Technisch organisatorische Maßnahmen INNEO Cloud Services

(INNEO Cloud TOMs)

öffentlich – zur Weitergabe an Kunden

Version 3.2

Geltungsbereich

Dieses Dokument gilt für alle Standorte und Unternehmensbereiche, die im Anwendungsbereich des ISMS liegen.

Zielgruppen

Diese Richtlinie ist für folgende Zielgruppen gültig:

Zielgruppe	verpflichtend	informativ
Mitarbeiter des Unternehmens	x	
Kunden		x
Wirtschaftsprüfer		x
Datenschutz	x	
Externe Dienstleister	x	

INNEO Solutions GmbH
IT-Campus 1
73479 Ellwangen

www.inneo.com
inneo@inneo.com
kostenlose* Infoline 0800/7263742 (*innerhalb DE)

Telefon +49 (0) 7961 890-0
Telefax +49 (0) 7961 890-177

Revisionsverfolgung

Revision	Datum	Autor	Kommentar
1.0	02.03.2018	INNEO	Erstellung Version 1
1.1	7.05.2018	Peter Behnisch	Überarbeitung
2.0	20.12.2019	Peter Behnisch	Überarbeitung
3.0	02.11.2023	Sophia Völkl	Überarbeitung (Click&Acceppt)
3.1	23.01.2024	Julian Neumann	Anpassungen
3.2	30.01.2024	Peter Behnisch	Freigegebene Version

Inhaltsverzeichnis

Ziel und Zweck

Im Rahmen des INNEO Datenschutzmanagementsystems sind die technisch, organisatorischen Maßnahmen, die allgemein im Zusammenhang mit dem INNEO Cloud Services Rechenzentrum für die Verarbeitung von personenbezogenen Daten getroffen werden, definiert. Sie werden zusammen-gefasst als „INNEO Cloud TOMs“ bezeichnet.

Geltungsbereich

Dieses Dokument gilt für alle Standorte und Unternehmensbereiche, die im Anwendungsbereich des ISMS liegen.
Der Scope umfasst die Entwicklung den Betrieb und von Cloud Services und SaaS-Lösungen. Und damit alle aktuell bei INNEO verfügbaren Cloud Services.

ZERTIFIKAT ◆ CERTIFICATE ◆ 認證證書 ◆ СЕРТИФИКАТ ◆ CERTIFICADO ◆ CERTIFICAT

TÜV SÜD Management Service

ZERTIFIKAT

Zertifikat-Registrier-Nr.: **12 310 66508 TMS** / Auftrags-Nr.: **70003032**

Die Zertifizierungsstelle
der TÜV SÜD Management Service GmbH
bescheinigt, dass die Organisation

INNEO That's IT.

INNEO Solutions GmbH
IT-Campus 1
73479 Ellwangen
Deutschland

für den Geltungsbereich

Entwicklung und Betrieb von
Cloud Services und SaaS Lösungen

ein Informationssicherheitsmanagementsystem gemäß
„Erklärung zur Anwendbarkeit“ eingeführt hat und anwendet.
Durch ein Audit wurde der Nachweis erbracht,
dass die Forderungen der

DIN EN ISO/IEC 27001:2017

erfüllt sind.

Dieses Zertifikat ist gültig vom **09.10.2023** bis **31.10.2025**.
Version der Erklärung zur Anwendbarkeit: **1.0 vom 24.05.2023**

Fred Wenke
Leiter der Zertifizierungsstelle
München, 10.10.2023

IAF DAkkS

TÜV SÜD Management Service GmbH • Zertifizierungsstelle • Ridlerstrasse 57 • 80339 München • Germany
www.tuvsud.com/de-certificate-validity-check

TÜV®

Abb. 1: INNEO ISO 27001:2017 Zertifikat vom 10.10.2023

Pseudonymisierung und Verschlüsselung personenbezogener Daten (Art. 32 Abs. 1 lit. a DS-GVO)

Die Verarbeitung personenbezogener Daten erfolgt in einer Weise, dass die Daten ohne Hinzuzie-hung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können. Diese zusätzlichen Informationen werden gesondert aufbewahrt und unterliegen ebenfalls den technischen und organisatorischen Maßnahmen.

