**Informationssicherheit**

# Vorgaben zur Informationssicherheit

## an die Lieferanten der netgo group

Versionsnummer: 1.0

Status: freigegeben

Datum: 31.10.2024

# Änderungshistorie

# Inhaltsverzeichnis

# 1 Zielsetzung

Ziel des vorliegenden Dokumentes ist es, die Anforderungen gemäß Informationssicherheit und Datenschutz für Lieferanten und Dienstleister der netgo group zu definieren.

# 2 Adressaten und Geltungsbereich

Vorgaben dieses Dokuments gelten verbindlich für alle Lieferanten und Dienstleister und deren Subdienstleister, welche für die netgo group GmbH sowie deren Tochter- und Enkelgesellschaften (im Weiteren „**netgo group**" oder „**Auftraggeber**") Leistungen erbringen. Der Geltungsbereich umfasst alle Informationen der netgo group, die im Zuge der Auftragserfüllung zur Verfügung gestellt werden.

# 3 Anforderungen bei Lieferantenbeziehungen

Die netgo group handelt nach einem organisierten Einkaufsprozess. Dieser unterteilt sich in unterschiedliche Beschaffungsbereiche, die demselben Prozess folgen. Alle Lieferantenbeziehungen werden von dem jeweils zuständigen Beschaffungsbereich verwaltet.

## 3.1 Informationssicherheits- und Datenschutzrelevante Lieferanten

Lieferanten oder Dienstleister (im folgenden Dokument auch als **Auftragnehmer** bezeichnet), die *Zugriff* auf vertrauliche Daten, *Zugang* zu kritischen Systemen und/oder *Zutritt* zu vertraulichen Bereichen (siehe Physische Sicherheit) haben, werden innerhalb der netgo group als informationssicherheitsrelevante Lieferanten oder Dienstleister klassifiziert. Insofern auch personenbezogene Daten betroffen sind, ist der Datenschutz ebenfalls zu beachten. Die Feststellung erfolgt in Zusammenarbeit zwischen dem Anforderer auf Seiten der netgo group und dem jeweils zuständigen Auftragnehmer, ggf. in Rücksprache mit dem ISB der netgo group.

Diese Vorgaben zur Informationssicherheit sind durch den Auftragnehmer zur Kenntnis zu nehmen und einzuhalten.

## 3.2 Allgemeine Anforderungen an sicherheitsrelevante Lieferanten

### 3.2.1 Ansprechpartner für den Auftrag und sicherheitsrelevante Themen

Der Auftragnehmer verpflichtet sich, bei einer eventuellen Auftragserteilung, der netgo group unaufgefordert und in Textform eine natürliche Person als Ansprechpartner für alle sicherheitsrelevanten Themen mitzuteilen und Änderungen anzuzeigen.

### 3.2.2 Vertragliche Regelungen zum Datenschutz

Ergänzend zu den in diesem Auftrag genannten Pflichten muss im Falle der Verarbeitung von personenbezogenen Daten ein gesonderter Auftragsverarbeitungsvertrag (AVV) zwischen der netgo und dem Auftragnehmer abgeschlossen werden.

### 3.2.3 Allgemeine Anforderungen an die Informationssicherheit

1. Alle Informationen gelten grundsätzlich als vertraulich.
2. Vertrauliche Informationen sind ausschließlich zur Vorbereitung und Durchführung des gemeinsamen Vorhabens zu verwenden.
3. Die Auftragnehmer dürfen nicht freigegebene Informationen, die ihnen anvertraut oder die ihnen bei der Zusammenarbeit bekannt werden, während der Dauer und nach Beendigung des Vertragsverhältnisses nicht an Dritte offenbaren oder unbefugt für eigene Geschäftszwecke verwerten.

4. Auf Unterlagen eventuell vorhandene Urheber- und / oder sonstige gewerbliche Schutzrechtsvermerke dürfen von den Auftragnehmern nicht entfernt oder auf sonstige Weise unkenntlich gemacht und auf diese Weise bearbeitetes Material darf nicht an Dritte weitergegeben werden.

5. Aus dem Auftragsverhältnis und aus der Bekanntgabe technischer Einzelheiten und Zusammenhänge - gleichgültig, ob hierfür Schutzrechte bestehen oder nicht - können von den Auftragnehmern, die die vertraulichen Informationen erhalten haben, keine Lizenz-, Nachbau-, Nutzungs- oder sonstige Rechte hergeleitet werden.

6. Die Auftragnehmer verpflichten sich, Informationen nur solchen Beschäftigten oder Dritten zu überlassen, die ihrerseits diesen Vorgaben zur Informationssicherheit unterliegen. Sofern zur Auftragserfüllung Dritte erforderlich sind, müssen die Dritten diese Vorgaben zur Informationssicherheit ebenfalls dokumentiert zur Kenntnis nehmen und sich zur Einhaltung verpflichten.

