Technische und organisatorische Maßnahmen (ToM)

Datum: 01.11.2021

Stand 11/21

Technische und organisatorische Maßnahmen (ToM)

gemäß Art. 32 EU-DSGVO

Inhaltsverzeichnis

Stand 11/21

Vorwort

Die netgo GmbH ist ein mittelständisches IT-Systemhaus, welches auf die Betreuung von IT-Systemen bei Steuerberatern und Wirtschaftsprüfern bzw. deren Mandanten, d.h. Unternehmen spezialisiert ist. Neben klassischen vor Ort IT-Servicearbeiten und Netzwerkbetreuungen beim Auftraggeber hat sich netgo auf das „Application-Service-Providing" (ASP) spezialisiert und erbringt „Cloud-Computing"-Leistungen in einem eigenen Rechenzentrum in Würselen.

Zur Infrastruktur des netgo-Rechenzentrums zählen:

- Zutritts- und Zugangskontrolle,
- 24/7 Objektschutz durch einen externen Sicherheitsdienst,
- Alarmanlage und 24/7h-Video-Überwachung,
- eine Anbindung an das öffentliche, ringförmige 10 KV-Stromnetz,
- eine mehrfach redundante unterbrechungsfreie Stromversorgung (USV),
- ein Dieselgenerator-Notstrombetrieb (Tier III+),
- mehrere voll redundant ausgelegte Klimaanlagen,
- eine Brandmeldeüberwachung mit Novec™ 1230-Löschgasanlage,
- eine Multi-Carrier-Hochgeschwindigkeits-Internet-Anbindung mit zwei Hauseinführungen
- mit 24/7 Routing-Überwachung und Administration, usw...

Für netgo ist, sowohl als Auftragnehmer als auch als Auftragsverarbeiter, der Datenschutz von besonderer Bedeutung. Daher hat netgo Schutzmaßnahmen für jeglichen Umgang mit vertraulichen oder sicherungsbedürftigen Daten etabliert, die im Rahmen des technischen Fortschritts stetig weiterentwickelt werden.

Die grundlegende Verpflichtung zum Schutz personenbezogener Daten im Rahmen der Verarbeitung konkretisiert Art. 32 EU-DSGVO, der besondere Anforderungen an die Sicherheit der Verarbeitung stellt. Der Verantwortliche hat ein den festgestellten Risiken angemessenes Schutzniveau sicherzustellen. Zu verhindern ist insbesondere, dass personenbezogene Daten unbeabsichtigt und/oder unrechtmäßig vernichtet, verändert oder

Gesetzesgrundlage

unbefugt offengelegt werden oder auf sonstige Weise verloren gehen bzw. Dritte unbefugt Zugang zu verarbeiteten personenbezogenen Daten erhalten.
Hier zunächst nachfolgend einige Grundlagen aus der europäischen Datenschutz-Grundverordnung (EU-DSGVO) zum besseren Verständnis:
Art. 30 EU-DSGVO „Verzeichnis von Verarbeitungstätigkeiten“:

a) Jeder Verantwortliche und gegebenenfalls sein Vertreter führen ein Verzeichnis aller Verarbeitungstätigkeiten, die ihrer Zuständigkeit unterliegen. Dieses Verzeichnis enthält sämtliche folgende Angaben:

- **(1)** den Namen und die Kontaktdaten des Verantwortlichen und gegebenenfalls des gemeinsam mit ihm Verantwortlichen, des Vertreters des Verantwortlichen sowie eines etwaigen Datenschutzbeauftragten;
- **(2)** die Zwecke der Verarbeitung;
- **(3)** eine Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten;
- **(4)** die Kategorien von Empfängern gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden, einschließlich Empfänger in Drittländern oder internationalen Organisationen;
- **(5)** gegebenenfalls Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation, einschließlich der Angabe des betreffenden Drittlands oder der betreffenden internationalen Organisation, sowie bei den in Artikel 49 Absatz 1 Unterabsatz 2 EU-DSGVO genannten Datenübermittlungen die Dokumentierung geeigneter Garantien;
- **(6)** wenn möglich, die vorgesehenen Fristen für die Löschung der verschiedenen Datenkategorien;
- **(7)** wenn möglich, eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Artikel 32 Absatz 1.

b) Jeder Auftragsverarbeiter und gegebenenfalls sein Vertreter führen ein Verzeichnis zu allen Kategorien von im Auftrag eines Verantwortlichen durchgeführten Tätigkeiten der Verarbeitung, die Folgendes enthält:

