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

Stand: 30.4.2018

Die hier aufgeführten Maßnahmen werden in Übereinstimmung mit der Datenschutz-Grundverordnung (DSGVO) und dem Bundesdatenschutzgesetz (BDSG neu) realisiert.

Grundsätzlich behandelt der Datenschutz nur personenbezogene Daten (pbD). Der Datenschutz bezieht sich jedoch beim Begriff der Datensicherung von personenbezogenen Daten auch auf die Gefahr des Verlustes, des Missbrauchs, der Beschädigung oder Zerstörung der verwendeten IT-Systeme (Hard- und Software), sowie deren benutzter Infrastruktur. Geschützt werden müssen somit Hard- und Software, Daten und Informationen. Dementsprechend gelten die hier beschriebenen technischen und organisatorischen Schutzmaßnahmen für alle sensiblen Daten.

Die Datenschutzmaßnahmen gelten

- für Netik als Unternehmensgruppe und Auftragnehmer
- für Netik als Solution Provider
- für Netik als Dienstleister

in allen Vertragsbeziehungen, in deren Rahmen wir Daten des jeweiligen Auftraggebers speichern oder verarbeiten.

Begriffe

Wir bezeichnet den Auftragnehmer – die Unternehmen der Netik Gruppe – Dr. Netik & Partner GmbH, Software und Service Dr. Netik GmbH und Cloud Link GmbH – mit ihren Mitarbeitern und Beauftragten.

Personenbezogene Daten (pbD) sind entsprechend den Rechtgrundlagen alle Informationen, die sich auf eine natürliche Person beziehen oder zumindest beziehbar sind und so Rückschlüsse auf deren Persönlichkeit erlauben. Das betrifft sowohl pbD, die wir selbst erfassen, speichern und verarbeiten, als auch pbD des Auftraggebers, auf die wir als Auftragnehmer Zugriff haben.

Weitere sensible Daten sind kaufmännische, Kunden- und Finanzdaten des Auftraggebers. Der Auftraggeber kann uns für weitere sensible Daten besondere Vorgaben zum Datenschutz erteilen. Ohne weitere Vorgaben beschränken wir uns auf die gesetzlichen Anforderungen.

Auftraggeberdaten sind sämtliche Daten, die uns vom Auftraggeber bereitgestellt werden.

IT-Services sind alle Services, die wir im Rahmen eines Vertrages bereitstellen.

Benutzer bezeichnet eine Person, die auf unsere IT-Services zugreift.

Rechenzentrum (RZ) steht für das Netik Rechenzentrum, in dem IT-Ressourcen für Netik selbst, sowie auch für Auftraggeber bereitgestellt werden.

Datenschutz

Wir halten alle Gesetze zum Datenschutz ein, die im Allgemeinen für die Bereitstellung von IT-Services gelten. Unsere IT-Services stellen wir einheitlich für eine Vielzahl von Auftraggebern bereit.

Für spezielle Datenschutzerfordernisse, die für bestimmte Datenkategorien, einen bestimmten Auftraggeber oder dessen Branche und nicht allgemein für Dienstanbieter im Bereich der Informationstechnologie gelten, muss uns der Auftraggeber spezielle Weisung erteilen.

Auftraggeberdaten

- **Datenverarbeitung:** Wir verarbeiten Auftraggeberdaten gemäß den hier niedergelegten Regeln und, sofern der Vertrag mit dem Auftraggeber und diese Ergänzung keine Ausnahmen vorsehen, (a) erwerben wir keine Rechte an Auftraggeberdaten und (b) nutzen und legen wir Auftraggeberdaten nur zu den unten genannten Zwecken offen. Wir nutzen Auftraggeberdaten wie folgt:

  Auftraggeberdaten werden ausschließlich für die Bereitstellung unserer IT-Services genutzt. Dies umfasst möglicherweise auch die Fehlerbehebung, um Problemen, die die Bereitstellung der IT-Services beeinträchtigen, vorzubeugen, diese zu erkennen und zu beheben, sowie die Verbesserung von Funktionen, die neue oder sich entwickelnde Bedrohungen für den Benutzer (wie Malware oder Spam) erkennen und einen entsprechenden Schutz bieten.

