Technische und organisatorische Maßnahmen (TOM) zum Schutz der Daten des Auftraggebers

Inhaltsverzeichnis

Letze Änderung durch: Stefan Krüger	Letzter Export am: 05.09.2025, (12:14:32)

1. Organisatorische Maßnahmen

AddOns Global > Datenschutz > TOM

Bezeichnung
Beschreibung (Ziel)
01 Organisatorische Massnahmen
Die Umsetzung der gesetzlichen Pflichten (DSGVO) erfolgt durch - Identifizierung der Verfahren, in denen PbD nach Art. 4 DSGVO verarbeitet werden - Führung eines Verfahrensverzeichnisses - Berufung deines DSB - Vereinbarung über Auftragsverarbeitung mit jedem AG - Einweisung jedes MA in die Verfahrensanweisung für den Datenschutz und abgeleitete Arbeitsanweisungen; Nachweisführung über die Kenntnisnahme - Verpflichtung zum Datenschutz für jeden Mitarbeiter; Nachweisführung durch Unterschrift, Verankerung im Anstellungsvertrag - Einführung eines Auditprozesses für die Überprüfung und Korrektur der Datenschutzmaßnahmen

AddOns Mandant > Datenschutz > TOM Lösungen

Beschreibung	
Referenz auf Globale Daten	**Anwendungsbereich**
Beschreibung	
01 Organisatorische Maßnahmen	
1	
Für personenbezogene Daten gelten gesetzliche Pflichten, denen wir in folgender Weise nachkommen: - Wir haben die Verfahren identifiziert, die personenbezogene Daten nach Art. 4 DSGVO verarbeiten. - Wir führen ein Verarbeitungsverzeichnis über diese Verfahren. - Wir haben einen Datenschutzbeauftragten berufen. - Wir haben den Umgang mit pbD und den Datenschutz in die betriebliche „Verfahrensanweisung für die Datenverwaltung“ aufgenommen. Weitere Anweisungen für Prozesse mit Bezug zum Datenschutz für Auftraggeber Daten sind - das „Betriebshandbuch für das Rechenzentrum“, der „Wartungsplan für das Rechenzentrum“, - die „Checkliste für neue Mitarbeiter“ und „Checkliste für ausscheidende Mitarbeiter“ und weitere. - Jeder Mitarbeiter erhält eine Einweisung in die Verfahrensanweisung für den Datenschutz und abgeleitete Arbeitsanweisungen. Über die Einweisung wird ein Nachweis geführt. - Jeder Mitarbeiter muss die betriebliche „Verpflichtung zum Datenschutz“ unterschreiben. Die Einhaltung der betrieblichen Anweisungen zum Umgang mit Auftraggeberdaten und betrieblichen Daten	

ist im Anstellungsvertrag vereinbart.
-Für die Überprüfung und Korrektur der Datenschutzmaßnahmen haben wir einen internen Audit-Prozess eingeführt.

Freigabe / Unterschrift Geschäftsführung : 

Bernd Scheller (5. September 2025 12:29:52 GMT+2)

Letze Änderung durch: Stefan Krüger	Letzter Export am: 05.09.2025, (12:14:33)

2. Grundsätze

AddOns Global > Datenschutz > TOM

Bezeichnung
Beschreibung (Ziel)
02 Grundsätze für IT-Infrastruktur, Anwendungen, und Serviceleistungen
Für die verschiedenen Bereiche der IT-Infrastruktur, der IT-Anwendungen und der Datenhaltung wurden Grundsätze formuliert, nach denen das IT-Sicherheitsmanagement den Datenschutz gestaltet und umgesetzt wird: .. für das eigene Rechenzentrum .. für die Nutzung externer Cloud-Services (Outsourcing: Netik RZ, Microsoft Cloud, Citrix Cloud u.a.) .. für die eigenen lokalen Ressourcen (Unternehmensstandorte, Mobile IT, Home Office usw.) .. für die Leistungen externer Dienstleister

AddOns Mandant > Datenschutz > TOM Lösungen

Beschreibung	
Referenz auf Globale Daten	**Anwendungsbereich**
Beschreibung	
02.01 Grundsätze - Netik RZ	
2	Netik Rechenzentrum Berlin 1
Unsere zentralen IT-Ressourcen sind überwiegend im Netik Rechenzentrum („RZ“) zentralisiert. Zu den zentralen IT-Ressourcen zählen: - sämtliche Server mit ihren Anwendungen und Services - sämtliche Datenspeicher - Firewall, Router und Netscaler für den gesicherten Zugriff auf die Ressourcen des RZ. - sämtliche Verbindungen für den gesicherten Zugriff auf die zentralen Systeme, Anwendungen und Daten unserer Auftraggeber für die Erbringung von Serviceleistungen - IT-Sicherheitslösungen auf dem aktuellen Stand der Technik. Das RZ wird ausschließlich durch uns administriert. Das Netik-RZ befindet sich in den Räumen eines professionellen Co-Location Providers in Deutschland. Der Provider hat keinen Zugriff auf die IT-Ressourcen des Netik-RZ. Die IT-Ressourcen im RZ werden laufend auf dem aktuellen Stand der Technik gehalten	
02.02 Grundsätze - Microsoft Cloud	