- **(1)** den Namen und die Kontaktdaten des Auftragsverarbeiters oder der Auftragsverarbeiter und jedes Verantwortlichen, in dessen Auftrag der Auftragsverarbeiter tätig ist, sowie gegebenenfalls des Vertreters des Verantwortlichen oder des Auftragsverarbeiters und eines etwaigen Datenschutzbeauftragten;
- **(2)** die Kategorien von Verarbeitungen, die im Auftrag jedes Verantwortlichen durchgeführt werden;
- **(3)** gegebenenfalls Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation, einschließlich der Angabe des betreffenden Drittlands oder der betreffenden internationalen Organisation, sowie bei den in Artikel 49 Absatz 1 Unterabsatz 2 genannten Datenübermittlungen die Dokumentierung geeigneter Garantien;
- **(4)** wenn möglich, eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Artikel 32 Absatz 1 EU-DSGVO.

Art. 32 Abs. 1 EU-DSGVO „Sicherheit der Verarbeitung“:
Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten; diese Maßnahmen schließen unter anderem Folgendes ein:

a) die Pseudonymisierung und Verschlüsselung personenbezogener Daten;

b) die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;

c) die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen;

Technische und organisatorische Maßnahmen (ToM)

d) ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

Nachfolgend befindet sich die Beschreibung der „technischen und organisatorischen Maßnahmen (ToM)" der netgo am Standort Carlo-Schmid-Str. 15 in 52146 Würselen gemäß Art. 32 Abs. 1 EU-DSGVO für Verantwortliche (Art. 30 Abs. 1 lit. a) und Auftragsverarbeiter (Art. 30 Abs. 2 lit. b) inkl. der Einwahltechnik auf das netgo-RZ:

Eine Änderung der getroffenen technischen und organisatorischen Maßnahmen behält sich netgo vor, sofern das Schutzniveau nach EU-DSGVO nicht unterschritten wird.

1. **Pseudonymisierung**
   Grundsätzlich können Daten mit einem Pseudonym, d.h. einem nicht personenbezogenen Namen, einer Nummer oder Ähnlichem versehen werden, welches eine Zuordnung erschwert. Wichtig für eine wirksame Pseudonymisierung ist dabei, dass die pseudonymisierten Daten ohne Hinzuziehung zusätzlicher Informationen keine Zuordnung erlauben. Als Auftragsverarbeiter trifft netgo keine Maßnahmen zur Pseudonymisierung, es sei denn, dass der Auftraggeber netgo hierzu beauftragt oder wenn sich eine Pseudonymisierung aus den jeweiligen Leistungsbeschreibungen der Produkte / Dienstleistungen von netgo ergibt.

2. **Verschlüsselung**
   Daten können verschlüsselt werden. Hierbei wird die Information mit Hilfe eines kryptografischen Verfahrens in eine nicht leserbare Zeichenfolge verwandelt. Bei der Nutzung der Verschlüsselung bleibt der Personenbezug der Daten erhalten. Die Daten werden jedoch auf Basis von mathematischen Algorithmen so verändert, dass sie ohne Kenntnis des zugehörigen Schlüssels mit der aktuell verfügbaren Technik nicht lesbar gemacht werden können.

   Zur Verschlüsselung setzt netgo für den elektronischen Transport Verschlüsselungsverfahren ein, die dem Stand der Technik entsprechen und ein Schutzniveau erreichen, das den Anforderungen z.B. von Berufsgeheimnisträgern (wie Steuerberatern, Wirtschaftsprüfern, Rechtsanwälten, Ärzten usw.) angemessen ist.

   Dies sind für den elektronischen Transport zwischen Rechenzentrum

   - und dem Verantwortlichem: über VPN- oder TLS-Verbindung mit Zertifikaten oder Zwei-Faktor-Authentifikation abgesichert
   - und Einzelpersonen: abgesichert mit Verschlüsselungsverfahren nach dem Stand der Technik
   - und Mitarbeitern von netgo Verschlüsselte Verbindung mit Zertifikaten oder Zwei-Faktor-Authentifikation.

   Mobile Endgeräte der netgo-Mitarbeiter (Smartphones, Tablets, Notebooks) werden – sofern hier personenbezogene Daten verarbeitet werden – verschlüsselt und mit Passwort, Fingerabdruck oder Pin geschützt.

3. **Sicherstellung der Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste**
   Maßnahmen sollen die Vertraulichkeit der verwendeten Systeme & Dienste schützen. Es soll verhindert werden, dass es zu unbefugter oder unrechtmäßiger Verarbeitung kommt. Hierunter fallen Maßnahmen, welche den Zutritt, Zugang und Zugriff auf Systeme und Dienste regeln (Beispiele: Bauliche Maßnahmen, Zugangskontrollen, Zugriffsrechte, Alarmanlagen). Ebenso soll die Integrität der Systeme geschützt werden. Daten sollen stets richtig und verlässlich sein und dürfen nicht unbeabsichtigt oder schadhaft geändert oder zerstört werden können.

