NOVENTI myYOLO

Papierloser Rehasport.

Datenschutzhandbuch

NOVENTI myYOLO

| V3.0.|

www.azh-myYOLO.de

NOVENTI Health Care GmbH
Einsteinring 41-43 | 85609 Aschheim bei München
Tel. (089) 943 969 700

Datenschutzhandbuch

Technisch-organisatorische Maßnahmen

1 Maßnahmen zu Gewährleistung der Vertraulichkeit

1.1 Zutrittskontrolle

Zutrittskontrolle Ein unbefugter Zutritt ist zu verhindern, wobei der Begriff räumlich zu verstehen ist.	**vorhanden ja**
Elektronische Zutrittscodekarten/ Transponder	☒
Zutrittsberechtigungskonzept	☒
Alarmanlage	☒
Schlüsselbuch	☒
Besucherausweise	☒
Begleitung von Besucherzutritten durch eigene Mitarbeiter	☒
Protokoll der Besucher	☒
Empfang/Rezeption	☒
Aufbewahrung der Server in verschlossenen Räumen	☒

1.2 Zugangskontrolle

Zugangskontrolle Das Eindringen Unbefugter in die DV-Systeme bzw. deren unbefugte Nutzung ist zu verhindern.	**vorhanden 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 Unerlaubte Tätigkeiten in DV-Systemen außerhalb eingeräumter Berechtigungen sind zu verhindern.	**vorhanden ja**
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?	
▪ Virenscanner	☒
▪ Firewalls	☒
▪ SPAM-Filter	☒
Beschränkter Zugriff auf LogFiles (nur Log-Admin)	☒
Datenschutztonne/externer Aktenvernichter	☒

1.4 Auftragskontrolle

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

1.5 Trennungskontrolle

Trennungskontrolle Daten, die zu unterschiedlichen Zwecken erhoben wurden, sind auch getrennt zu verarbeiten.	**vorhanden ja**
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**
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	☒
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	☒
Technisches Monitoring aller relevanten Systeme, Alerting	☒
(Mindestens) doppelte Auslegung aller relevanten Komponenten (Hard- und Software)	☒

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)	☒