2	Microsoft Cloud
Weitere zentrale IT-Ressourcen werden aus der Microsoft Cloud bezogen, und zwar ausschließlich von Standorten in Ländern der Europäischen Union („Europäische Cloud“) bzw. auf besondere Anforderung in Deutschland („Microsoft Cloud Deutschland“). Microsoft sichert seinerseits die Einhaltung der Europäischen Gesetzgebung, insbesondere der DSGVO zu: siehe Microsoft Trust Center	
02.03 Grundsätze - Citrix Cloud	
2	Citrix Cloud
Wir beziehen für uns, und falls vereinbart für Kunden, Services aus der Citrix Cloud (Cloud Software Group) . Alle Daten liegen innerhalb der Europäischen Union, solange der Kunde keine anderen Einstellungen vornimmt.	
02.04 Grundsätze - eigene Standorte	
2	Eigene Standorte (lokale IT-Ressourcen)
Als lokale IT-Ressourcen sind bei uns (Dr. Netik & Partner GmbH) zugelassen: - Verwaltete stationäre und mobile Clients (Thin Client, PC/Notebook, MAC, Smartphone/Tablet) mit Client-Anwendungen - Private Geräte dürfen bei uns genutzt werden, wenn sie durch die Administration verwaltet werden - Telefonanlagen, wobei der CTI-Server im RZ steht	
02.05 Grundsätze - Dienstleistung	
2	Netik als externer Dienstleister für Kunden
Unsere Mitarbeiter sind im Unternehmen Dr. Netik & Partner beschäftigt. Leistungen im Rahmen von Serviceverträgen der Netik Online GmbH werden durch die Dr. Netik & Partner GmbH erbracht. Externe Mitarbeiter und Subunternehmer werden durch entsprechende Vereinbarungen genauso wie eigene Mitarbeiter auf den Datenschutz verpflichtet.	
02.06 Grundsätze Sharefile Cloud	
Wir beziehen für uns, und falls vereinbart für Kunden, Services aus der Sharefile Cloud. Die Metadaten der Kundeninstanzen liegen auf Speichern in der EU. Damit gilt durchgängig EU Recht. Für Daten, die unsere Kunden in Sharefile speichern, liegt der Cloud Speicher je nach Vereinbarung/Lizenz im Netik Rechenzentrum oder in der Sharefile Cloud.	

Letze Änderung durch: Stefan Krüger	Letzter Export am: 05.09.2025, (12:14:33)

3. Zutrittskontrolle

AddOns Global > Datenschutz > TOM

Bezeichnung
Beschreibung (Ziel)
03 Maßnahmen der Zutrittskontrolle
Die Maßnahmen der Zutrittskontrolle verhindern, dass Unbefugte räumlich Zutritt zu den IT-Ressourcen erhalten, mit denen Auftraggeberdaten gespeichert oder verarbeitet werden.

AddOns Mandant > Datenschutz > TOM Lösungen

Beschreibung	
Referenz auf Globale Daten	**Anwendungsbereich**
Beschreibung	
03.01 Zutrittskontrolle - Netik RZ	
3	Netik Rechenzentrum Berlin 1
Die Maßnahmen der Zutrittskontrolle verhindern, dass Unbefugte räumlich Zutritt zu den IT-Ressourcen erhalten, mit denen Auftraggeber Daten gespeichert oder verarbeitet werden. Die Zutrittskontrolle zum Netik Rechenzentrum ist im Vertrag mit dem Co-Location Provider geregelt. Es handelt sich um professionelle Zutrittskontrollsysteme auf dem aktuellen Stand der Technik. 1. Tür zum Rechenzentrum = geschützter Zugang zum Raum 2. Tür zum Cage (Käfig) = geschützter Zugang zum Netik-eigenen Bereich Wir haben eine Gruppe von Mitarbeitern benannt, die Zugang und administrativen Zugriff auf das Netik Rechenzentrum hat. Die persönlichen Chipkarten für den Zugang unserer benannten Mitarbeiter sind mit Passfoto und biometrischen Merkmalen gekoppelt. Im Backup RZ (Netik2) Zugang mit separater Chipkarte und An.- und Abmeldung beim Provider Zugang zum Schrank mit Schlüssel	
03.02 Zutrittskontrolle - eigene Standorte	

3	Eigene Standorte (lokale IT-Ressourcen)

Die Maßnahmen der Zutrittskontrolle verhindern, dass Unbefugte räumlich Zutritt zu den IT-Ressourcen erhalten, mit denen Auftraggeber Daten gespeichert oder verarbeitet werden.

Unsere eigenen Standorte

Die Geschäftsräume in Neubrandenburg und Güstrow sind mit Schließanlagen, Einbruchmeldeanlagen ausgestattet. Die Alarmverfolgung sowie die Aufrechterhaltung der Funktion ist in Verträgen mit Fachfirmen geregelt.

Unsere eigenen Mitarbeiter haben uneingeschränkten Zutritt zu den Geschäftsräumen.
Mitarbeiter in Gruppe:
Angestellte uneingeschränkt
Azubis, Praktikanten eingeschränkt auf Geschäftszeiten.
Reinigungskräfte zu festgelegten Zeiten unbeaufsichtigt.

Alle weiteren Mitarbeiter und Subunternehmer können die Geschäftsräume nur in den Betriebszeiten in Anwesenheit unserer Mitarbeiter betreten.

03.03 Zutrittskontrolle als Dienstleister bei Kunden

3	Netik als externer Dienstleister für Kunden

Für IT-Ressourcen am Standort des Auftraggebers liegt die Verantwortung für die Zutrittskontrolle beim Auftraggeber. Unsere Mitarbeiter werden vom Auftraggeber eingewiesen und haben die festgelegten Zutrittskontrollmaßnahmen einzuhalten.

Letze Änderung durch: Stefan Krüger	Letzter Export am: 05.09.2025, (12:14:33)

4. Zugangskontrolle

AddOns Global > Datenschutz > TOM

Bezeichnung
Beschreibung (Ziel)
04 Maßnahmen der Zugangskontrolle
Die Maßnahmen der Zugangskontrolle verhindern, dass Unbefugte Zugang zu den IT-Ressourcen erhalten, mit denen Auftraggeberdaten gespeichert oder verarbeitet werden.