   3.1. Vertraulichkeit
   Unbefugten ist der Zutritt zu den Datenverarbeitungs-, Datenspeicherungs-, Netzwerk- und Telekommunikationsanlagen (Sprache, Daten), mit denen Daten im Auftrag verarbeitet werden, zu verwehren. Die Vertraulichkeit von Systemen (Hardware) und Diensten (Software) setzt im Rahmen der Verarbeitung zwingend ein Zugriffskonzept voraus, das mit Gruppen- und Benutzerrechten arbeitet und den Zugriff auf einzelne Daten im Rahmen der Verarbeitung abhängig von den erforderlichen Prozessen ermöglicht. Hierzu gehören auch Maßnahmen der Zutrittskontrolle, der Zugangskontrolle und der Zugriffskontrolle.

Alle im Auftrag verarbeiteten Daten des Auftraggebers werden grundsätzlich im netgo-Rechenzentrum gespeichert.

3.1.1. Benutzer-/Rechteverwaltung – Authentifizierung

netgo hat für am IT-System zugelassene Benutzer und angelegte Benutzergruppen Rechteprofile erstellt. In Anlehnung an die Maßnahme M 2.31 des BSI IT-Grundschutz (Dokumentation der zugelassenen Benutzer und Rechteprofile) umfasst dies insbesondere folgende Angaben:

1) Rechtevergabe an zugelassene Benutzer

- zugeordnetes Rechteprofil (in Einzelfall mit Abweichungen vom verwendeten Standard-Rechteprofil)
- Begründung für die Wahl des Rechteprofils und gegebenenfalls der Abweichungen
- Zuordnung des Benutzers zu einer Organisationeinheit mit Zeitpunkt und Grund der Einrichtung
- Befristung der Einrichtung / Löschen der Benutzergruppen

2) Rechtevergabe an zugelassene Gruppen

- Zugehörige Benutzer
- Zeitpunkt der Einrichtung
- Befristung der Einrichtung

3.1.2. Zutrittskontrolle

- Das Gebäude (Standort des Firmensitzes Carlo-Schmid-Str. 15, 52146 Würselen) ist außerhalb der Arbeitszeit verschlossen.
- Damit sich Besucher zu jeder Zeit anmelden können ist der Empfang während der Arbeitszeiten durchgehend von 08:00 Uhr bis 17:00 Uhr (Freitags von 08:00 Uhr bis 16:00 Uhr) besetzt
- Das gesamte netgo-Gebäude ist durch eine Alarmanlage, die an einen Wachdienst aufgeschaltet ist, gesichert.
- Im Gebäude erfolgt eine Videoüberwachung für den Zugang zum Rechenzentrum und das Rechenzentrum selber.
- Alle Personen müssen sich am Empfang anmelden. Vor Einlassgewährung wird Rücksprache mit dem Besuchten gehalten. Der Besucher wird am Empfang abgeholt und wird stets von einem netgo-Mitarbeiter begleitet.
- Alle Besucher müssen einen Besuchsschein ausfüllen. Der Besucherschein ist formularmäßig gestaltet und besteht aus zwei Spalten, die auszufüllen sind. Die beiden linken Textfelder sind vom Besucher, die drei rechten Textfelder vom Betrieb auszufüllen. Der Durchschlag wird dabei nicht mitabgegeben, sondern am Empfang vorgehalten, bis der dazugehörige Besucherschein nach Beendigung des Besuchs wieder abgegeben wurde.
- Jeder Besucher ist beim Betreten des Gebäudes vom Empfangsmitarbeiter über die Verhaltensregeln im Betrieb aufzuklären. Dem Besucher ist die Besucherordnung auszuhändigen, die mit Unterschrift des Besucherscheins (s. Anlage 1, Feld 1) zur Kenntnis genommen wird.
- Nachdem der besuchte Mitarbeiter den Gast zurück zum Empfang begleitet hat, füllt dieser noch das mittlere Kästchen auf der rechten Seite des Besucherscheines aus und übergibt den Schein an den Empfangsmitarbeiter. Dieser vervollständigt das letzte Kästchen, verabschiedet den Besucher und heftet den Schein dann zusammen mit dem dazugehörigen Durschlag in einen dafür vorgesehenen Aktenordner.
- Das Grundstück (Carlo-Schmid-Str. 15, 52146 Würselen) ist außerhalb der Geschäftszeiten außerdem mit einer Torschließanlage verschlossen.
- Der Zutritt zum netgo-Rechenzentrum ist nur speziell autorisierten Mitarbeitern von netgo gestattet.
- Die Geschäftsleitung von netgo prüft periodisch die Notwendigkeit von Zutrittsberechtigungen für die Mitarbeiter.