  Auftraggeberdaten werden den Strafverfolgungsbehörden nur offengelegt, wenn wir gesetzlich dazu verpflichtet sind. Sollte sich eine Strafverfolgungsbehörde mit der Bitte um Herausgabe von Auftraggeberdaten an uns wenden, versuchen wir, diese mit ihrer Bitte direkt an den Auftraggeber zu verweisen. In diesem Fall geben wir die allgemeinen Kontaktdaten des Auftraggebers möglicherweise an die Behörde weiter. Wenn wir zur Offenlegung von Auftraggeberdaten gegenüber der Strafverfolgungsbehörde verpflichtet sind, unternehmen wir – sofern gesetzlich zulässig – alle üblichen Schritte, um den Auftraggeber im Voraus über eine derartige Offenlegung zu informieren.
- **Speicherung von Auftraggeberdaten:** Wir speichern Auftraggeberdaten in Ländern der Europäischen Union.
  Auf besondere Anweisung speichern wir Daten in Deutschland.
  Wir geben dem Auftraggeber auf Anfrage Auskunft über den Speicherort.
  Wir übermitteln keine Auftraggeberdaten in andere Staaten.
- **Anfragen von Benutzern:** Wir beantworten keine sachlichen Datenschutzanfragen der Benutzer des Auftraggebers ohne eine vorherige Weisung des Auftraggebers, es sei denn, wir sind gesetzlich dazu verpflichtet.
- **Löschung oder Rückgabe von Auftraggeberdaten:** Nach Ablauf oder Kündigung des Vertrages kann der Auftraggeber seine Daten extrahieren und exportieren oder löschen lassen. Die Auftraggeberdaten werden in einem Format entsprechend dem aktuellen Stand der Technik bereitgestellt. Der Auftraggeber hat keinen Anspruch auf die Auswahl des Formats.

- **Verarbeitung durch unsere Mitarbeiter:** Unsere Mitarbeiter verarbeiten Auftraggeberdaten nicht ohne vorherige Genehmigung. Sie sind verpflichtet, die Vertraulichkeit von Auftraggeberdaten zu wahren, auch nach Beendigung ihres Arbeitsverhältnisses. Diese Verpflichtung bestätigt jeder Mitarbeiter persönlich per Unterschrift.
- **Subunternehmen:** Möglicherweise beauftragen wir Subunternehmen mit der Erbringung bestimmter Dienstleistungen wie Kundensupport. Diese Subunternehmen dürfen Auftraggeberdaten nur zur Erbringung der Dienstleistungen abrufen, für die sie von uns beauftragt wurden. Eine Nutzung für andere Zwecke ist nicht gestattet. Wir bleiben für die Einhaltung der Verpflichtungen dieser Ergänzung durch unsere Subunternehmen verantwortlich. Wir geben keine persönlichen Daten, die der Auftraggeber uns durch die Nutzung unserer Services bereitstellt, an Dritte weiter.

Sicherheit

- **Technische und organisatorische Sicherheitsmaßnahmen:** Durch die unten aufgeführten Maßnahmen sowie durch interne Kontrollen und Routinen zur Informationssicherheit schützen wir Auftraggeberdaten vor versehentlichem Verlust, Zerstörung oder Änderung, nicht autorisierter Weitergabe oder unberechtigtem Zugriff sowie gesetzeswidriger Vernichtung. Unsere technischen und organisatorischen Maßnahmen entsprechen dem fortgeschrittenen Stand der Technik.