AddOns Mandant > Datenschutz > TOM Lösungen

Beschreibung	
Referenz auf Globale Daten	**Anwendungsbereich**
Beschreibung	
04.01 Zugangskontrolle - Netik RZ	
4	Netik Rechenzentrum Berlin 1
Das Netik Rechenzentrum ist durch ein mehrstufiges Zugangskontrollsystem gesichert. Der Zugang aus der IT-Umgebung eines Netik- oder Kundenstandorts erfolgt über eine eingeschränkte Site-to-Site VPN-Verbindung zwischen Standort und Rechenzentrum. Somit hat jeder Kunde (auch Netik) nur Zugriff auf seine freigegebenen Ressourcen. Der Zugang erfolgt für die Dr. Netik & Partner GmbH ausschließlich über eine Multifaktor Authentifizierung. Der mobile Zugang (Mobil, Home Office) über das Netscaler Gateway ist für alle Rechenzentrums Kunden nur mit zusätzlicher personalisierter Multifaktor-Authentifizierung möglich. Die Verbindung ist verschlüsselt. Ein- und ausgehende Internetverbindungen sind mit einer Firewall auf dem aktuellen Stand der Technik gesichert. Das RZ 2 (Backup RZ) ist ausschließlich nur über das RZ1 erreichbar.	
04.02 Zugangskontolle als Dienstleister für Kunden	
4	Netik als externer Dienstleister für Kunden
Für IT-Ressourcen am Standort des Auftraggebers liegt die Verantwortung für die Zugangskontrolle beim Auftraggeber. Unsere Mitarbeiter werden vom Auftraggeber eingewiesen und haben die festgelegten Zugangskontrollmaßnahmen einzuhalten.	

Letze Änderung durch: Stefan Krüger	Letzter Export am: 05.09.2025, (12:14:33)

5. Zugriffskontrolle

AddOns Global > Datenschutz > TOM

Bezeichnung
Beschreibung (Ziel)
05 Zugriffskontrolle
Die Maßnahmen der Zugriffskontrolle sichern, dass die zur Benutzung von IT-Ressourcen Berechtigten ausschließlich auf Inhalte zugreifen können, für die sie entsprechende Berechtigungen besitzen, und dass Auftraggeberdaten bei der Verarbeitung und Nutzung nicht unbefugt kopiert, verändert oder gelöscht werden können.

AddOns Mandant > Datenschutz > TOM Lösungen

Beschreibung	
Referenz auf Globale Daten	**Anwendungsbereich**
Beschreibung	
05.01 Zugriffskontrolle - Eigene IT-Umgebung	
5	Eigene Standorte (lokale IT-Ressourcen)
Die Zugriffssteuerung wird im Netik Rechenzentrum verwaltet. Es werden eindeutige digitale Identitäten für jeden Benutzer geführt. Jeder Benutzer arbeitet mit seinem persönlichen Windows Domänenkonto. Der Zugriff auf die IT-Ressourcen des Rechenzentrums wird durch Windows Domänenauthentifizierung mittels Microsoft Active Directory verwaltet und gesteuert. Soweit möglich, beziehen alle IT-Anwendungen ihre Anmeldedaten und Berechtigungen aus dem Microsoft Active Directory (z.B. Exchange, MS SQL, CTI, Firewall, Sharepoint u.a.). Andere Anwendungen nutzen eine eigene Benutzerverwaltung und -authentifizierung. Benutzerkonten, Administratorkonten, Dienstbenutzerkonten werden konsequent getrennt. Automatisierte Anwendungen laufen mit dedizierten Dienstkonten. Berechtigungen und Richtlinien werden gruppenbasiert administriert und gesteuert. Es werden restriktive Passwortrichtlinien laut BSI Empfehlung durchgesetzt. Die IT-Verwaltung erfolgt durch eine benannte, speziell eingewiesene Gruppe von Administratoren, die grundsätzlich Mitarbeiter in unserem Unternehmen sind. Jeder Administrator hat ein eigenes	

Administratorkonto für die administrativen Aufgaben. Das primäre Administratorkonto hat ein separates Kennwort, dass im Unternehmen nicht veröffentlicht wird, und das nur für Notfälle genutzt werden darf. Der Zugriff auf Administratorkonten wird protokolliert.

05.02 Zugriffskontrolle für Auftraggeber im Netik RZ	
5	Netik Rechenzentrum Berlin 1

Auftraggeber erhalten im Rechenzentrum einen eigenen Bereich in einer geteilten Active Directory Umgebung, welche strikt durch Sicherheitsmaßnahmen von anderen Kunden getrennt ist. Zusätzlich sind die Ressourcen der Kunden (auch Dr. Netik & Partner GmbH) durch Netzwerksegmentierung und eigene virtuelle Server voneinander getrennt. Die Regeln für den Zugriff von Benutzern eines Auftraggebers auf das Rechenzentrum sind die gleichen wie in Punkt 5.01 beschrieben

Das Berechtigungskonzept auf Kundeneigene Ressourcen wird mit jeweiligem Auftraggeber abgestimmt.

05.03 Zugriffskontrolle als Dienstleistung für den Kunden	
5	Netik als externer Dienstleister für Kunden

Für IT-Ressourcen am Standort des Auftraggebers liegt die Verantwortung für die Zugriffskontrolle beim Auftraggeber. Unsere Mitarbeiter werden vom Auftraggeber eingewiesen und haben die festgelegten Zugriffskontrollmaßnahmen einzuhalten.

Ein Zugriff auf die IT-Ressourcen des Auftraggebers ohne Information und Freigabe erfolgt nur bei direkter Vereinbarung mit dem Kunden durch einen Wartungsvertrag.

Unsere Mitarbeiter arbeiten nicht mit Benutzerkonten des Auftraggebers. Für Serviceleistungen steht uns ein Servicekonto in der Domäne des Auftraggebers zur Verfügung. Der Administrator (des Auftraggebers) kann das Servicekonto jederzeit sperren.