3.1.3. Zugangskontrolle

1) Zunächst greifen alle Maßnahmen der voran beschriebenen Zutrittskontrolle.

2) Alle Rechner (Arbeitsplatz-PC's, Server, Tablets, Smartphones usw.) bei netgo verfügen mindestens über ein Zugangskontrollsystem (UserID, Passwort). Es gibt vorgeschriebene Regeln zur Passwortvergabe. Dies betrifft die notwendige Komplexität, die Lebensdauer des Passwortes sowie die Wiederverwendung alter Passwörter.

3) Zur Prüfung der Wirksamkeit der Absicherungsmaßnahmen werden bei sensiblen Systemen in Zeitabständen Penetrationen durchgeführt.

4) Arbeitsplatz-PC-Sicherheit:

- Benutzerkennung mit mindestens 8-stelliger Passwortvergabe. Jeder User bekommt eine eigene Benutzerkennung mit eigenem Passwort. (Netzwerk Authentifizierung).
- Automatische passwortgeschützte Bildschirm- und PC-Sperren.
- Alle Mitarbeiter von netgo werden kontinuierlich angewiesen, ihre PC's bei kurzzeitigem Verlassen des Arbeitsplatzes zu sperren. Die Einhaltung dieser Anweisung wird strengstens überwacht.
- Für alle Remote-Zugänge bei netgo geschieht der Zugang grundsätzlich mit einer 2-Faktor-Autorisierung.

5) Zugangskontrolle zu Systemen zur Auftragsbearbeitung:

- Die zur Benutzung von IT-Systemen Berechtigten dürfen ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen.
- Im Auftrag verarbeitete Daten dürfen bei der Verarbeitung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden.
- Die eingesetzten IT-Systeme haben ein dediziertes Rechtesystem, welche es ermöglicht, Datenzugriffe und -veränderungen auf Basis von Rollen und individuellen Berechtigungen zu vergeben.
- Es gibt vorgeschriebene Regeln zur Passwortvergabe.

3.1.4. Zugriffskontrolle

- Innerhalb des hausinternen netgo-Firmennetzwerks werden für verschiedene User unterschiedliche Berechtigungsrollen vergeben. So wird gewährleistet, dass ein Nutzer nur auf solche Verzeichnisse oder Bereiche Berechtigungen erhält, die er auch sehen darf.
- Jeder Mitarbeiter kann im Rahmen seiner Aufgabenerfüllung nur auf die für seine Tätigkeit notwendigen Systeme und mit der ihm zugewiesenen Berechtigung auf die erforderlichen Daten zugreifen.
- Zusätzlich ist das netgo -Firmennetzwerk in differenzierte hausinterne Netzsegmente eingeteilt. User können folglich nicht auf bestimmte Server zugreifen.

3.1.5. Zugriff auf das Rechenzentrum

- Der Zugriff erfolgt nur über VPN-Verbindungen.
- Die Datenübertragung zwischen netgo und den lokalen Netzen der Auftragnehmer oder anderen Kommunikationspartnern erfolgt grundsätzlich verschlüsselt. Unter der „Leistungsbeschreibung aixGate-Gateway" unter www.netgo.de/Kundenbereich befindet sich die Beschreibung für diese VPN-Verbindung.
- Auf die Server der Auftraggeber im netgo-Rechenzentrum, im Rahmen der Auftragsverarbeitung, kann von den netgo -Mitarbeitern über das netgo -Firmennetzwerk nicht direkt zugegriffen werden. Hier erfolgt der Zugriff immer über eine dazwischengeschaltete Sicherheits-Ebene (Admin-Server). Hier werden auch alle Zugriffe kontinuierlich protokolliert und die Zugriffe von der netgo -Geschäftsleitung turnusmäßig stichprobenartig anhand der erteilten Auftragsverarbeitungs-Aufträge und den Einträgen im Ticket-System überprüft.

- Die IT-Systeme von netgo werden kontinuierlich auf die Wirksamkeit eingesetzter Maßnahmen gegen das Eindringen seitens unbefugter Dritter getestet.