7. Die von der netgo group überlassenen und im Rahmen des Auftragsverhältnisses generierten Daten gehören der netgo group. Sofern die netgo group Daten überlassen, über die zu verfügen sich ein Dritter vorbehalten hat, sind diese Daten im Zweifel so zu behandeln, als gehörten sie der netgo group.

8. Die Auftragnehmer verpflichten sich, die überlassenen Daten der netgo group nach der Erfüllung des abgestimmten Kooperationsvorhabens oder nach Beendigung des Vertragsverhältnisses, sowie bei Nichtzustandekommen, ohne Aufforderung zu löschen. Sind die Daten aus gesetzlichen Gründen länger aufzubewahren, so sind sie nach Ablauf der gesetzlichen Aufbewahrungsfrist zu löschen. Angemessene Löschnachweise sind nach Aufforderung der netgo group zur Verfügung zu stellen. Vertrauliche Informationen, die in routinemäßig elektronisch abgespeicherten Dateien enthalten sind oder aufgrund von Notfallwiederherstellungsprozessen gespeichert werden, müssen nicht gelöscht werden, soweit dies nur mit unverhältnismäßigem Aufwand möglich wäre. Die so erhaltenen Vertraulichen Informationen sind weiterhin vertraulich zu behandeln.

9. Bei einem Verstoß gegen die hier genannten Bestimmungen durch die Auftragnehmer besteht für die netgo group das Recht, die sofortige Herausgabe sämtlicher überlassener vertraulicher Informationen, einschließlich Kopien aller Kopien, Abschriften jeder Art etc., zu verlangen oder den Nachweis der Unbrauchbarmachung einzufordern. Die Auftragnehmer haften in vollem Umfang für Missbrauch und Weitergabe der zur Verfügung gestellten Daten.

10. Sollten einzelne hier genannte Bestimmungen ganz oder teilweise unwirksam oder nichtig sein oder werden, so bleibt die Wirksamkeit der übrigen Bestimmungen hier genannten unberührt. An die Stelle der unwirksamen oder nichtigen Bestimmung tritt diejenige wirksame Bestimmung, die die netgo group und die Auftragnehmer vereinbart hätten, um den gleichen Erfolg zu erzielen. Dies gilt für fehlende Bestandteile entsprechend.

### 3.2.4 Umgang mit Arbeitsmitteln

1. Grundsätzlich sind bei Arbeiten auf Systemen der netgo group ausschließlich die zur Verfügung gestellten Arbeitsmittel (insbesondere Hardware / Software) zu verwenden. Ausnahmen sind nur nach Prüfung und Genehmigung durch den Verantwortlichen des jeweiligen technischen Systems, in dem die beauftragte Maßnahme umgesetzt wird, zulässig.

2. Sollte ein dringender Bedarf, durch eine begründete nachgewiesene Ausnahme, zur Anbindung von fremdem IT-Equipment an das Datennetzwerk (z. B. Ethernet / WLAN oder sonstige IT-Systemschnittstellen der netgo group erforderlich werden, so ist durch den Auftragnehmer stets sicherzustellen, dass:

    - Alle eingesetzten Fremdsysteme (Host inklusive aller virtuellen Maschinen auf dem Host) über einen anerkannten Antivirenscanner mit aktuellen Virensignaturen verfügen und schadcodefrei betrieben werden.

    - Das Betriebssystem über einen zeitgemäßen Status (mit aktivem Support durch den Hersteller / Distributor) und vor allem aktuellen Betriebssystem-Patchstand verfügt.

- Keinerlei Hackertools oder unlizenzierte gehackte Softwarekomponenten zum Einsatz kommen, die die Geschäftsprozesse negativ beeinflussen könnten. Dazu gehören u. a. Netzwerksniffer oder anderweitige Software.
- Über das Fremdsystem darf keine gleichzeitige Weitervernetzung, z. B. über Mobilfunk, möglich sein.
- Das Fremdsystem muss, wie oben beschrieben, vorgezeigt, geprüft und durch die Ansprechpartner der netgo freigegeben werden. Dies muss vor jedem Einsatz erfolgen, da sich die Rahmenbedingungen der Softwareumgebung verändert haben könnten.
- Es darf keinerlei schwachstellenbehaftete Software auf dem Fremdsystem installiert sein.

3. Sicherheitshinweise des Auftraggebers sind zu beachten.
4. Bei begründetem Bedarf kann die Nutzung von E-Mail-Accounts und Internetzugängen über die netgo eigene Domäne gewährt werden. Dazu wird eine Benutzerkennung zur Verfügung gestellt. Die private Nutzung von E-Mail und Internet durch Beschäftigte des Auftragnehmers ist untersagt. Arbeitsmittel der netgo group dürfen nur zur Vertragserfüllung genutzt werden.
    - Externe Accounts sind durch eine gesonderte Kennung explizit erkennbar.
    - Weiterhin ist das gleichzeitige Versenden von E-Mails an alle Teilnehmer im Adressbuch untersagt.
    - Aus Gründen der Datensicherheit für das Netzwerk wird eine Firewall betrieben, die u. a. einen Spam- und Virenscanner und einen Internetadressfilter umfasst. Die Internetzugriffe, auch privater Natur, werden protokolliert und können kontrolliert werden.
    - Downloads von Software sind ausschließlich im Rahmen der Auftragserfüllung zulässig.