Der Zugriff unserer Administratoren auf IT-Ressourcen des Auftraggebers erfolgt ausschließlich über das Netik RZ. Die Administratoren müssen sich zunächst im Netik RZ authentifizieren bevor über eine gesicherte Verbindung auf die Kundenumgebung zugegriffen werden kann.

Der Auftraggeber kann unserem Mitarbeiter den überwachten Zugriff auf seine IT-Ressourcen mittels Fernwartungstool erlauben bzw. vorschreiben.

05.04 Zugriffskontrolle - Public Cloud	

Die Anbindung an Public Cloud Diensten erfolgt nach Möglichkeit über das Active Directory im Netikrz. Sowohl der Hersteller als auch die Dr. Netik & Partner GmbH haben einen Administrativen Zugriff.
Je nach Wunsch und Machbarkeit erhält auch der Kunde administrativen Zugriff auf die Cloud.

Es gelten die Nutzungsbestimmungen der Hersteller.

Letze Änderung durch: Stefan Krüger	Letzter Export am: 05.09.2025, (12:14:34)

6. Datenträgerkontrolle

AddOns Global > Datenschutz > TOM

Bezeichnung
Beschreibung (Ziel)
06 Datenträgerkontrolle
Die Maßnahmen für Datenträgerkontrolle verhindern, dass Datenträger mit pbD und anderen sensiblen Daten in eine unbefugte oder unkontrollierte Umgebung geraten.

AddOns Mandant > Datenschutz > TOM Lösungen

Beschreibung	
Referenz auf Globale Daten	**Anwendungsbereich**
Beschreibung	
06.01 Datenträgerkontrolle im Netik RZ	
6	Netik Rechenzentrum Berlin 1
Im Rechenzentrum befinden sich die primären Datenträger in der sicheren Umgebung des primären Rechenzentrums. Das Backup befindet sich in der sicheren Umgebung des Backuprechenzentrums. Austausch und Versand von Backup-Datenträgern erfolgt nach Maßgabe der jeweiligen Verfahren durch Kurierdienste oder eigene Mitarbeiter. Die Bereitstellung von Backupdatenträger von Kundeneigenen Ressourcen erfolgt ausschließlich nach Zusatzvereinbarung. Die Wahl der Transportmethode obliegt dem Auftraggeber. Das Archiv für ausgelagerte Backup-Datenträger befindet sich an einem gesicherten Unternehmensstandort der Dr. Netik & Partner GmbH in einem Datensafe. Backup-Datenträger werden verwaltet und einer regelmäßigen Inventur unterzogen. Der Transport der Backupdatenträger zwischen dem Backuprechenzentrum und dem Unternehmensstandort wird durch ausgewählte Mitarbeiter der Dr. Netik & Partner GmbH durchgeführt. Ausgesonderte Datenträger werden durch professionelle Entsorgungsunternehmen vernichtet.	
06.02 Datenträgerkontrolle als Dienstleister für Kunden	
6	Netik als externer Dienstleister für Kunden
Für Datenträger am Standort des Auftraggebers liegt die Verantwortung für Datenträgerkontrolle beim Auftraggeber. Unsere Mitarbeiter werden vom Auftraggeber eingewiesen und haben die festgelegten Kontrollmaßnahmen für Datenträger einzuhalten.	

Letze Änderung durch: Stefan Krüger	Letzter Export am: 05.09.2025, (12:14:34)

7. Speicherkontrolle

AddOns Global > Datenschutz > TOM

Bezeichnung
Beschreibung (Ziel)
07 Speicherkontrolle
Die Maßnahmen für Speicherkontrolle gewährleisten, dass Benutzer nur Zugriff auf solche Daten erhalten, für die sie berechtigt sind: Benutzerverwaltung und Berechtigungen (Zugriffsrechte)

AddOns Mandant > Datenschutz > TOM Lösungen

Beschreibung	
Referenz auf Globale Daten	**Anwendungsbereich**
Beschreibung	
07.01 Speicherkontrolle - Netik RZ	
7	Netik Rechenzentrum Berlin 1
Der Zugriff auf personenbezogene und sensible Daten wird auf das notwendige Maß begrenzt. Die Maßnahmen für Speicherkontrolle gewährleisten, dass Benutzer nur Zugriff auf solche Daten erhalten, für die sie berechtigt sind. Die zentrale Verwaltung von Berechtigungen erfolgt mittels Gruppen im Active Directory. In Ausnahmefällen erfolgt die Verwaltung direkt in der Anwendung wenn diese keine Active Directory Unterstützung bietet. Der ein- und ausgehende Mailverkehr der Dr. Netik & Partner GmbH wird archiviert.	
07.02 Speicherkontrolle - eigene Standorte	
7	Eigene Standorte (lokale IT-Ressourcen)
Die Produktivdaten der Dr. Netik & Partner GmbH liegen ausschließlich im Rechenzentrum und in der Microsoft Cloud. Diese Geräte sind nach aktuellem Stand der Technik verschlüsselt.	
07.03 Speicherkontrolle - Auftraggeber im Rechenzentrum	
7	Netik Rechenzentrum Berlin 1
Durch Kundenspezifische Berechtigungsgruppen in der Active-Directory Domäne werden folgende Zugriffsrechte auf folgende Speicherorte einheitlich verwaltet. Benutzer werden Berechtigungsgruppen	

zugewiesen.
z.B.
- Zugriff Fileserver und Dateifreigaben
- Zugriff SQL Datenbanken
weitere Dienste je nach Anforderung des Auftrageber.

In Ausnahmefällen erfolgt die Verwaltung direkt in der Anwendung wenn diese keine Active Directory Unterstützung bietet.

Windows Clients eines Auftraggebers werden nur dann durch uns administriert, wenn das vertraglich vereinbart ist.