3.1.6. Sicherheitsmaßnahmen bei Fernwartung

- Der Aufbau der Fernwartungsverbindung darf nur durch den Auftraggeber erfolgen; Fernwartungsarbeiten dürfen nur mit seiner Zustimmung begonnen werden.
- netgo darf von den eingeräumten Zugriffsrechten nur in dem für die Durchführung der Fernwartungsarbeiten unerlässlich notwendigen Umfang Gebrauch machen.
- netgo darf personenbezogene Daten nur dann vom DV-System des Auftraggebers herunterladen und auf den eigenen Systemen speichern, wenn zuvor die Erlaubnis des Auftraggebers in Textform vorliegt.
- Der Auftraggeber ist berechtigt, die Fernwartungsarbeiten von einem Kontrollbildschirm aus zu verfolgen und jederzeit abzubrechen.
- netgo muss personenbezogene Daten, die bei der Fernwartung übermittelt wurden, unverzüglich löschen oder dem Auftraggeber zurückgeben, wenn sie für die Durchführung der Fernwartungsarbeiten nicht mehr erforderlich sind.

3.2. Integrität

Das Risiko physischer, materieller oder immaterieller Schäden bzw. das Risiko der Beeinträchtigung der Rechte und Freiheiten für betroffene Personen durch unbeabsichtigte oder unbefugte Veränderung oder unrechtmäßiges oder fahrlässiges Handeln von im Auftrag verarbeiteten Daten ist zu reduzieren. Die Integrität ist neben der Verfügbarkeit und Vertraulichkeit eines der drei klassischen Ziele der Informationstechnologie. Die Integrität von Systemen und Diensten erfordert die Absicherung gegen Manipulationen.

Dazu zählen:

- die Wahrung der referentiellen Sicherheit in Datenbanken
- die Protokollierung von Änderungen
- das Durchführen von Plausibilitätsprüfungen
- die Verhinderung von der Eingabe von ungültigen Werten
- die Verhinderung der ungewollten Löschung, Überschreibung oder Änderung von Daten

Es ist sicherzustellen, dass Programme und Daten nicht verfälscht und/oder falsche Daten verarbeitet werden, damit sie nicht unbemerkt fehlerhafte Ergebnisse erzeugen oder Funktionen ausführen, die nicht erwünscht sind.

netgo hat mit den Herstellern der eingesetzten Komponenten im Rechenzentrum und den Internet-Anbindungs-Providern grundsätzlich Service-Level-Agreements (SLA) geschlossen. Hierbei werden von den Herstellern/Providern netgo laufend bekannte Schwachstellen gemeldet, um geeignete Maßnahmen zur Risikoreduzierung und Fehlerbehebung zu treffen.

Die persönliche Verantwortung jedes netgo-Mitarbeiters für die Sicherheit, Vertraulichkeit, Integrität und Verfügbarkeit von Daten und Informationen wird bei netgo durch jährliche Schulungsmaßnahmen, weitergehende Seminare und zentral bereitgestellte Informationen gestärkt.

In den Sicherheitsbereichen des netgo-Rechenzentrums gilt ein grundsätzliches Fotografierverbot, es wird von den Führungskräften und vom Sicherheitsdienst überwacht.

Für den Sicherheitsbereich des netgo-Rechenzentrums haben nur wenige, besonders autorisierte Mitarbeiter Zutritt. Jeder Zutritt wird protokolliert.

3.2.1. Weitergabekontrolle

netgo stellt sicher, dass personenbezogene Daten bei der elektronischen Übertragung, beim Transport oder bei der Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder gelöscht werden können. Hierzu wählt netgo geeignete Maßnahmen wie Verschlüsselung o.Ä. bei Transport, Übertragung und Übermittlung oder Speicherung auf Datenträger.

Sicherung bei der elektronischen Übertragung:

- Bei der elektronischen Übertragung von Auftragnehmerdaten in das netgo-Rechenzentrum sind alle Verbindungen über einen VPN-Tunnel verschlüsselt.
- Die elektronische Übertragung von Auftragnehmerdaten in das netgo-Rechenzentrum wird protokolliert.
- Bevor die elektronische Übertragung stattfindet, wird geprüft, ob diese zulässig ist.

Sicherung bei der Lagerung und Transport:

- Es besteht ausreichender Zugriffsschutz zwischen dem Speichern der Daten auf den Datenträgern und dem Transport. Die Datenträger liegen in Würselen in einem gesicherten Raum und dort in Datensicherungsschränken, die nur Mitarbeiter mit einer entsprechenden Berechtigung zugänglich sind.
- Der Transport von Sicherungsdatenträgern wird ausschließlich durch eigene netgo-Mitarbeiter in verschlossenen speziellen Transportboxen durchgeführt. Der Transport bzw. Transportweg wird in einem Protokoll festgehalten.
- Alle Datenexporte verlassen das Unternehmen nur verschlüsselt.
- Datenexporte werden durch das Vier-Augen-Prinzip geprüft

3.2.2. Eingabekontrolle

Maßnahmen zur Gewährleistung der nachträglichen Überprüfung und Nachvollziehbarkeit der Datenverwaltung und -pflege, insbesondere hinsichtlich Eingabe, Veränderung oder Löschung von Daten.

