netgo group GmbH

Anlage: Technische und organisatorische Maßnahmen (TOM)

gemäß Art. 32 DSGVO

Versionsnummer: 6.0

Status: freigegeben

Datum: 15.07.2026

Änderungshistorie

Inhaltsverzeichnis

Technische und organisatorische Maßnahmen (TOM)

Nachfolgend befindet sich die Beschreibung der technischen und organisatorischen Maßnahmen (TOM) der netgo group GmbH gemäß Art. 32 Abs. 1 Datenschutz-Grundverordnung (DSGVO) für Verantwortliche und Auftragsverarbeiter. Eine Änderung der getroffenen technischen und organisatorischen Maßnahmen behält sich die netgo group GmbH vor, sofern das Schutzniveau nach DSGVO nicht unterschritten wird.

Die technischen und organisatorischen Maßnahmen gelten ergänzend für alle verbundenen Unternehmen gemäß §§ 15 ff. Aktiengesetz.

1 Grundsätzliches

Die netgo group GmbH (im Weiteren „**netgo group**") hat einen Datenschutzbeauftragten bestellt:

Roland Nießing
E-Mail: datenschutz@netgo.de

Vertretung:
Thorsten Stelter
E-Mail: datenschutz@netgo.de

Die netgo group betreibt ein Datenschutzmanagementsystem (DSMS), um die datenschutzrechtlichen Anforderungen zu steuern und besitzt eine Datenschutzleitlinie, ein Datenschutzkonzept bzw. ein Datenschutzhandbuch zur Regelung und Umsetzung des Datenschutzes im Unternehmen.

Mitarbeitende der netgo group sind zur Wahrung der Vertraulichkeit und zur Einhaltung der datenschutzrechtlichen Anforderungen nach der DSGVO verpflichtet.

Die Datenverarbeitung wird grundsätzlich nur auf dem Gebiet der Bundesrepublik Deutschland bzw. innerhalb der Europäischen Union oder der Staaten des Europäischen Wirtschaftsraums durchgeführt, sofern nicht anders vertraglich geregelt.

Mitarbeitende werden regelmäßig durch Informationen und Schulung in die Anforderungen des Datenschutzes eingewiesen.

1.1 Zertifizierungen

Die netgo group verfügt u. a. über folgende Zertifizierungen:

- Zertifikat ISO27001
- Konformitätsbescheinigung nach ISO27017 Informationssicherheit für Cloud-Dienste
- Konformitätsbescheinigung nach ISO27701 Datenschutz
- Konformitätsbescheinigung nach ISO27018 Datenschutz für Cloud-Dienste

Diese und weitere Zertifikate können auf der Homepage unter www.netgo.de aufgerufen werden.

1.2 Security Operations Center (SOC)

Zum Schutz der IT-Infrastruktur setzt die netgo group ein Security Operations Center (SOC) ein, dass die Systeme in Echtzeit rund um die Uhr überwacht und bei möglichen Vorfällen umgehend reagiert. Es wird eingesetzt, um Anomalien bzw. Angriffe frühzeitig zu erkennen, geeignete Gegenmaßnahmen einzuleiten und die Sicherheit der Verarbeitung personenbezogener Daten gemäß Art. 32 DSGVO zu gewährleisten.
Es dient dem Schutz sämtlicher Schutzziele:

- Vertraulichkeit: Schutz vor unbefugtem Zugriff auf personenbezogene Daten durch Echtzeit-Monitoring und Incident Detection.
- Integrität: Erkennung von Manipulationsversuchen und Schutz vor unautorisierten Änderungen an Daten.
- Verfügbarkeit: Reaktion auf sicherheitsrelevante Vorfälle wie z. B. DDoS-Angriffe zur Aufrechterhaltung des Systembetriebs.