  Die in diesem Abschnitt beschriebenen Maßnahmen stellen unsere einzige Verpflichtung in Bezug auf die Sicherheit und Handhabung von Auftraggeberdaten dar, und wir kommen damit sämtlichen Vertraulichkeitsverpflichtungen im Vertrag oder anderen Geheimhaltungsvereinbarungen mit dem Auftraggeber nach.
- **Sicherheitsrelevante Vorfälle:** Wenn wir von einem rechtswidrigen Zugriff auf Auftraggeberdaten erfahren, die auf unseren Geräten oder in unseren Räumlichkeiten gespeichert sind, oder ein nicht autorisierter Zugriff auf solche Geräte oder Zugang zu diesen Räumlichkeiten führt zu einem Verlust, einer Offenlegung oder einer Änderung von Auftraggeberdaten (jeweils ein "sicherheitsrelevanter Vorfall"), werden wir:
  (a) den Auftraggeber [unverzüglich] über den sicherheitsrelevanten Vorfall in Kenntnis setzen;
  (b) den sicherheitsrelevanten Vorfall untersuchen und den Auftraggeber darüber informieren;
  (c) die Meldepflichten gegenüber Aufsichtsbehörden erfüllen und
  (d) alle erforderlichen Schritte ergreifen, um die Auswirkungen und den Schaden des sicherheitsrelevanten Vorfalls auf ein Minimum zu reduzieren.
- Ein erfolgloser sicherheitsrelevanter Vorfall unterliegt nicht diesem Abschnitt. Ein erfolgloser sicherheitsrelevanter Vorfall ist ein Vorfall, der nicht zu einem unberechtigten Zugriff auf Auftraggeberdaten oder Zugang zu Geräten oder Räumlichkeiten führt, auf oder in denen Auftraggeberdaten gespeichert sind, und kann, ohne Beschränkung, Folgendes umfassen: Pings und andere Broadcast-Angriffe auf Firewalls oder Edge-Server, Portscans, erfolglose Anmeldeversuche, Denial-of-Service-Angriffe, Packet Sniffing (oder andere nicht autorisierte Zugriffe auf Informationen zum Datenverkehr, die nicht über IP-Adressen oder Header hinausgehen) oder ähnliche Vorfälle.
- Zudem darf unsere Melde- oder Handlungspflicht im Hinblick auf sicherheitsrelevante Vorfälle im Rahmen dieses Abschnitts nicht als Fehler- oder Schuldeingeständnis in Bezug auf den sicherheitsrelevanten Vorfall ausgelegt werden.

- Die Meldung sicherheitsrelevanter Vorfälle erfolgt an den gesetzlichen Vertreter des Auftraggebers, wobei die Wahl der Mittel uns überlassen bleibt (darunter E-Mail). Die Richtigkeit der Kontaktdaten des gesetzlichen Vertreters liegt in alleiniger Verantwortung des Auftraggebers.
- Nach Maßgabe des Vertrages können Leistungen ggf. in Rechnung gestellt werden.

Pflichten des Auftraggebers

Der Auftraggeber ist verpflichtet, sich an die geltenden rechtlichen Vorgaben im Hinblick auf Datenschutz und Vertraulichkeit von Kommunikation zu halten, die der Nutzung unserer Services zugrunde liegen.

- **Rolle der Parteien:** Im Rahmen unserer Verträge ist der Auftraggeber der Datencontroller, und wir sind der Datenverarbeiter, der im Namen des Auftraggebers handelt. Als Daten-verarbeiter werden wir nur auf Anweisung des Auftraggebers hin aktiv. Sein Vertrag sowie die „Vereinbarung über Auftragsverarbeitung" enthalten die vollständigen und endgültigen Anweisungen an uns im Hinblick auf die Verarbeitung von Auftraggeberdaten.
- **Dauer der Datenverarbeitung:** Die Dauer der Datenverarbeitung richtet sich nach der im Rahmen des Vertrags festgelegten Laufzeit.

Neubrandenburg, 30.4.2018

Heimon Hinze
für die Unternehmen der Netik Gruppe:

Dr. Netik & Partner GmbH
Software und Service Dr. Netik GmbH
Cloud Link GmbH

1. Organisatorische Maßnahmen

Für personenbezogene Daten gelten gesetzliche Pflichten, denen wir in folgender Weise nachkommen:

- Wir haben den die Verfahren identifiziert, die personenbezogene Daten nach Art. 4 DSGVO verarbeiten.
- Wir führen ein Verarbeitungsverzeichnis über diese Verfahren.
- Wir haben eine Datenschutzbeauftragte berufen.
- Wir schließen mit jedem Auftraggeber eine „Vereinbarung über Auftragsverarbeitung" ab.
- 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 Auftraggeberdaten 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.