Eine Pseudonymisierung erfolgt an den Stellen, an denen dies datenverarbeitungstechnisch möglich und sinnvoll ist.

- Anonymisierung von Nutzungsdaten
- Verschlüsselung von Passwort- und Benutzerdaten
- Zugriff über das Internet über durch Verschlüsselung gesicherte Virtual Private Network (VPN) Tunnel oder andere verschlüsselte Verbindungen möglich
- Einsatz von Verschlüsselungsverfahren nach dem Stand der Technik
- Zusätzlich die Verwendung von Remote- und Desktopübertragungssystemen mit integrierter Verschlüsselungstechnologie
- Bereitstellung von webbasierten Inhalten ausschließlich über verschlüsselte HTTPS-Kommunikation

Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme (Art. 32 Abs. 1 lit. b DS-GVO) Rechenzentrum

- Zugang nur nach Anmeldung an Pforte möglich
- Abholung und Begleitung von Besuchern, regelmäßige Kontrollgänge sowie umfassende Protokollierung der Zutritte und Abgänge
- Verwendung eines elektronischen Schließsystems
- Einbruchsschutz in Anlehnung an EN 1627, WK II
- Einbruchmeldeanlage mit Aufschaltung auf Sicherheitsdienst
- Videoüberwachung im Flur und Eingangsbereich
- Zutrittskontrolle durch Chipkarten bei sämtlichen Türen des Rechenzentrums
- Klimatisierung der RZ-Räume durch Deckenkühlgeräte
- Klimatisierung jedes einzelnen Rackschrankes durch LCP Einheiten (Liquid Cooling Packa-ge)
- Feuerwiderstandswert F90 nach DIN4102 (EN1363), ECBS-Zertifizierung R60D, typgeprüft nach EN1047-2
- Wasser/Gasschutz in Ableitung aus dem Feuerwiderstandstest und dem Stoßtest nach EN 1047-2
- RAS – Brandfrühersterkennung mit Novec Gas Löschung (Schranklöschung)
- BMA – Brandmeldeanlage (über Rauchmelder)
- Rauchgasdichtigkeit nach EN18095
- Wasserwarnanlage bei Wasserleckagen
- Überwachung sämtlicher Temperaturen der Räume

- Zur Überbrückung von Stromunterbrechungen- bzw. Schwankungen ist das RZ mit einer USV ausgestattet, die 15 Minuten Vollast-Betrieb ermöglicht. Die Netzersatzversorgung er-folgt über BHKW Turbinen aus dem Wärmewerk, die nach 7 Minuten bereit zur Übernahme der Netzlast sind. Als Redundanz hierzu dient ein Diesel Notstromaggregat das nach spätes-tens 8 Minuten ebenfalls die Netzlast übernehmen kann.
- Jeder Rackschrank besitzt ein PSM - Aktives Power System Modul
- 24 x 7 Rufbereitschaft SI Stadtwerke Aalen

Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme (Art. 32 Abs. 1 lit. b DS-GVO) INNEO Cloud Services