Bei der Erfassung von Kundendaten werden folgende Maßnahmen umgesetzt:

- netgo erfasst nur Kundendaten, die auftragsrelevant sind.
- Protokollierung der Eingabe, Änderung und Löschung von Daten
- Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)
- Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts
- Erstellung einer Übersicht, aus der sich ergibt, mit welchen Applikationen welche Daten eingegeben, geändert und gelöscht werden können.

3.2.3. Auftragskontrolle

Ziel der Auftragskontrolle ist es, zu gewährleisten, dass personenbezogene Daten lediglich entsprechend den Weisungen des jeweiligen Auftraggebers verarbeitet werden.

netgo hat hierzu die folgenden Maßnahmen festgelegt:

- Schriftliche Vereinbarungen und Verträge
- Klare Abgrenzung der Kompetenzen und Pflichten zwischen netgo und Auftraggeber
- Festlegung der Sicherheitsmaßnahmen
- Weisungsbefugnisse eindeutig definiert
- Vor-Ort-Kontrollen
- Verpflichtung der Mitarbeiter des Auftragnehmers auf das Datengeheimnis (§ 5 BDSG)
- Vereinbarungen zur Auftragsverarbeitung nach Art. 28 der EU-DSGVO
- Bestellung eines Datenschutzbeauftragten

3.2.4. Trennungskontrolle

Es ist sicher zu stellen, dass personenbezogene Daten, die zu unterschiedlichen Zwecken erhoben wurden, getrennt verarbeitet werden können.

Stichpunktartig hier die wichtigsten Maßnahmen, die netgo umgesetzt hat:

- Trennung von Produktiv- und Test-System
- Getrennte Ordnerstrukturen (Mandantenfähigkeit)
- Getrennte Tables in der Datenbank
- Getrennte Datenbanken
- Getrennte Server

3.2.5. Löschen von Daten

Personenbezogene Daten dürfen nur so lange gespeichert werden, wie es die Zwecke, für die sie verarbeitet werden, erforderlich machen. Die Leistungsbeschreibungen von netgo für Produkte und Dienstleistungen – einsehbar unter www.netgo.de/Kundenbereich – die Kundenaufträge (Auftragsbestätigungen von netgo) und die Vereinbarungen zur Auftragsverarbeitung nach Art. 28 der EU-DSGVO mit den Auftraggebern sehen hier verschiedene Löschkonzepte vor.

1) Vernichtung von Datenträgern:
Datenträger werden zentral in eigens hierfür vorgehaltene verschlossene spezielle Behälter bei netgo zwischengelagert und nach spätestens 6 Monaten nach DIN-66399 („Büro- und Datentechnik – Vernichtung von Datenträgern Teil 3: Prozess der Datenträgervernichtung, Februar 2013" nach Schutzklasse 3 und Sicherheitsstufe 4) von einem externen Entsorger Datenschutzkonform vernichtet, mit dem netgo eine Vereinbarung zur Auftragsverarbeitung nach Art. 28 EU-DSGVO hat.

2) Vernichtung von Schriftstücken:
Papierbezogene Akten werden nach DIN-66399 bzw. DIN-EN-15713 zertifiziert vernichtet.
Die Löschung von Kundendaten auf ASP-, IaaS- und Server-Housing-Systemen oder bei Cloud-Speicher-Lösungen liegt in der Verantwortung der Auftraggeber und wird von netgo nur nach ausdrücklicher schriftlicher Weisung durchgeführt. Die Aufbewahrungsfristen der Daten werden im Rahmen der vertraglichen Beauftragung durch den Kunden vorgegeben bzw. ergeben sich aus den gesetzlichen Aufbewahrungsfristen.

3.2.6. Mandantentrennung

Zu unterschiedlichen Zwecken erhobene Daten werden getrennt verarbeitet. Daten von Auftraggebern werden im Rahmen der Auftragsverarbeitung getrennt verarbeitet, verwaltet und logisch getrennt.

3.2.7. Protokollierung

Die Verarbeitung von im Auftrag verarbeiteten Daten werden grundsätzlich protokolliert.
Die Dateneingabe und die Verarbeitung der im Auftrag verarbeiteten Daten erfolgen ausschließlich nach dem mit dem Auftraggeber festgelegten Verfahren.