2. Grundsätze für IT-Infrastruktur, Anwendungen, Datenspeicher und Serviceleistungen

Rechenzentrum

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
- VPN-Gateway und Access Gateway 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. Die Administration erfolgt mittels Windows AD.

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.

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.

Citrix Cloud

Wir beziehen für uns, und falls vereinbart für Kunden, Services aus der Citrix Cloud.

Für unsere in Sharefile gespeicherten Daten liegt der Cloud Speicher in der EU (Frankfurt/M). Die Controlplanes unserer Kunden liegen ebenfalls auf diesem Speicher. Damit gilt durchgängig EU Recht.

Für Daten, die unsere Kunden in Sharefile speichern, liegt der Cloud Speicher nicht in der Citrix Cloud, sondern im Netik Rechenzentrum.

Unsere eigenen lokalen IT-Ressourcen

Als lokale IT-Ressourcen sind bei uns 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
- VPN-Gateway für den gesicherten Zugriff auf die Ressourcen des RZ
- Telefonanlagen, wobei der CTI-Server im RZ steht

Die Nutzung lokaler Ressourcen bei Kunden ist nicht reglementiert.

Netik als Dienstleister

Unsere Mitarbeiter sind im Unternehmen Dr. Netik & Partner beschäftigt.

Leistungen im Rahmen von Serviceverträgen der Software und Service Dr. Netik GmbH oder der Cloud Link GmbH werden durch Mitarbeiter der Dr. Netik & Partner GmbH als interner Subunternehmer erbracht.

Externe Mitarbeiter und Subunternehmer werden durch entsprechende Vereinbarungen genauso wie eigene Mitarbeiter auf den Datenschutz verpflichtet.

3. Maßnahmen der Zutrittskontrolle

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

Rechenzentrum:

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.

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.

Unsere eigenen Standorte

Die Geschäftsräume in Neubrandenburg und Güstrow sind mit Schließanlagen, Einbruch-meldeanlagen und Brandmeldeanlage ausgestattet (BMA nur in Neubrandenburg). Die Alarmverfolgung sowie die Aufrechterhaltung der Funktion ist in Verträgen mit Fachfirmen geregelt.

Unsere eigenen Mitarbeiter haben uneingeschränkten Zutritt zu den Geschäftsräumen.

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

Rechenzentrum am Standort des Auftraggebers und Netik als Dienstleister:

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.

4. Maßnahmen der Zugangskontrolle

Die Maßnahmen der Zugangskontrolle verhindern, dass Unbefugte Zugang zu den IT-Ressourcen erhalten, mit denen Auftraggeberdaten gespeichert oder verarbeitet werden.

Rechenzentrum:

Das Netik Rechenzentrum ist durch ein mehrstufiges Zugangskontrollsystem gesichert.

Der Zugang aus der IT-Umgebung eines Netik Standorts erfolgt über die VPN-Verbindung zwischen Standort und Rechenzentrum.

Der Zugang von anderen Standorten (Mobil, Home Office, Kunde usw.) über das Access Gateway ist nur mit zusätzlicher personalisierter Multifaktor-Authentifizierung möglich. Die Verbindung ist verschlüsselt.

Gegen das Internet wird der Zugang mit einer Firewall auf dem aktuellen Stand der Technik gesichert.

Rechenzentrum am Standort des Auftraggebers und Netik als Dienstleister:

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.

5. 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.

Unsere eigene IT-Umgebung

Die Zugriffssteuerung wird im 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 Windows AD verwaltet und gesteuert.

Soweit möglich, beziehen alle IT-Anwendungen ihre Anmeldedaten und Berechtigungen aus dem Windows AD (z.B. Exchange, MS SQL, CTI, Firewall, Access Gateway, Sharepoint u.a.).

In anderen Fälle haben Anwendungen eine eigene Benutzerverwaltung und -authentifizierung.

Benutzerkonten, Administratorkonten, Dienstbenutzerkonten werden konsequent getrennt.

Automatisierte Anwendungen laufen mit dedizierten Dienstkonten.

Berechtigungen und Richtlinien werden gruppenbasiert administriert.

