefugter Zutritt ist zu verhindern, wobei der Begriff räumlich zu verstehen ist.	ja
Elektronische Zutrittscodekarten/ Transponder	☒
Zutrittsberechtigungskonzept	☒
Videoüberwachung am Produktionsstandort	☒
Alarmanlage	☒
Schlüsselbuch	☒
Besucherausweise	☒
Begleitung von Besucherzutritten durch eigene Mitarbeiter	☒
Protokoll der Besucher	☒
Empfang/Rezeption	☒
Gesonderter gesicherter Zutritt zum Rechenzentrum	☒
Aufbewahrung der Server in verschlossenen Räumen	☒
Scanner/Sorter in verschlossenen Räumen	☒
Produktionsdrucker in verschlossenen Räumen	☒

1.2 Zugangskontrolle

Zugangskontrolle	vorhanden
Das Eindringen Unbefugter in die DV-Systeme bzw. deren unbefugte Nutzung ist zu verhindern.	ja
Es gelten die Regelungen des zentralen IT-Dienstleisters der NOVENTI Health SE, insbesondere der ausgelagerte Rechenzentrums- und Serverbetrieb	☒
Zugang zu den zentralen Systemen nur für wenige Berechtigte	☒
Zugang von externen Arbeitsplätzen nur über VPN	☒
Schutz der zentralen Systeme durch mehrstufige Firewall mit vollständiger Abschirmung kritischer Bereiche	☒
Passwortsicherung von Bildschirmarbeitsplätzen	☒
Abgestufte und rollenbasierte Zugriffsberechtigungen in allen zentralen Systemen	☒
Password-Policy	☒
Prozess zur Rechtevergabe/-entzug für neue, wechselnde und ausscheidende Mitarbeiter	☒
Verpflichtung auf das Datengeheimnis nach DSGVO	☒
Prüfungs- und Freigabeverfahren bei Neuinstallationen	☒

1.3 Zugriffskontrolle

Zugriffskontrolle	vorhanden ja
Unerlaubte Tätigkeiten in DV-Systemen außerhalb eingeräumter Berechtigungen sind zu verhindern.	
Stringentes Berechtigungskonzept in allen zentralen Systemen	☒
Log-Files für Systemzugriff	☒
Trennung von Berechtigungsbewilligung (organisatorisch) und –vergabe (technisch)	☒
Regelmäßige Überprüfung von Berechtigungen	☒
Regelung zur Wiederherstellung aus Backups	☒
Werden entsprechende Sicherheitssysteme (Software/Hardware) eingesetzt?	
▪ Virens Scanner	☒
▪ Firewalls	☒
▪ SPAM-Filter	☒
Beschränkter Zugriff auf LogFiles (nur Log-Admin)	☒
Datenschutztonne/externer Aktenvernichter	☒

1.4 Auftragskontrolle

Auftragskontrolle	vorhanden ja
Es ist sicherzustellen, dass Daten die im Auftrag durch Dienstleister (Subauftragnehmer) verarbeitet werden, nur gemäß der Weisung des Auftragnehmers verarbeitet werden.	
Vertragsgestaltung gem. gesetzlichen Vorgaben (gem. DSGVO)	☒
Zentrale Erfassung vorhandener Dienstleister (einheitliches Vertragsmanagement)	☒
Schriftliche Weisung an den Auftragnehmer	☒

1.5 Trennungskontrolle

Trennungskontrolle	vorhanden ja
Daten, die zu unterschiedlichen Zwecken erhoben wurden, sind auch getrennt zu verarbeiten.	
Logische Datentrennung (z. B. auf Basis von Kundennummern)	☒
Trennung von Entwicklungs-, Test-, und Produktivsystemen	☒
Mandantenfähigkeit relevanter Anwendungen (z.B. FiBu)	☒
Festlegung von Datenbankrechten	☒
Steuerung über Berechtigungskonzept	☒

2 Maßnahmen zur Gewährleistung der Integrität

2.1 Weitergabekontrolle

Weitergabekontrolle Aspekte der Weitergabe (Übermittlung) personenbezogener Daten sind zu regeln: Elektronische Übertragung, Datentransport, sowie deren Kontrolle.	vorhanden ja
Datenübertragung gemäß TA-3/TA-4 nach SGB V, SGB XI	☒
Einsatz von VPN	☒
Bereitstellung über verschlüsselte Verbindungen (https, sftp)	☒
Übertragung zwischen den Standorten über MPLS-Leitung ohne Verbindung zum Internet	☒
Verschlüsselung der Festplatten mobiler Geräte	☒
Dateiverschlüsselung bei Übertragung über unsichere Kanäle (z.B. Email)	☒
Kontrollierte Vernichtung von Daten	☒
Verpackungs- und Versandvorschriften	☒
Vollständigkeitsprüfung	☒
Übersicht regelmäßiger Abruf- und Übermittlungsvorgänge	☒

2.2 Eingabekontrolle

Eingabekontrolle Die Nachvollziehbarkeit bzw. Dokumentation der Datenverwaltung und -pflege ist zu gewährleisten.	vorhanden ja
Protokollierung der Eingabe, Änderung und Löschung von Daten, wo organisatorisch sinnvoll	☒
Protokollauswertungssysteme	☒
Automatisierte Datenerfassung durch Scanner und „on-premise“-Erkennungssoftware	☒
Annahme verschlüsselter Datenlieferungen	☒
Manuelle Erfassung mit entsprechender Prüfung der Berechtigung	☒
Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts	☒