E-Mails und Digitale Belege eines Auftraggebers werden nur dann archiviert, wenn das vertraglich vereinbart ist.

07.04 Speicherkontrolle - Dienstleister	
7	Netik als externer Dienstleister für Kunden
Die Verantwortung für die Speicherkontrolle liegt beim Auftraggeber. Unsere Mitarbeiter werden vom Auftraggeber eingewiesen und haben die festgelegten Administrations- und Kontrollmaßnahmen für den Zugriff auf Datenspeicher einzuhalten	

Letze Änderung durch: Stefan Krüger	Letzter Export am: 05.09.2025, (12:14:34)

8. Benutzerkontrolle

AddOns Global > Datenschutz > TOM

Bezeichnung
Beschreibung (Ziel)
08 Benutzerkontrolle
Durch die Massnahmen der Benutzerkontrolle wird der Abruf von Daten durch nicht Abrufberechtigte wird durch geeignete Vorkehrungen verhindert. - Benutzeranmeldung, MFA - Passwortrichtlinien

AddOns Mandant > Datenschutz > TOM Lösungen

Beschreibung	
Referenz auf Globale Daten	**Anwendungsbereich**
Beschreibung	
08.01 Benutzerkontrolle - Netik RZ	
8	Netik Rechenzentrum Berlin 1
Der Abruf von Daten durch nicht Abrufberechtigte wird durch geeignete Vorkehrungen verhindert. Jeder Benutzer muss sich an den IT-Systemen, von denen die personenbezogenen Daten abgerufen werden, eindeutig identifizieren und authentifizieren. Der Benutzer muss sich zuerst an der Windows Domäne anmelden. Benutzer, Geräte und andere Objekte werden durch das Verzeichnis der Windows Domäne verwaltet. Soweit möglich, verwenden alle Anwendungen das Verzeichnis für die Authentifizierung. Das gilt für die Anwendungen im Rechenzentrum, in der Microsoft Cloud und auf den Windows Clients. Es werden restriktive Passwortrichtlinien laut BSI Empfehlung durchgesetzt. Wenn Benutzer aus dem Internet, außerhalb eines Standorts des Unternehmens, auf Anwendungen im Rechenzentrum zugreifen wollen, dann melden sie sich mit Mehrfaktorauthentifizierung an. Wenn einzelne Anwendungen die Authentifizierung mittels Active Directory nicht unterstützen, dann haben sie eigenständige Anmeldekonten für die Benutzer.	
08.02 Benutzerkontrolle - Auftraggeber im Rechenzentrum	
8	Netik Rechenzentrum Berlin 1
Restriktive Passwortrichtlinien werden standardmäßig für alle Auftraggeber eingerichtet.	

Für Kundeneigene Anwendungen, welche nicht in das Active Directory integriert sind, obliegt die Verantwortung über die Passwortsicherheit beim Auftraggeber.
08.03 Benutzerkontrolle - als Dienstleister beim Kunden
Für IT-Ressourcen am Standort des Auftraggebers liegt die Verantwortung für die Benutzerkontrolle beim Auftraggeber. Unsere Mitarbeiter werden vom Auftraggeber eingewiesen und haben die festgelegten Maßnahmen einzuhalten.

Letze Änderung durch: Stefan Krüger	Letzter Export am: 05.09.2025, (12:14:34)

9. Eingabekontrolle

AddOns Global > Datenschutz > TOM

Bezeichnung
Beschreibung (Ziel)
09 Eingabekontrolle
Die Maßnahmen der Eingabekontrolle stellen sicher, dass Benutzer ausschließlich solche Daten eingeben, verändern oder löschen können, für die sie entsprechende Berechtigungen besitzen. Auftraggeberdaten werden durch unsere Mitarbeiter nur dann eingegeben oder geändert, wenn (a) ein Auftrag des Auftraggebers erteilt ist, z.B. Serviceauftrag, und wenn (b) der Zugriff durch den Auftraggeber überwacht wird, z.B. mittels Teamviewer.

AddOns Mandant > Datenschutz > TOM Lösungen

Beschreibung	
Referenz auf Globale Daten	**Anwendungsbereich**
Beschreibung	
09.01 Eingabekontrolle - Netik RZ	
9	Netik Rechenzentrum Berlin 1
Über die Zugriffskontrolle hinaus verfügen unsere Anwendungen (die Auftraggeberdaten verwalten) über ein Rollenkonzept, dass die Berechtigung der Benutzer für die Ausführung von Operationen über die Daten steuert. Die Rollen, ihre Berechtigungen und die Zuordnung der Benutzer zu Rollen werden durch ausgewiesene Anwendungsadministratoren verwaltet.	
09.02 Eingabekontrolle - Dienstleistung	
9	Netik als externer Dienstleister für Kunden
Für IT-Ressourcen am Standort des Auftraggebers liegt die Verantwortung für die Eingabekontrolle beim Auftraggeber. Unsere Mitarbeiter werden vom Auftraggeber eingewiesen und haben die festgelegten Eingabekontrollmaßnahmen einzuhalten.	

Letze Änderung durch: Stefan Krüger	Letzter Export am: 05.09.2025, (12:14:35)

10. Übertragungs- und Transportkontrolle

AddOns Global > Datenschutz > TOM

Bezeichnung
Beschreibung (Ziel)
10 Übertragungs- und Transportkontrolle
Unsere Maßnahmen für Übertragungskontrolle gewährleisten, dass überprüft und festgestellt werden kann, an welche Stellen personenbezogene Daten mit Hilfe von Einrichtungen zur Datenübertragung übermittelt oder zur Verfügung gestellt wurden oder werden können. Die Maßnahmen der Transportkontrolle gewährleisten, dass personenbezogene und sensible Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können. Im Verarbeitungsverzeichnis ist dokumentiert, an welchen Stellen und wie eine Übermittlung solcher Daten vorgesehen ist. Andere Formen der Weitergabe von Daten sind nicht erlaubt.