1.3 Einsatz von Künstlicher Intelligenz (KI/AI)

Wir setzen in unserem Unternehmen Systeme der Künstlichen Intelligenz (KI) zur Unterstützung unserer Geschäftsprozesse ein, insbesondere in den Bereichen Kundenservice und Kommunikation, Dokumentenanalyse und -erstellung, Termin- und Organisationsplanung sowie interne Recherche und Wissensmanagement. Die KI-Systeme dienen der Unterstützung der Mitarbeitenden; eine ausschließlich automatisierte Entscheidungsfindung mit rechtlicher Wirkung oder vergleichbarer erheblicher Beeinträchtigung gegenüber betroffenen Personen (Art. 22 DSGVO) findet nicht statt.

Für den Einsatz von KI-Systemen gelten ergänzend zu den nachstehenden Maßnahmen die folgenden technischen und organisatorischen Maßnahmen:

- Einsatz ausschließlich freigegebener und dokumentierter KI-Systeme; die Nutzung 2nicht freigegebener Dienste sowie privater Nutzerkonten ist untersagt.
- Durchführung einer datenschutz- und informationssicherheitsbezogenen Bewertung vor Produktiveinsatz; Prüfung der Erforderlichkeit einer Datenschutz-Folgenabschätzung nach Art. 35 DSGVO im Einzelfall.
- Beschränkung der Verarbeitung und Übermittlung personenbezogener Daten auf das erforderliche Minimum (Grundsatz der Datenminimierung, Art. 5 Abs. 1 lit. c DSGVO; Need-to-know-Prinzip).
- Bevorzugte Verwendung anonymisierter oder pseudonymisierter Daten; Verbot der Eingabe besonderer Kategorien personenbezogener Daten (Art. 9 DSGVO) sowie geheimhaltungsbedürftiger Informationen in nicht hierfür freigegebene Systeme.
- Zugriff auf KI-Systeme ausschließlich über organisationsverwaltete Konten mit rollen- und berechtigungsbasierter Zugriffssteuerung sowie sicherer Authentifizierung.
- Protokollierung sicherheitsrelevanter Verarbeitungsvorgänge im erforderlichen Umfang unter Beachtung des Beschäftigtendatenschutzes.
- Sicherstellung durch vertragliche Vereinbarung (Art. 28 DSGVO), dass eingegebene Daten – insbesondere Kundendaten – nicht zum Training oder zur Weiterentwicklung der KI-Modelle des Anbieters verwendet werden, sofern hierfür keine gesonderte Rechtsgrundlage oder ausdrückliche Weisung besteht.
- Prüfung und Absicherung etwaiger Drittlandübermittlungen (Art. 44 ff. DSGVO) einschließlich fortlaufender Bewertung des Übermittlungsmechanismus.
- Menschliche Aufsicht und Letztkontrolle der KI-Ergebnisse vor deren geschäftlicher Verwendung.
- Regelmäßige Überprüfung der eingesetzten KI-Systeme hinsichtlich Datenschutzes, Informationssicherheit und Compliance sowie Aktualisierung der zugrunde liegenden Verträge und Konfigurationen.
- Einhaltung der Vorgaben der Verordnung (EU) 2024/1689 (KI-VO / „EU AI Act"), der DSGVO und des BDSG sowie der internen KI-Richtlinien der netgo group.
- Dokumentation aller produktiv eingesetzten KI-Systeme einschließlich Zweck, Datenkategorien, Anbieter und Risikobewertung.

2 Vertraulichkeit

2.1 Zutrittskontrolle

Ziel der Zutrittskontrolle ist es, mit Hilfe geeigneter baulicher, technischer, organisatorischer und personeller Maßnahmen zu verhindern, dass Unbefugte Zutritt zu den Datenverarbeitungsanlagen, den zugehörigen Archiven und all den Räumlichkeiten haben, in denen personenbezogene Daten verarbeitet werden.