3.3. Verfügbarkeit

Das Glossar des IT-Grundschutzkataloges des BSI definiert Verfügbarkeit wie folgt:

„Die Verfügbarkeit von Dienstleistungen, Funktionen eines IT-Systems, IT-Anwendungen oder IT-Netzen oder auch von Informationen ist vorhanden, wenn diese von den Anwendern stets wie vorgesehen genutzt werden können."

Gemeint ist damit die jederzeitige Betriebsbereitschaft von Systemen und Diensten im Sinne der Sicherstellung einer jederzeitigen Nutzbarkeit.

netgo stellt sicher, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt werden.

Alle Alarmierungspläne, Handlungsanweisungen, Notfallregelungen sowie Wiederanlaufpläne sind in einem elektronischen Notfallhandbuch festgehalten. netgo führt eine laufende Überwachung der Nutzung der Dienste und der Auslastung der Systeme durch. netgo hat ein Notfallkonzept umgesetzt, das z. B. Maßnahmen zur Abwehr von Angriffen aus dem Internet beinhaltet. Dieses Notfallkonzept wird laufend fortgeschrieben und regelmäßig auf Wirksamkeit geprüft.
Für die IT-Infrastruktur am netgo-Standort (Carlo-Schmid-Str. 15, 52146 Würselen) und im netgo-Rechenzentrum sind hier einige wesentlichen Maßnahmen stichpunktartig genannt:

- Klimaanlagen im Serverraum
- Unterbrechungsfreie Stromversorgung (USV)
- Zugangskonzept für das Gebäude
- Mehrstufiges Backupkonzept
- RAID Verfahren
- Datenübertragung und Datenspiegelung
- Cluster-Betrieb und redundante Systeme
- Alle Server werden live überwacht.
- Die Server- und Storage-Systeme, die Einwahl- und Router-Technik, die Switche und Internet-Anbindungen im netgo-Rechenzentrum sind doppelt, gespiegelt, geclustert oder anderweitig redundant bzw. ausfallgesichert aufgebaut.
- netgo hält Ersatzteile und Ersatzgeräte vor bzw. hat mit Herstellern Subcontractor-Wartungsverträge mit entsprechenden Service-Level-Agreements (SLA) und kurzen Reaktionszeiten, um bei einem Komponentenausfall umgehend einen Not- bzw. Ersatzbetrieb sicherstellen zu können, der geeignet ist, die Rechenzentrumsleistungen grundsätzlich aufrecht zu erhalten.
- Wartungen der Hardware sind Bestandteil der netgo-Grundleistungen bei Server-Housing-, IaaS- und ASP-Verträgen.
- Regelmäßige Wartungen gewährleisten die Betriebsbereitschaft, die Leistungsfähigkeit sowie das Qualitätsniveau der Systeme.
- Das Einspielen von Patches und Hotfixes erfolgt regelmäßig, sobald diese verfügbar sind und nach netgo-interne Tests freigegeben wurden.
- Die Server- und Storage-Systeme im netgo-Rechenzentrum werden durch den Ein-satz von Managed-Service-Softwareagenten permanent überwacht.
- Das Monitoring und das Management der gesamten RZ-Systemlandschaft trägt zum Erhalt der Betriebsbereitschaft sowie der Leistungsfähigkeit der Systeme bei.

Zweckbindung:

- Personenbezogene Daten, die im Auftrag verarbeitet werden, dürfen nur entsprechend den Weisungen des Auftraggebers verarbeitet werden. Dies gilt insbesondere auch für die Löschung von Daten.
- Die Verarbeitung von Auftragsdaten erfolgt ausschließlich entsprechend den produktbezogen Leistungsbeschreibungen bzw. den individuellen Vereinbarungen mit dem Auftraggeber.
- Individuelle Weisungen oder Auskunftsersuchen des Auftraggebers werden nur nach einer verifizierbaren Authentisierung (z. B. Fax mit Unterschrift eines Weisungsbeauftragten) im Rahmen des vereinbarten Leistungsumfangs angenommen.
- Weisungen zur Verarbeitung und insbesondere zur Löschung von im Auftrag verarbeiteten Daten werden nur ausgeführt, wenn der Auftraggeber sie in der vertraglich vorgeschriebenen Form erteilt. Dies gilt besonders für die Neuanlage, das Ändern oder die Deaktivierung von Benutzern und deren Zugriffsrechten auf ein Server-Housing-, IaaS- oder ASP-System von netgo.