## 3.3 Zutritt zu netgo Gebäuden/Räumen

Der physikalische Zutritt zu Arbeitsorten der netgo group wird nur nach Anmeldung und in Gegenwart von Beschäftigten der netgo gewährt. Ausnahmen sind schriftlich festzulegen. Der Zutritt ist gemäß den jeweiligen Vorschriften des Standorts zu beantragen und zu gewähren.

Zutritte zu Sicherheitszonen, insbesondere Personal- und Geschäftsführungsbereiche und Rechenzentren sind zu dokumentieren und bedürfen der Begleitung durch netgo Personal bzw. Ansprechpartnern.

## 3.4 Datensicherheit

### 3.4.1 Zugriff auf Daten des Auftraggebers

Dem Auftragnehmer werden gemäß dem „Prinzip der minimalen Berechtigungsvergabe“ ausschließlich Berechtigungen zugewiesen, die zur Bearbeitung des Auftrags erforderlich sind. Die Berechtigungen dürfen nur für Tätigkeiten genutzt werden, die für die Auftragserfüllung notwendig und mit der Vorhaben- / Projektleitung abgestimmt sind. Die netgo behält sich vor, die Zugriffe des Auftragnehmers zu protokollieren und anlassbezogen auszuwerten.

Es werden weiterhin ggf. Fernzugriffe genehmigt. Der Umfang und die Nutzungsarten werden in den systemspezifischen Festlegungen geregelt oder mit dem Auftragnehmer explizit vereinbart. Die netgo behält sich jedoch vor, die zur Verfügung gestellten Fernzugriffe bei berechtigtem betrieblichem Interesse ohne Vorankündigung zu unterbinden.

### 3.4.2 Verfahren zum Datenaustausch

Daten der netgo group dürfen nur verschlüsselt über die von der netgo zur Verfügung gestellte IT-Infrastruktur ausgetauscht werden.

### 3.4.3 Umgang mit mobilen Datenträgern

Der Einsatz von mobilen Datenträgern ist grundsätzlich untersagt. Sollte die Nutzung dennoch erforderlich sein, ist in jedem Fall eine abgestimmte Verschlüsselung einzusetzen. Dabei sind bei Bedarf nur bereitgestellte USB-Sticks einzusetzen. Ausnahmen sind zu dokumentieren. Betriebsfremde Datenträger dürfen grundsätzlich nicht eingesetzt werden.

### 3.4.4 Datensicherung von Projektierungsständen

Projektierungsstände sind vom Auftragnehmer und in einer gesicherten und abgestimmten Umgebung aufzubewahren.

### 3.4.5 Datenablage beim Auftragnehmer

Der Auftragnehmer hat nachzuweisen, welche seiner Beschäftigten auf die Daten des Auftraggebers zugreifen können.

Der Auftragnehmer verpflichtet sich, geeignete und angemessene technische und organisatorische Maßnahmen zum Schutz der Daten der netgo zu ergreifen. Die netgo behält sich vor, eine Kontrolle dieser Maßnahmen beim Auftragnehmer durchzuführen und nach billigem Ermessen Nachbesserungen zu verlangen.

## 3.5 Verbot eigener nicht beauftragter Aufzeichnungen

Jegliche nicht durch das Auftragsverhältnis legitimierte Aufzeichnungen sind untersagt. Als Aufzeichnungen gelten auch handschriftliche Notizen und Fotos.

## 3.6 Meldepflichten des Auftragnehmers

Bei Bekanntwerden von Verstößen gegen Vorgaben zur Informationssicherheit (auch dritter Personen) oder sonstiger Risiken für den Auftraggeber und dessen Assets oder dessen Kunden verpflichtet sich der Auftragnehmer unaufgefordert zur sofortigen Meldung an den Informationssicherheitsbeauftragten (ISB) der netgo group.

# 4 Bestätigung der Vorgaben zur Informationssicherheit

Hiermit bestätige ich verbindlich für den Auftragnehmer, dass ich dieses Dokument „Vorgaben Lieferanten zur Informationssicherheit“ zur Kenntnis genommen und verstanden habe sowie der Auftragnehmer die Vorgaben einhalten wird und sicherstellen wird, dass Erfüllungsgehilfen diese ebenfalls einhalten bzw. ihre Einhaltung, durch die von mir mit der Auftragserfüllung betrauten Personen sicherstellen werde.

| Name (Rolle) | Datum | Unterschrift |
|---|---|---|
| | | |
| | | |
| | | |

# 5 Geltungsdauer

Dieses Dokument gilt verbindlich ab Vertragsbeginn des Lieferanten oder Dienstleisterverhältnisses mit der netgo