Je nach Schutzbedarf bzw. den Anforderungen physischer Sicherheit verfügen die Standorte der netgo über unterschiedliche Schutzmaßnahmen. Diese stellen sich wie folgt dar:

- Sämtliche Gebäude der netgo group sind außerhalb der Arbeitszeit verschlossen.
- Zusätzliche Zutrittssicherungen über Zutrittskontrollsystem mit Sicherheitszonen sind eingerichtet.
- Je nach Schutzbedarf sind verfügen die Standorte über eine Alarmanlage und sind teilweise mit Videoüberwachung gesichert.
- Verfahren zur Besucherführung über den Empfang.
- Es existieren geregelte Prozesse zur Zutrittsverwaltung und der Dokumentation der Zutrittsberechtigungen.

Für Standorte von Rechenzentren der netgo existieren zusätzlich folgende Maßnahmen:

- Absicherung mit einer Alarmanlage mit Aufschaltung zum Wachdienst
- Das Gebäude ist in den Eingangsbereichen und in kritischen Zonen mit Videoüberwachungsanlagen ausgestattet.
- 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 group-Mitarbeitenden begleitet.
- Das Grundstück ist außerhalb der Geschäftszeiten außerdem mit einer Torschließanlage verschlossen.
- Der Zutritt zu netgo group Rechenzentren ist nur speziell autorisierten Mitarbeitenden der netgo group gestattet.
- Die Standortleitung prüft periodisch die Notwendigkeit von Zutrittsberechtigungen für die Mitarbeitenden.

2.2 Zugangskontrolle

Ziel der Zugangskontrolle ist es, mit Hilfe geeigneter Maßnahmen das Eindringen in und die Nutzung von Datenverarbeitungssysteme durch Unbefugte zu verhindern.

- Folgende Zugangskontrollen zum Desktop und zu den vernetzten Systemen sind eingerichtet:
  - Userkennung
  - Sicheres Passwort
  - Passwortwiederholungssperre
- Für alle Zugriffsebenen (Netz, Server, Anwendungen) bestehen Passwortregeln zur Gewährleistung eines sicheren Passwortes.
- Für Remote-Zugänge wird grundsätzlich eine Mehrfaktor-Authentifizierung (MFA) eingesetzt.
- Die Einhaltung dieser Regeln wird auf allen Ebenen bei der Eingabe automatisiert kontrolliert.
- Es ist eine zeitgesteuerte passwortgeschützte Pausenhaltung (Bildschirmschoner) eingerichtet.
- Alle Mitarbeitende der netgo group werden kontinuierlich angewiesen, ihre PC's bei kurzzeitigem Verlassen des Arbeitsplatzes zu sperren.
- Folgende Maßnahmen sind gegen unbefugtes Eindringen in vernetzten Systemen umgesetzt:
  - Firewall
  - Virenscanner
  - Benutzung des internen Netzwerks ist nur nach interner Freischaltung möglich

2.3 Zugriffskontrolle

Ziel der Zugriffskontrolle ist zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten –unabhängig vom Speichermedium –bei der Verarbeitung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

- Es besteht ein Berechtigungsprofil, das sicherstellt, dass jeder Mitarbeitende nur über die Zugriffsbefugnisse verfügt, die er zur Aufgabenerledigung benötigt.
    - differenziert nach Leseberechtigung und Schreibberechtigung
- Sämtliche festgelegten Berechtigungen sind nachvollziehbar dokumentiert durch ein Benutzerkonzept.
- Es sind Regelungen eingerichtet, die bei einer Veränderung des Aufgabengebietes eine zeitnahe Aufhebung nicht mehr benötigter Rechte sicherstellt.
- Zusätzlich werden sicherheitskritische Vorfälle protokolliert und ausgewertet.