AddOns Mandant > Datenschutz > TOM Lösungen

Beschreibung	
Referenz auf Globale Daten	**Anwendungsbereich**
Beschreibung	
10.01 Übertragungs- und Transportkontrolle - Netik RZ	
10	Netik Rechenzentrum Berlin 1
Die Weitergabe von Daten auf Grund gesetzlicher oder behördlicher Auflagen erfolgt in der dafür vorgesehenen Form (z.B. Finanzamt, Bundesagentur für Arbeit, Krankenkassen). Der Austausch von personenbezogenen Daten erfolgt nur in enger Abstimmung mit dem Kunden. Die Übertragung von E-Mails wird verschlüsselt. Unsere Mitarbeiter sind angewiesen, pbD bzw. Kontaktdaten nicht mittels E-Mail an Dritte zu übermitteln. Dokumente in Papierform werden nur auf dem offiziellen Postweg übertragen. Der Einsatz von Papierform und Fax wird auf das notwendige Minimum begrenzt bzw. entfällt ganz. Bevorzugt wird generell die elektronische Übertragung.	
10.02 Übertragungs- und Transportkontrolle - Dienstleistung	
10	Netik als externer Dienstleister für Kunden

Für Übertragung und Transport von Daten liegt die Verantwortung beim Auftraggeber. Unsere Mitarbeiter werden vom Auftraggeber eingewiesen und haben die festgelegten Übertragungs- und Transportkontrollmaßnahmen einzuhalten.

Die Weitergabe von Daten des Auftraggebers ohne Information und Freigabe durch den Auftraggeber ist unseren Mitarbeitern nicht erlaubt.

Weitere technische Einschränkungen zum Download von Daten aus dem Netik-RZ sind individuell mit dem Kunden abgestimmt.

Letze Änderung durch: Stefan Krüger	Letzter Export am: 05.09.2025, (12:14:35)

11. Wiederherstellbarkeit

AddOns Global > Datenschutz > TOM

Bezeichnung
Beschreibung (Ziel)
11 Wiederherstellbarkeit
Die Massnahmen für die Wiederherstellbarkeit stellen sicher, dass Systeme, Anwendungen und Daten nach einer Störung oder nach einem Notfall wiederhergestellt werden können: - Backup und Recovery - Snapshots

AddOns Mandant > Datenschutz > TOM Lösungen

Beschreibung	
Referenz auf Globale Daten	**Anwendungsbereich**
Beschreibung	
11 Wiederherstellbarkeit	
11	Netik Rechenzentrum Berlin 1
Alle Daten im Netik-RZ können von mehrstufigen Backups wiederhergestellt werden. Die primäre Datensicherung erfolgt auf einem separaten Storage, von welchem sowohl einzelne Dateien als auch ganze Server in kürzester Zeit wiederhergestellt werden können. Die Datensicherung erfolgt täglich nach Sicherungsplänen und wird 30 Tage vorgehalten. Zusätzlich dazu werden noch 4 Monatssicherungen aufbewahrt. Die zweite Datensicherung erfolgt unabhängig auf eine Magnetband-Library. Diese Library steht im Netik Rechenzentrum 2. Die Monatssicherungen werden regelmäßig ausgelagert und für 12 Monate aufbewahrt. Option zusätzliche Sicherungsbänder: Auf Wunsch erstellen wir zusätzliche kundenspezifische Datensicherungsbänder, die der Kunde selbst aufbewahren kann (z.B. quartalsweise oder in anderen Perioden). Als zusätzliche Sicherheit werden täglich Snapshots erstellt, die 7 Tage vorgehalten werden. Diese können aufgrund des Safemode nur im Vier-Augen-Prinzip zwischen Netik und dem Hersteller gelöscht werden. Daten in der Cloud sowie Daten auf lokalen Clients werden nach separater Beauftragung durch den Auftraggeber von uns gesichert.	

Letze Änderung durch: Stefan Krüger	Letzter Export am: 05.09.2025, (12:14:35)

12. Zuverlässigkeit

AddOns Global > Datenschutz > TOM

Bezeichnung
Beschreibung (Ziel)
12 Zuverlässigkeit
Unsere Massnahmen stellen die Zuverlässigkeit und Verfügbarkeit von Systemem, Anwendungen und Daten sicher: - Hochverfügbarkeit - Redundanzen - Virtualisierung - Outsourcing

AddOns Mandant > Datenschutz > TOM Lösungen

Beschreibung	
Referenz auf Globale Daten	**Anwendungsbereich**
Beschreibung	
12 Zuverlässigkeit	
12	Netik Rechenzentrum Berlin 1
Die unterbrechungsfreie Funktion der Systeme ist durch Maßnahmen für Hochverfügbarkeit und Redundanz sichergestellt. Hochverfügbarkeit wird durch Redundanzen erreicht: - Redundanz und Load Balancing für wichtige Systeme, z.B. Internetverbindung und Internetsicherheit, Stromversorgung u.a. - Trennung von Hardware und Anwendung durch Virtualisierung, soweit technisch möglich. - Trennung von Verarbeitung und Speicherung: Es werden hochverfügbare Storage Systeme (SAN) eingesetzt, die Daten für die verschiedene Server Systeme bereitstellen. - Outsourcing von Cloud-Anwendungen an Provider.	

Letze Änderung durch: Stefan Krüger	Letzter Export am: 05.09.2025, (12:14:35)

13. Datenintegrität

AddOns Global > Datenschutz > TOM

Bezeichnung
Beschreibung (Ziel)
13 Datenintegrität
Die Massnahmen für Datenintegrität gewährleisten, dass gespeicherte Daten nicht durch Fehlfunktionen des Systems beschädigt werden.