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, das im Unternehmen nicht veröffentlicht wird, und das nur für Notfälle genutzt werden darf. Der Zugriff auf Administratorkonten wird protokolliert.

Auftraggeber im Rechenzentrum

Auftraggeber erhalten im Rechenzentrum eine eigene AD-basierte Windows Domänenverwaltung mit eigenen redundanten DC. Die Regeln für den Zugriff von Benutzern eines Auftraggebers auf das Rechenzentrum sind die gleichen wie oben beschrieben, mit folgender Ausnahme.

Passwortrichtlinien werden nicht standardmäßig eingerichtet, sondern müssen durch den Auftraggeber vorgegeben werden.

Das Berechtigungskonzept für den Zugriff seiner eigenen Benutzer wird mit dem Auftraggeber vereinbart.

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

Rechenzentrum am Standort des Auftraggebers und Netik als Dienstleister:

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 durch den Auftraggeber ist nicht erlaubt.

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

Der Zugriff unserer Mitarbeiter auf IT-Ressourcen des Auftraggebers erfolgt nach unseren Regeln ausschließlich über das Netik Rechenzentrum oder aus der gesicherten Umgebung eines Standort-LAN. Unser Mitarbeiter muss erst über unsere Windows Domäne authentifiziert werden, ehe er über eine gesicherte Verbindung auf die Kundenumgebung zugreifen kann.

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

6. Datenträgerkontrolle

Die Maßnahmen für Datenträgerkontrolle verhindern, dass Datenträger mit pbD und anderen sensiblen Daten in eine unbefugte oder unkontrollierte Umgebung geraten.

Rechenzentrum

Im Rechenzentrum befinden sich die Datenträger in einer sicheren Umgebung.

Datenträgeraustausch und -versand erfolgt nach Maßgabe der jeweiligen Verfahren durch Kurierdienst oder Online. Soweit wir Einfluss auf die Verfahren haben, werden Daten nach aktuellem Stand der Technik verschlüsselt.

Das Archiv für ausgelagerte Backup-Datenträger befindet sich an einem gesicherten Unternehmensstandort in einem Datensafe. Backup-Datenträger werden verwaltet und einer regelmäßigen Inventur unterzogen.

Datenträger werden nicht mehrfach verwendet. Ausgesonderte Datenträger werden durch professionelle Entsorgungsunternehmen vernichtet. Mit den Entsorgungsunternehmen bestehen Verträge, die die Verpflichtung auf den Datenschutz beinhalten.

Rechenzentrum am Standort des Auftraggebers und Netik als Dienstleister:

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.

7. Speicherkontrolle

Rechenzentrum

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.

Durch die Berechtigungsgruppen in der Windows Domäne werden folgende Zugriffsrechte auf folgende Speicherorte einheitlich verwaltet. Benutzer werden Berechtigungsgruppen zugewiesen.

- Zugriffsrechte auf Dateiserver, Dateiverzeichnisse, Unterverzeichnisse und Dokumente
- Zugriffsrechte auf Datenbankserver, Datenbanken und Tabellen
- Zugriffsrechte auf Sharepoint Online, OneDrive for Business und andere Speicherorte in der Microsoft Cloud
- Zugriffsrechte auf Sharefile in der Citrix Cloud.

Alle ein- und ausgehenden E-Mails werden bei uns archiviert.

Digitale Belege aus ERP-Prozessen werden (digital) archiviert.

Unsere eigenen lokalen IT-Ressourcen

Zugriffsrechte auf lokale Datenträger der Windows Clients:

- Die Datenträger lokaler Windows Clients werden zusätzlich verschlüsselt, sofern es sich um mobile Geräte handelt (Notebooks und Tablets).
- Auf Client-Datenträgern werden nur Kopien von Live-Daten gespeichert.

Auftraggeber im Rechenzentrum

- 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.

Rechenzentrum am Standort des Auftraggebers und Netik als Dienstleister

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.

8. Benutzerkontrolle

Rechenzentrum

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 authentisieren. Der Benutzer hat sich zuerst an der Windows Domäne zu authentisieren.

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.

Für die Windows Domäne sind strenge Passwortrichtlinien definiert.