2.3.1 Benutzer-/Rechteverwaltung

Die netgo group hat für am IT-System zugelassene Benutzer und angelegte Benutzergruppen Rechteprofile erstellt. Dies umfasst insbesondere folgende Angaben:

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 Organisationseinheit mit Zeitpunkt und Grund der Einrichtung
- Befristung der Einrichtung / Löschen der Benutzergruppen

Rechtevergabe an zugelassene Gruppen

- Zugehörige Benutzer
- Zeitpunkt der Einrichtung
- Befristung der Einrichtung

2.3.2 Zugriff auf das Rechenzentrum

- Der Zugriff erfolgt nur über VPN-Verbindungen oder anderer ZTNA-Lösungen.
- Die Datenübertragung zwischen der netgo group und den lokalen Netzen der Auftragnehmer oder anderen Kommunikationspartnern erfolgt grundsätzlich verschlüsselt.
- Auf die Server der Auftraggeber im netgo group Rechenzentrum, im Rahmen der Auftragsverarbeitung, kann von den netgo group Mitarbeitenden über das netgo group Firmennetzwerk nicht direkt zugegriffen werden. Hier erfolgt der Zugriff immer über eine dazwischengeschaltete Sicherheits-Ebene (Admin-Server).

2.3.3 Sicherheitsmaßnahmen bei Fernwartung

- Der Aufbau der Fernwartungsverbindung darf nur durch den Auftraggeber erfolgen; Fernwartungsarbeiten dürfen nur mit seiner Zustimmung begonnen werden.
- Die netgo group darf von den eingeräumten Zugriffsrechten nur in dem für die Durchführung der Fernwartungsarbeiten unerlässlich notwendigen Umfang Gebrauch machen.
- Die netgo group 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.
- Die netgo group 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.

2.4 Pseudonymisierung

Personenbezogene Daten können in einer Weise verarbeitet werden, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden.

Als Auftragsverarbeiter trifft die netgo group keine Maßnahmen zur Pseudonymisierung, es sei denn, dass der Auftraggeber die netgo group hierzu beauftragt oder wenn sich eine Pseudonymisierung aus den jeweiligen Leistungsbeschreibungen der Produkte / Dienstleistungen der netgo group ergibt.

2.5 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 die netgo group 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 der netgo group

- und dem Verantwortlichem: über VPN- oder TLS-Verbindung mit Zertifikaten abgesichert.
- und Einzelpersonen: abgesichert mit Verschlüsselungsverfahren nach dem Stand der Technik.
- und Mitarbeitenden: verschlüsselte Verbindung mit Zertifikaten.

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

2.6 Trennungskontrolle

Ziel der Trennungskontrolle ist es, zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten grundsätzlich auch getrennt verarbeitet werden können.

U.a. werden folgende Maßnahmen umgesetzt:

- Trennung von Produktiv- und Test-System
- Logische und/oder physische Trennung
- Getrennte Tables in der Datenbank
- Getrennte Datenbanken
- Getrennte Server

2.7 Mandantentrennung

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

3 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.

Die netgo group 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 der netgo group laufend bekannte Schwachstellen gemeldet, um geeignete Maßnahmen zur Risikoreduzierung und Fehlerbehebung zu treffen.

3.1 Weitergabekontrolle

Ziel der Weitergabekontrolle ist es, mit Hilfe geeigneter Maßnahmen zu gewährleisten, dass personenbezogene Daten während der elektronischen Übertragung oder während des Transports oder ihrer Speicherung auf Datenträgern nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

- Sensible Daten werden bei ihrer Übertragung vor unbefugter Kenntnisnahme geschützt.
- Datenübermittlungen werden nachvollziehbar protokolliert und kontrolliert.
- Schnittstellen von PCs und externe Laufwerke (mobile Festplatten, USB-Sticks etc.) sind gegen Missbrauch geschützt.
- Die sichere Nutzung mobiler Datenträger ist durch folgende Punkte geregelt:
    - Für den Transport mit Informationen gelten die Vorgaben der Richtlinie „Dokumentenlenkung“.
    - sichere Löschung von Datenträgern
    - Beauftragung eines externen Dienstleisters zur Vernichtung von Datenträgern.
- Bei Fernwartung erfolgt der Zugriff auf die Kundendaten und Kundensysteme nur über sichere Leitungen:
    - VPN
    - Verschlüsselung
- Bei Fernwartung ist eine sichere Identifizierung / Authentifizierung gewährleistet:
    - Es werden nur Fernwartungstools genutzt, welche eine Verschlüsselung nach Stand der Technik haben.
    - zufällige Kennwörter für den einmaligen Zugriff.