3.4. Belastbarkeit

Die Belastbarkeit umfasst u.a., dass Systeme ausreichend dimensioniert sind, um Verarbeitungen ohne Ausfälle und Wartezeiten durchführen zu können. Ebenso ist hiermit die Toleranz eines Systems gegenüber Störungen gemeint, die in der IT allgemein als „Resilienz" beschrieben wird („Resilienz" = die Fähigkeit von technischen Systemen, bei Störungen bzw. Teil-Ausfällen nicht vollständig zu versagen, sondern wesentliche Systemdienstleistungen aufrechtzuerhalten). Dies umfasst auch die Ausfallsicherheit der IT-Systeme und Dienste.
Die für unternehmenskritische Prozesse eingesetzten IT-Systeme sind hochredundant ausgelegt. netgo verfügt über eine skalierbare IT-

Architektur, die eine schnelle und flexible Reaktion auf die Veränderung der Bedingungen durch Verfahren zur Wiederherstellung der Verfügbarkeit personenbezogener Daten nach einem physischen oder technischen Zwischenfall sicherstellt.

An dieser Stelle sei auch auf den Notfallplan der netgo verwiesen. Sämtliche Maßnahmen werden durch permanentes Monitoring überwacht und dokumentiert. Zusätzlich prüft netgo durch regelmäßige Wiederanlauf-Tests die ordentliche Funktionsweise aller getroffenen Maßnahmen. Für netgo -ASP-, IaaS- und Server-Housing-Leistungen weist netgo hier auf die entspr. Leistungsbeschreibungen unter www.netgo.de/Kundenbereich hin. Hier finden sich unter dem Punkt „Verfügbarkeit - Service-Level-Agreements (SLA) und Schadensersatzregelung" detaillierte Ausführungen zur Belastbarkeit von Rechenzentrums-Leistungen.

Für die Anbindung von lokalen Kunden-Netzwerken an das Internet bietet netgo den abgesicherten Internet-Zugang aixGate an. Bei aixGate sorgt eine Vielzahl von Mechanismen für die Absicherung gegen Gefahren aus dem Internet (z.B. Proxy-Systeme, Firewalls, Viren-Scanner, Filter-Systeme usw.). Unter www.netgo.de/Kundenbereich „Leistungsbeschreibung aixGate – der abgesicherte Internet Zugang" finden Sie weitere Informationen hierzu.

4. Wiederherstellbarkeit

Als weitere technische Maßnahme beschreibt Art. 32 Abs. 1 lit. c) DSGVO die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen.

Das Risiko physischer, materieller oder immaterieller Schäden bzw. das Risiko der Beeinträchtigung der Rechte und Freiheiten auch durch unrechtmäßiges oder fahrlässiges Handeln für betroffene Personen durch Vernichtung, Verlust, Veränderung oder unbefugte Offenlegung von im Auftrag verarbeiteten Daten oder des unbefugten Zugangs zu diesen durch einen physischen oder technischen Zwischenfall ist zu reduzieren.

netgo hat hierzu u.a. folgende Maßnahmen etabliert:

- Sicherung der Installationen (Bare-Metal-Recovery)
- Sicherung der Daten
- Sicherung von Systemdateien und Datencontainern
- Sicherung von LOG-Dateien
- Sicherung von Benutzerkonten

Siehe hierzu auch „Leistungsbeschreibung Datensicherung im netgo-RZ bei Server-Housing-, IaaS- und ASP-Leistungen" unter www.netgo.de/Kundenbereich.

5. Organisatorische Maßnahmen

Regelmäßige Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen

Es sind Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen und zur Gewährleistung der Sicherheit der Verarbeitung bei netgo etabliert. Der externe Datenschutzbeauftrage, Roland Niessing, hat sich bei seiner Unternehmensdatenschutzanalyse von den oben beschriebenen Maßnahmen überzeugt. Im Zuge der Umstellung auf die EU-DSVGO wird ein regelmäßiges Datenschutzaudit durch den Datenschutzbeauftragten durchgeführt und dokumentiert.

Die Einsicht der Protokolle der Hard- und Software-Komponenten der Infrastruktur gehört zu den täglichen Aufgaben des zuständigen IT-Administrators. Darüber hinaus ist ein System der Benachrichtigung bzw. Alarmierung bei automatisierten Vorgängen eingerichtet.

netgo hat ein Qualitäts-Managementsystem nach DIN ISO 9001:2008 für den Geltungsbereich „Beratung, Vertrieb, Installation, Einführung und Betreuung von komplexen IT-Systemen mit eigenem Hochsicherheits-Rechenzentrum" implementiert und zertifizieren lassen. Durch regelmäßige interne Audits wird die Wirksamkeit der getroffenen Maßnahmen geprüft, um ggf. Maßnahmen weiter zu entwickeln. Zur Aufrechterhaltung des Zertifikats werden regelmäßige Re-Zertifizierungsaudits durchgeführt.