AddOns Mandant > Datenschutz > TOM Lösungen

Beschreibung	
Referenz auf Globale Daten	**Anwendungsbereich**
Beschreibung	
13.01 Datenintegrität - Netik RZ	
13	Netik Rechenzentrum Berlin 1
Daten, insbesondere personenbezogene Daten und sensible Daten, befinden sich auf sicheren, hochverfügbaren Speichersystemen im Netik Rechenzentrum oder auf Cloud-Speichern – in jedem Fall in Übereinstimmung mit der vertraglichen Vereinbarung. Daten sind gegen Zerstörung, Veränderung oder Verlust durch Schadsoftware durch Maßnahmen entsprechend dem aktuellen Stand der Technik geschützt. Zusätzlich zu den durch uns getroffenen Maßnahmen bieten wir dem Auftraggeber eine Reihe von Lösungen für Datenschutz und Compliance auf der zentralen Infrastruktur und auf seiner Client Landschaft an.	
13.02 Datenintegrität - Dienstleistung	
13	Netik als externer Dienstleister für Kunden
Für Datenschutz und Compliance am Standort des Auftraggebers liegt die Verantwortung beim Auftraggeber, wobei wir ihn durch Lösungen auf der zentralen Infrastruktur und auf lokalen Infrastruktur (Clients, Firewall u.a.) unterstützen. Dies setzt eine vertragliche Vereinbarung voraus. Buchung entsprechender Lösungen und der zugehörigen Wartungsleistung.	

Letze Änderung durch: Stefan Krüger	Letzter Export am: 05.09.2025, (12:14:35)

14. Auftragskontrolle

AddOns Global > Datenschutz > TOM

Bezeichnung
Beschreibung (Ziel)
14 Auftragskontrolle
Die Maßnahmen der Auftragskontrolle stellen sicher, dass Auftraggeberdaten gemäß Weisung des Auftraggebers verarbeitet werden. Mit jedem Auftraggeber wird eine Vereinbarung über Auftragsverarbeitung abgeschlossen. Im Rahmen der Vereinbarung zur Auftragsverarbeitung werden wir Auftraggeberdaten entsprechend Weisung des Auftraggebers erheben, verarbeiten, speichern, sperren oder löschen. Wenn der Auftraggeber keine spezifische Weisung erteilt, werden wir nach unseren aktuellen TOM (Technische und organisatorische Maßnahmen zum Schutz der Daten des Auftraggebers – dieses Dokument) handeln.

AddOns Mandant > Datenschutz > TOM Lösungen

Beschreibung	
Referenz auf Globale Daten	**Anwendungsbereich**
Beschreibung	
14.01 Auftragskontrolle - als Dienstleister	
14	Netik Rechenzentrum Berlin 1
Mittels automatisierter IT-Dokumentation wird der Status der IT-Ressourcen im Netik RZ regelmäßig dokumentiert. Der Auftraggeber und ein durch ihn Beauftragter (z.B. Wirtschaftsprüfer, DSB) haben das Recht, mittels Audit, Einsichtnahme in die Einhaltung der zu prüfenden Prozesse des Auftraggebers zu nehmen.	
14.02 Auftragskontrolle - Dienstleister beim Kunden	
14	Netik als externer Dienstleister für Kunden
Auftragskontrolle erfolgt über die Leisungserfassung innerhalb unserer monatlichen Servicerechnung bzw. durch bestätigung der Leistung im Lieferschein.	
14.03 Auftragskontrolle - externe Dienstleister	

14	Netik als externer Dienstleister für Kunden
Externe Dienstleister, die zufällig Einblick in Auftraggeber Daten erhalten könnten (z.B. Reinigungsunternehmen, Datenträgerentsorgung) werden auf den Datenschutz und Vertraulichkeit verpflichtet.	

Letze Änderung durch: Stefan Krüger	Letzter Export am: 05.09.2025, (12:14:36)

15. Verfügbarkeitskontrolle

AddOns Global > Datenschutz > TOM

Bezeichnung
Beschreibung (Ziel)
15 Verfügbarkeitskontrolle
Die Maßnahmen der Verfügbarkeitskontrolle stellen sicher, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt werden.

AddOns Mandant > Datenschutz > TOM Lösungen

Beschreibung	
Referenz auf Globale Daten	**Anwendungsbereich**
Beschreibung	
15.01 Verfügbarkeitskontrolle - Netik RZ	
15	Netik Rechenzentrum Berlin 1
Das Netik Rechenzentrum befindet sich in den Räumen eines professionellen Co-Location Providers. Die Schutzmaßnahmen gegen Einbruch-, Brand-, Wasser-, Klima- und Überspannungsschäden und gegen Ausfall von Medien wie Strom und Internet sind vertraglich geregelt. Für den Schutz der pbD und anderer sensibler Daten betreiben wir (unabhängig von den Vorkehrungen des Housing Providers) ein umfangreiches Sicherheitskonzept, das folgende Maßnahmen auf dem fortgeschrittenen Stand der Technik einschließt: - leistungsfähige, hochverfügbare Server und Virtualisierungsplattform - aktuelle Windows Infrastruktur: Domänenverwaltung, aktuelle Windows Serverbetriebssysteme einschl. Management von Funktions- und Sicherheits-Updates - provisionierte Server - Wiederanlaufkonzept - sichere Datenspeicher: SAN-Infrastruktur, NAS - Sicherung der Daten auf einer leistungsfähigen Tape Library mit einem mehrstufigen Datensicherungsprozess: VSS, Tages-, Wochen-, Monats- und Jahressicherung - stichprobenartige Rücksicherungstests im Rahmen der Wartungsprozesse - regelmäßige Auslagerung der Backup-Datenträger aus dem Rechenzentrum - sichere Verbindungen und Schutz gegen Gefahren aus dem Internet durch hochverfügbare Firewall - Viren-Schutz, E-Mail Security, Content-Filter für Zugriff auf Internetinhalte - planmäßige Wartungs- und Erneuerungsprozesse - regelmäßige Inventur und Dokumentation der IT-Ressourcen - proaktives Systemmonitoring - Störungsmanagement - Angriffsfrüherkennung (MDR) und Schwachstellenmanagement (MR)	

15.02 Verfügbarkeitskontrolle - Dienstleister	
15	Netik als externer Dienstleister für Kunden
Für IT-Ressourcen am Standort des Auftraggebers liegt die Verantwortung für die Verfügbarkeitskontrolle beim Auftraggeber. Unsere Mitarbeiter werden vom Auftraggeber eingewiesen und haben die festgelegten Verfügbarkeitskontrollmaßnahmen einzuhalten.	