Bei Fernwartungen werden die Leitungen durch geeignete Sicherheitseinrichtungen, z. B. Protokollierung und Protokollauswertung überwacht.

3.2 Eingabekontrolle

Ziel der Eingabekontrolle ist es, mit Hilfe geeigneter Maßnahmen sicherzustellen, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

Bei der Erfassung von Kundendaten werden folgende Maßnahmen umgesetzt:

- Die netgo group 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.

3.3 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.

3.4 Löschen von Daten

Personenbezogene Daten dürfen nur so lange gespeichert werden, wie es die Zwecke, für die sie verarbeitet werden, erforderlich machen.

Die Leistungsbeschreibungen der netgo group für Produkte und Dienstleistungen, die Kundenaufträge und die Vereinbarungen zur Auftragsverarbeitung nach Art. 28 der DSGVO mit den Auftraggebern sehen hier verschiedene Löschkonzepte vor.

- Vernichtung von Datenträgern:
  - Datenträger werden in eigens hierfür vorgehaltene verschlossene spezielle Behälter zwischengelagert und nach spätestens 6 Monaten nach ISO/IEC 21964 von einem externen Entsorger datenschutzkonform vernichtet, mit dem die netgo group eine Vereinbarung zur Auftragsverarbeitung nach Art. 28 DSGVO hat.

- Vernichtung von Daten:
  - Papierbezogene Akten werden nach ISO/IEC 21964 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 der netgo group 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.

4 Verfügbarkeit und Belastbarkeit

Zur Sicherstellung der Verfügbarkeit von Systemen und Diensten sind Maßnahmen zu ergreifen, die diese vor inneren und äußeren Einflüssen schützen. Im Falle einer Verletzung der Datensicherheit oder der Sicherheit eines Systems, das personenbezogene Daten verarbeitet, müssen Maßnahmen getroffen werden, die den Verantwortlichen in die Lage versetzen, die Verfügbarkeit der personenbezogenen Daten sowie den Zugang zu ihnen schnellstmöglich wiederherzustellen.

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

Alarmierungspläne, Richtlinien, Notfallregelungen sowie Wiederanlaufpläne sind in einem Notfallhandbuch festgehalten. Die netgo group führt eine laufende Überwachung der Nutzung der Dienste und der Auslastung der Systeme durch. Dieses Notfallhandbuch wird laufend fortgeschrieben und regelmäßig auf Wirksamkeit geprüft.

Für die IT-Infrastruktur der netgo group sind hier die wesentlichen Maßnahmen stichpunktartig genannt:

- Redundante und ausfallsichere Infrastruktur: Server, Storage, Router, Switches und Internet-Anbindungen sind doppelt, gespiegelt, geclustert oder anderweitig redundant aufgebaut, um Ausfälle abzufangen.
- Strom- und Klimasicherung: Serverräume sind mit Klimaanlagen ausgestattet und verfügen über unterbrechungsfreie Stromversorgung (USV) zur Sicherstellung des Dauerbetriebs.
- Datenverfügbarkeit durch Backup und Spiegelung: Mehrstufiges Backupkonzept, RAID-Verfahren sowie Datenübertragung und Datenspiegelung gewährleisten Datenintegrität und schnelle Wiederherstellung.
- Monitoring und Wartung: Permanente Überwachung aller Systeme durch Managed-Service-Agenten sowie regelmäßige Wartungen und Patch-Management sichern die Betriebsbereitschaft und Systemqualität.
- Schnelle Reaktion bei Ausfällen: Ersatzteile und -geräte sind verfügbar, ergänzt durch SLA-gestützte Subcontractor-Wartungsverträge für Not- und Ersatzbetrieb bei Komponentenausfall.
- Umfassende Sicherungs- und Wiederherstellungsstrategie, einschließlich Bare-Metal-Recovery, Datensicherung, Sicherung von Systemdateien, Datencontainern, Log-Dateien sowie Benutzerkonten, ergänzt durch etablierte Notfall- und Wiederherstellungspläne zur raschen und geordneten Systemwiederherstellung im Ernstfall.