Wenn Benutzer aus dem Internet, außerhalb eines Standorts des Unternehmens, auf Anwendungen im Rechenzentrum zugreifen wollen, dann melden sie sich mit Mehrfaktorauthetisierung an.

Wenn einzelne Anwendungen die Authentifizierung mittels Domäne nicht unterstützen, dann haben sie eigenständige Anmeldekonten für die Benutzer.

Personen, die nicht in der Windows Domäne verwaltet werden, haben keinen Zugriff auf Ressourcen des Unternehmen. An solche Personen können Daten dennoch manuell durch berechtigte Mitarbeiter, z.B. mittels E-Mail, übertragen werden. Der gesamte aus- und eingehende E-Mail Verkehr kann im Archiv eingesehen werden.

Auftraggeber im Rechenzentrum

Passwortrichtlinien werden nicht standardmäßig eingerichtet, sondern müssen durch den Auftraggeber vorgegeben werden.

Der E-Mail Verkehr wird nur dann archiviert, wenn das vertraglich vereinbart ist.

9. 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

Rechenzentrum:

Über die Zugriffskontrolle hinaus verfügen unsere Anwendungen (die Auftraggeberdaten verwalten) über ein Rollenkonzept, das 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.

Rechenzentrum am Standort des Auftraggebers und Netik als Dienstleister

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.

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.

Rechenzentrum:

Die Weitergabe von Daten auf Grund gesetzlicher oder behördlicher Auflagen erfolgt in der dafür vorgesehenen Form (z.B. Finanzamt, Bundesagentur für Arbeit, Krankenkassen).

In übrigen Fällen erfolgt die Weitergabe von Daten über VPN-Verbindungen.

E-Mail wird per TLS verschlüsselt.

Unsere Mitarbeiter sind angewiesen, pbD bzw. Kontaktdaten nicht per 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.

Auftraggeber im Netik Rechenzentrum und Rechenzentrum am Standort des Auftraggebers und Netik als Dienstleister

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.

Die Möglichkeit des Downloads von Daten aus der sicheren Umgebung des Netik Rechenzentrums auf lokale Datenträger ist Standard. Wir sperren Downloadmöglichkeiten, wenn der Auftraggeber uns dazu Anweisung erteilt.

11.Wiederherstellbarkeit

Rechenzentrum und Auftraggeber im Rechenzentrum

Alle Daten können von mehrstufigen Backups wiederhergestellt werden.

Die zentralen IT-Systeme sind virtualisiert und werden von Images gestartet. Die Images werden regelmäßig aktualisiert und gesichert.

Daten auf lokalen Clients können in die Cloud gesichert werden. Das ist ein optionaler Service, der durch den Auftraggeber vereinbart werden kann.

12.Zuverlässigkeit

Rechenzentrum und Auftraggeber im Rechenzentrum

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

  Es werden Systemimages bereitgehalten, regelmäßig aktualisiert und gesichert. Von den Images werden die virtualisierten Maschinen (ggf. auf neuer Hardware) gestartet.
- Trennung von Verarbeitung und Speicherung: Es werden hochverfügbare Storage Systeme (SANs) eingesetzt, die Daten für die verschiedenen Server System bereitstellen.
- Outsourcing wichtiger Anwendungen an professionelle Provider

13. Datenintegrität

Die Massnahmen für Datenintegrität gewährleisten, dass gespeicherte Daten nicht durch Fehlfunktionen des Systems beschädigt werden.

Rechenzentrum und Auftraggeber im Rechenzentrum

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 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.

Rechenzentrum am Standort des Auftraggebers und Netik als Dienstleister

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.

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.

Rechenzentrum:

Mittels automatisierter IT-Dokumentation wird der Status der IT-Ressourcen regelmäßig dokumentiert.

Der Auftraggeber und ein durch ihn Beauftragter (z.B. Wirtschaftsprüfer, DSB) haben das Recht, mittels externem Audit, Einsichtnahme in die IT-Administration u.ä. die Einhaltung der Vereinbarungen zu nehmen.

Rechenzentrum am Standort des Auftraggebers und Netik als Dienstleister

Der Auftraggeber hat das Recht, eine automatisierte IT-Dokumentation über den Status der IT-Ressourcen von uns zu fordern.