- Vollständige system- und netzwerktechnische Trennung der einzelnen, auf den Systemen betreuten Mandanten
- Dokumentierte granulare Zuordnung von Benutzerrechten
- Authentifizierung erfolgt über Benutzername und Passwort, und wird mitprotokolliert
- Zusätzlich ist eine Multi-Faktor-Authentifizierung mittels TOTP-Verfahren möglich (kunden-individuell zu vereinbaren)
- Betrieb eines SIEM-Systems mit 6-monatiger Speicherung der Authentifizierungs- und Be-wegungsdaten im Netzwerk
- Einsatz einer eigenen Anti-Viren Software, bzw. eines vom Kunden gewünschten Produktes
- Zero-Trust-Architektur, Einsatz von Reverse-Proxys und Mikrosegmentierung der Netzwerke
- Einsatz von Routern zur Bildung von einzelnen Netzwerksegmenten
- Service-spezifische DoS-Protection
- Abgestuftes Berechtigungskonzept mit AD Gruppen und Organisationseinheiten
- Verwaltung der Rechte erfolgt ausschließlich durch benannte Systemadministratoren
- Passwortvergabe folgt einer Passwortrichtlinie
- Passwörter und Credentials werden in einem Passwort-Safe verwahrt
- Aktenvernichter und Dienstleister zur Entsorgung von Akten und Datenträgern
- Versionierung und Protokollierung von Änderungen der Systemkonfiguration im ISMS
- Strikte physikalische und virtuelle Trennung von Produktiv- und Testsystemen
- Security by Design, d.h. Einsatz technischer Redundanz zur Absicherung des Betriebs
- Skalierbare Server- und Speicher-Infrastruktur
- Hochverfügbarkeit durch Load-Balancing kritischer Dienste/Services
- Redundante Internetanbindung über 2 Provider, mit getrennter Trassenführung von außen ins Rechenzentrum
- Definition von Plausibilitätskontrollen zur Eingabe, Änderung und Löschung
- Sichere Ablage und fristgerechte Löschung von Protokollen

Wiederherstellung (Art. 32 Abs. 1 lit. c DS-GVO)

- Notfallplan und Betriebsanweisungen redundant zur Verfügung
- ICERT-Team (INNEO Cloud Emergency Response Team) benannt und Alarmierungsproce-dere definiert
- Hohe Verfügbarkeit durch den Einsatz von Virtualisierungstechnologie
- High-Availability by Design durch ein Konzept mit:
    - RAID abgesicherten Speichersystemen
    - Redundanz aller wesentlichen Komponenten von Server, Speicher, Netzwerk etc. (Festplatten, Netzteile…)
    - Redundante Serverapplikationsarchitekturen
    - Redundante Netzwerkverbindungen
    - Clusterung der wichtigsten Systeme
    - Systemverfügbarkeit mit Kennzahlenüberwachung durch den Einsatz eines ISMS
    - Einsatz von hochverfügbarer Speichertechnologie
- Mehrschichtiges Backup-Konzept nach der 3-2-1-Regel. Produktivsystem und erstes Backup innerhalb des Rechenzentrum in zwei getrennten Lampertz-Zellen (Brandabschnitte).
    - Die Backups werden verschlüsselt und in unmanipulierbarer Form (Retention Lock) auf den Systemen von INNEO abgelegt.
    - In regelmäßigen Abständen werden die Backups auf Ihre Wiederverwendbarkeit ge-testet.
    - Eine weitere, verschlüsselte Kopie der Sicherung wird zusätzlich an einem sicheren Speicherort, nicht im RZ der Stadtwerke Aalen, abgelegt. (Geo-redundantes Backup mit sogenanntem „Air-Gap“)

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

- Überwachung der kompletten Rechenzentrum-Infrastruktur mit Hilfe einer Störmeldeanlage mit redundanten Meldewegen (ISDN u. GSM) durch den Bereitschaftsdienst der SWA (7 Ta-ge je 24 Stunden)
- Kontinuierliches, automatisiertes Monitoring der Cloud-Infrastruktur und der INNEO Cloud Services durch den INNEO Managed Service
    - Diverse IT-spezifische Key Performance Indicator (KPI)
    - Diverse Applikations- bzw. Cloud Service spezifische KPI´s
    - Benachrichtigung der Systemadministratoren bei Unregelmäßigkeiten
    - Direkte Integration in das Ticketsystem
- Automatisiertes Backupmonitoring
- Automatisierte Validierung der Wiederherstellbarkeit von Backups