5 Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

5.1 Datenschutz-Management

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 der netgo group etabliert.

- Ein Datenschutzbeauftragter wurde bestellt.
- Zentrale Dokumentation aller Verfahrensweisen und Regelungen zum Datenschutz mit Zugriffsmöglichkeit für Mitarbeitenden nach Bedarf / Berechtigung.
- Es ist ein Datenschutz- und Informationssicherheits-Team eingerichtet, das Maßnahmen im Bereich von Datenschutz und Datensicherheit plant, umsetzt, evaluiert und Anpassungen vornimmt.
- Alle Mitarbeitenden wurden auf Vertraulichkeit verpflichtet. Es erfolgen hinreichende Schulungen der Mitarbeitenden in Datenschutzangelegenheiten.
- In einer Übersicht werden die Verarbeitungstätigkeiten aufgeführt.
- Verfahren für regelmäßige Kontrollen bzw. Audits wurden implementiert (z. B. im Rahmen einer ISO-Zertifizierung) und durchgeführt.
- Eine Überprüfung der Wirksamkeit der technischen Schutzmaßnahmen wird mindestens jährlich durchgeführt.

5.2 Incident-Response-Management

Es sind Verfahren zu implementieren, die gewährleisten, dass im Fall von Datenschutzverstößen Meldeprozesse ausgelöst werden.

Meldeprozesse für Datenschutzverletzungen nach Art. 4 Ziffer 12 DSGVO gegenüber den Aufsichtsbehörden (Art. 33 DSGVO) sowie gegenüber den Betroffenen (Art. 34 DSGVO) wurden etabliert.

Ein Prozess zur Vorgehensweise zum Umgang mit Sicherheitsvorfällen ist implementiert. Die Vorfälle werden mittels Meldeformular dokumentiert und anschließend durch den DSB bewertet.

5.3 Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen

Privacy by Design / Privacy by Default

Schon bei der Einführung neuer Systeme bzw. bei der Entwicklung von Software wird dafür Sorge getragen, dass dem Grundsatz der Erforderlichkeit schon im Zusammenhang mit Benutzer-Interfaces Rechnung getragen wird. So können Pflichtfelder vorgesehen oder Felder deaktiviert werden.

Sämtliche Systeme bzw. Software unterstützen die Eingabekontrolle z. B. durch Logmechanismen, die eine unveränderliche Speicherung von Änderungen an Daten und Nutzerberechtigungen ermöglicht.

Berechtigungen auf Daten oder Applikationen können flexibel und granular über Rollenkonzepte gesetzt werden.

5.4 Auftragskontrolle

Ziel der Auftragskontrolle ist es zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers erhoben, verarbeitet oder genutzt werden können.

Die netgo group stellt hierzu einen schriftlichen Vertrag zur Auftragsverarbeitung nach Art. 28 DSGVO mit folgenden Inhalten bereit:

- Klare Abgrenzung der Kompetenzen und Pflichten zwischen netgo und Auftraggeber
- Festlegung der Sicherheitsmaßnahmen
- Weisungsbefugnisse eindeutig definiert
- Vor-Ort-Kontrollen
- Verpflichtung der Mitarbeitenden des Auftragnehmers auf die Vertraulichkeit
- Bestellung eines Datenschutzbeauftragten

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 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 group.

netgo group GmbH
Sachsendamm 63-64
10829 Berlin

t. +49 30 224 900
e. info@netgo.de
www.netgo.de