Subunternehmer

Mit jedem Subunternehmen, der Zugriff auf Auftraggeberdaten erhält oder erhalten könnte, wird eine Vereinbarung über Auftragsvereinbarung abgeschlossen. Im Rahmen der Vereinbarung erteilen wir Weisung über den Umgang mit Auftraggeberdaten.

Subunternehmen, die zufällig Einblick in Auftraggeberdaten erhalten könnten (z.B. Reinigungsunternehmen, Datenträgerentsorgung) werden auf den Datenschutz und Vertraulichkeit verpflichtet.

15. Verfügbarkeitskontrolle

Die Maßnahmen der Verfügbarkeitskontrolle stellen sicher, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt werden.

Rechenzentrum:

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
- Aushändigung der Backup-Datenträger seiner Daten an den Auftraggeber auf Anforderung
- sichere Verbindungen und Schutz gegen Gefahren aus dem Internet durch hochverfügbare Firewall mit DMZ und Access-Gateway
- Viren-Schutz, E-Mail Security, Content-Filter für Zugriff auf Internetinhalte
- Schutz gegen Überspannung und gezielte Reaktion auf Unterbrechung der Stromversorgung
- planmäßige Wartungs- und Erneuerungsprozesse
- regelmäßige Inventur und Dokumentation der IT-Ressourcen
- proaktives Systemmonitoring
- Störungsmanagement

Rechenzentrum am Standort des Auftraggebers und Netik als Dienstleister

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.

16. Datentrennung

Die Maßnahmen der Datentrennung stellen sicher, dass Auftraggeberdaten für unterschiedliche Auftraggeber oder unterschiedliche Zwecke getrennt gespeichert und verarbeitet werden.

Rechenzentrum:

Jeder Auftraggeber erhält im Rechenzentrum eine eigene AD-basierte IT-Verwaltung mit redundanten Domänencontrollern. Mit dem AD wird die Cloud des Auftraggebers abgebildet und gesteuert.

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 Dynamics NAV Anwendung werden getrennte Produktiv-, Test- und Entwicklungsdaten-umgebungen bereitgestellt. Das gilt auch für andere Anwendungen, falls Entwicklungs- und Testprozesse stattfinden.

In einer Datenbank können mehrere Mandanten eines Auftraggebers unterschieden werden.

Auf Anforderung wird dem Auftraggeber für eine kundenspezifische Anwendung vor der Implementierung eine Testumgebung bereitgestellt.

Rechenzentrum am Standort des Auftraggebers und Netik als Dienstleister

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

17. Telearbeit

Die Maßnahmen für Telearbeit stellen sicher, dass Auftraggeberdaten ausschließlich in unserer gesicherten IT-Umgebung gespeichert und verarbeitet werden.

Rechenzentrum:

Telearbeit erfolgt auf Terminalservern im Rechenzentrum. Der Benutzer stellt über das Access Gateway eine verschlüsselte Verbindung zu einem virtuellen Desktop im Rechenzentrum her. Telearbeit erfolgt ausschließlich auf dem virtuellen Desktop. Daten werden zwischen Terminalserver und Receiver nicht übertragen.

Der Zugang von externen Standorten (mobil, Home Office, Kunde usw.) über das Access Gateway im Rechenzentrum ist nur mit zusätzlicher personalisierter Multifaktor-Authentifizierung möglich.

Auf einzelne Anwendungen ist der Zugriff über Browser oder Synchronisierungs-Prozeduren möglich. Die Verbindung zwischen den Client- und Serverschichten der Anwendung werden entsprechend dem aktuellen Stand der Technik gesichert:

- Outlook Web Access (OWA) und Exchange Active Sync
- Sharepoint
- Enterprise File Sharing mittels Sharefile

Der Download von pbD und anderen sensiblen Daten auf lokale Clients ist nicht erlaubt.

Andere Formen der Speicherung und Verarbeitung von pbD und anderen sensiblen Daten sind nicht erlaubt.

Rechenzentrum am Standort des Auftraggebers und Netik als Dienstleister

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.

(Ende des Dokuments)