3 Maßnahmen zur Gewährleistung der Verfügbarkeit und Belastbarkeit

3.1 Verfügbarkeit und Belastbarkeit

Die Daten sind gegen zufällige Zerstörung oder Verlust zu schützen. Systeme müssen die Fähigkeit besitzen mit risikobedingten Veränderungen umgehen zu können und eine Toleranz und Ausgleichsfähigkeit gegenüber Störungen aufweisen.	vorhanden ja
Es gelten die Regelungen des zentralen IT-Dienstleisters der NOVENTI Health SE, insbesondere der ausgelagerte Rechenzentrums- und Serverbetrieb	☒
Feuer- und Rauchmeldeanlagen	☒
Wasserlose Brandbekämpfungssysteme in Scanner- und Druckerräumen am Produktionsstandort	☒
Getrennte Scannerräume in verschiedenen Brandabschnitten am Produktionsstandort	☒
Technisches Monitoring aller relevanten Systeme, Alerting	☒
(Mindestens) doppelte Auslegung aller relevanten Komponenten (Hard- und Software)	☒
Risikoabschätzung unter direkter Beteiligung des Top-Management	☒

4 Maßnahmen zur regelmäßigen Überprüfung, Bewertung und Evaluierung

4.1 Kontrollverfahren

Kontrollverfahren Ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der Datensicherheitsmaßnahmen ist zu implementieren.	vorhanden ja
Interne Verfahrensverzeichnisse werden mind. jährlich aktualisiert	☒
Meldung neuer/veränderter Datenverarbeitungsverfahren an den Datenschutzbeauftragten	☒
Es werden datenschutzfreundliche Voreinstellungen gewählt	☒
Getroffene Sicherheitsmaßnahmen werden einer regelmäßigen internen Kontrolle unterzogen	☒
Bei negativem Verlauf der zuvor genannten Überprüfung werden die Sicherheitsmaßnahmen risikobezogen angepasst, erneuert und umgesetzt	☒
Es besteht ein Prozess zur Vorbereitung auf Sicherheitsverletzungen (Angriffen) und Systemstörungen sowie zur Identifizierung, Eingrenzung, Beseitigung und Erholung von selbigen (Incident-Response-Prozess)	☒

Unterauftragnehmer

Im Zusammenhang mit der Erbringung der vertraglichen Leistungen beauftragt der Auftragnehmer folgende Subunternehmer:

Unterauftragnehmer	Aufgabenfeld
NOVENTI Health SE Tomannweg 6, 81673 München	Rechenzentrumsbetreiber, CD-Produktion
Kodak Alaris Germany GmbH Hedelfinger Straße 60, 70327 Stuttgart	Wartung und Reparatur Scanner
Swiss Post Solutions AG Integrated Document Solutions AG (IDS) Niederlassung Villingen Wilhelm-Binder-Str. 19, D-78048 Villingen-Schwenningen	Programmierung Erkennung
Riello UPS GmbH Wilhelm-Bergner-Straße 9b, 21509 Glinde	Wartung Server
Zellner Recycling GmbH Budapester Straße 15, 93055 Regensburg	Akten-Vernichtung
Heinz Umweltservice GmbH Donau-Gewerbepark 27, 94486 Osterhofen	Akten-Vernichtung
Rhenus Data Office GmbH Rupert-Bodner-Straße 25, 81245 München	Akten-Vernichtung
Veolia Umweltservice Ost GmbH & Co.KG Rosenstraße 99-101, 01159 Dresden	Akten-Vernichtung
Reisswolf Akten- und Datenvernichtung GmbH Ziegeleiweg 12, 19057 Schwerin	Akten-Vernichtung
Taxiunternehmen Brigitte Peschke Schweriner Str. 42, 19073 Wittenförden	Rezeptabholung
Regiomed Systemlogistik GmbH Holzhauser Str. 158A, 13509 Berlin	Rezeptabholung
Canon Deutschland GmbH Siemensallee 2, 85586 Poing	Service Druckermanagement
SET Krauß & Partner GmbH Bäckergasse 13, 82335 Berg	Programmierdienstleistungen
Brillion GmbH Deutenbergstraße 7, 82327 Tutzing	Programmierdienstleistungen
RaPi GmbH Ahornstraße 11, 84030 Ergolding	Programmierdienstleistungen
KRONSOFT Development SRL Saturn Straße Nr. 51, 505600 Brasov, Rumänien	Programmierdienstleistungen
Retarus GmbH Aschauer Straße 30, 81549 München	Technischer Dienstleister im Rahmen Direktmarketing, azh KVCheck und azh TiM
Stempel-Kroul GmbH Friedenstr. 18, 81671 München	Druck- und Direktmarketingleistungen
Computershare GmbH Hansastr. 15, 80686 München	Druck und Versand Mahnungen
Lipako GmbH Wismarsche Str. 321, 19055 Schwerin	Druckerei

KuvertierService Richter GmbH Gaußring 28, 86415 Mering	Kuvertieren
MediaKom GmbH & Co. KG Kampenwandstr. 81, 83229 Aschau	Versanddienstleistungen
bgm Websolutions GmbH und Co KG Prof.-Messerschmitt-Str. 1, 85579 Biberach	Agenturleistungen, Unternehmenswebsites und Typo3
Söllner Communications AG Rosenkavalierplatz 5, 81925 München	Agenturleistungen
COBUS Marktforschung Leopoldstr. 1, 76133 Karlsruhe	Dienstleistungen im Bereich der Marktforschung
KCC GmbH Hansestraße 83, 51149 Köln	Call Center-Dienstleistungen