Letze Änderung durch: Stefan Krüger	Letzter Export am: 05.09.2025, (12:14:36)

16. Datentrennung

AddOns Global > Datenschutz > TOM

Bezeichnung
Beschreibung (Ziel)
16 Datentrennung
Die Maßnahmen der Datentrennung stellen sicher, dass Auftraggeberdaten für unterschiedliche Auftraggeber oder unterschiedliche Zwecke getrennt gespeichert und verarbeitet werden.

AddOns Mandant > Datenschutz > TOM Lösungen

Beschreibung	
Referenz auf Globale Daten	**Anwendungsbereich**
Beschreibung	
16.01 Datentrennung - Netik RZ	
16	Netik Rechenzentrum Berlin 1
Datentrennung zwischen Auftraggebern erfolgt wie im Punkt 05.02. beschrieben. Auf Anforderung oder auf Grund technischer Erfordernisse werden dem Auftraggeber private IT-Ressourcen – in der Regel in Form eigener virtueller Server – zur Verfügung gestellt. Auf shared Ressourcen verfügt jeder Auftraggeber über eigene Datenstrukturen: - eigene Datenbanken - eigene Dateiverzeichnisstrukturen - eigene Archive Unsere IT-Ressourcen werden in diesem Sinne ebenso wie die eines Auftraggebers behandelt. Für bereitgestellte Anwendungen werden getrennte Produktiv-, Test- und Entwicklungsdaten-Umgebungen bereitgestellt, sofern Entwicklungs- und Testprozesse stattfinden. Auf Anforderung wird dem Auftraggeber für eine kundenspezifische Anwendung vor der Implementierung eine Testumgebung bereitgestellt.	
16.02 Datentrennung - Dienstleistung	
16	Netik als externer Dienstleister für Kunden
Wenn vertraglich nicht anders festgehalten, liegt für IT-Ressourcen am Standort des Auftraggebers die Verantwortung für die Datentrennung beim Auftraggeber. Unsere Mitarbeiter werden vom Auftraggeber eingewiesen und haben die festgelegten Maßnahmen für Datentrennung einzuhalten.	

Letze Änderung durch: Stefan Krüger	Letzter Export am: 05.09.2025, (12:14:36)

17. Telearbeit

AddOns Global > Datenschutz > TOM

Bezeichnung	
Beschreibung (Ziel)	
17 Telearbeit und Mobile Nutzung der IT	
Die Maßnahmen für Telearbeit stellen sicher, dass Auftraggeberdaten ausschließlich in unserer gesicherten IT-Umgebung gespeichert und verarbeitet werden	

AddOns Mandant > Datenschutz > TOM Lösungen

Beschreibung	
Referenz auf Globale Daten	**Anwendungsbereich**
Beschreibung	
17.01 Telearbeit - Netik RZ	
17	Netik Rechenzentrum Berlin 1
Die Maßnahmen für Telearbeit stellen sicher, dass Auftraggeberdaten standardmäßig in unserer gesicherten IT Umgebung gespeichert und verarbeitet werden. Der mobile Zugang (mobil, Home Office) über das Netscaler Access Gateway im Rechenzentrum ist nur mit personalisierter Multifaktor-Authentifizierung möglich.	
17.02 Telearbeit - Dienstleistung	
17	Netik als externer Dienstleister für Kunden
Für IT-Ressourcen am Standort des Auftraggebers liegt die Verantwortung für Telearbeit beim Auftraggeber. Unser Mitarbeiter darf nach unseren Standards auf IT-Ressourcen des Auftraggebers ausschließlich über unser Rechenzentrum zugreifen. Im Fall Telearbeit muss er sich dafür erst am Rechenzentrum authentifizieren, ehe er über eine gesicherte Verbindung auf die IT-Umgebung des Auftraggebers zugreifen kann.	

TOM

Abschließender Prüfbericht 2025-09-05

Erstellt:	2025-09-05
Von:	Christoph Marx (cmarx@netik.de)
Status:	Signiert
Transaktions-ID:	CBJCHBCAABAAUFs1GYHOgO5tJ4_0728F-G5wR6-IU8lS

Verlauf für „TOM“

Christoph Marx (cmarx@netik.de) hat das Dokument erstellt.
2025-09-05 - 10:16:05 GMT– IP-Adresse: 217.70.133.162

Dokument wurde per E-Mail zur Signatur an Bernd Scheller (bscheller@netik.de) gesendet.
2025-09-05 - 10:16:37 GMT

Bernd Scheller (bscheller@netik.de) hat die E-Mail angezeigt.
2025-09-05 - 10:29:28 GMT– IP-Adresse: 82.193.231.121

Bernd Scheller (bscheller@netik.de) hat das Dokument mit einer E-Signatur versehen.
Signaturdatum: 2025-09-05 – 10:29:52 GMT – Zeitquelle: Server– IP-Adresse: 82.193.231.121

Vereinbarung abgeschlossen.
2025-09-05 - 10:29:52 GMT