Information security

Information security requirements

for the suppliers of netgo group

Version number: 1.0

Status: freigegeben

Date: 17.10.2025

Change history

Contents

Change history **2**
Contents **2**
1 Purpose **3**
2 Addressees and scope of application **3**
3 Requirements for supplier relationships **3**
3.1 Suppliers relevant to information security and data protection 3
3.2 General requirements for security-relevant suppliers 3
3.2.1 Contact person for the order and security-related topics 3
3.2.2 Contractual regulations on data protection 3
3.2.3 General requirements for information security 3
3.2.4 Handling of work equipment 4
3.3 Access to netgo buildings/rooms 5
3.4 Data security 5
3.4.1 Access to the Customer's data 5
3.4.2 Data exchange procedures 5
3.4.3 Handling of mobile data carriers 5
3.4.4 Data backup of project planning statuses 5
3.4.5 Data storage with the Contractor 5
3.5 Prohibition of own non-commissioned recordings 5
3.6 Reporting obligations of the Contractor 6
4 Confirmation of the information security requirements **6**
5 Period of validity **6**

1 Purpose

The purpose of this document is to define the information security and data protection requirements for suppliers and service providers of netgo group.

2 Addressees and scope of application

The provisions of this document are binding for all suppliers and service providers and their subcontractors who provide services for netgo group GmbH and its subsidiaries and sub-subsidiaries (hereinafter referred to as "**netgo group**" or "**Customer**"). The scope of application includes all information of netgo group provided during order fulfillment.

3 Requirements for supplier relationships

netgo group follows an organized purchasing process. This is divided into different procurement areas that follow the same procedure. All supplier relationships are managed by the responsible procurement department.

3.1 Suppliers relevant to information security and data protection

Suppliers or service providers (also referred to as **Contractors** in the following document) who have *access* to confidential data, *access* to critical systems and/or *access* to confidential areas (see Physical Security) are classified within netgo group as information security relevant suppliers or service providers. Data protection must also be observed insofar as personal data is affected. The determination is made in cooperation between the requestor on netgo group side and the respective responsible Contractor, if necessary in consultation with the ISB of netgo group.

The Contractor undertakes to take note and observe these information security requirements.

3.2 General requirements for security-relevant suppliers

3.2.1 Contact person for the order and security-related topics

The Contractor undertakes to inform netgo group in text form, without being prompted, of a natural person as the contact person for all security-related issues and to notify netgo group of any changes.

3.2.2 Contractual regulations on data protection

Further to the obligations specified herein, a separate order processing agreement (AVV) must be concluded between netgo and the Contractor should personal data be processed.

3.2.3 General requirements for information security

1. All information is considered confidential.
2. Confidential information is to be used exclusively for the preparation and implementation of the joint project.
3. Contractors may not disclose to third parties or use for their own business purposes without authorization any information that has not been released and that has been entrusted to them or that becomes known to them in the course of the collaboration, either during the term of the contractual relationship or after it has ended.
4. Any copyright and/or other industrial property right notices on documents may not be removed or otherwise made unrecognizable by the Contractors and material processed in this way may not be passed on to third parties.
5. No license, reproduction, usage or other rights can be derived from the contractual relationship and from the disclosure of technical details and contexts –regardless of whether industrial property rights exist or not– by the Contractors who have received the confidential information.

6. The Contractor undertakes to provide information only to those employees or third parties who are themselves subject to these information security requirements. If third parties are required to fulfill the order, they also undertake to take note and comply with these information security requirements in documented form.

7. Data provided by netgo group and generated as part of the contractual relationship belongs to netgo group. If netgo group provides data which a third party has reserved the right to dispose of, this data shall be treated in case of doubt as if it belonged to netgo group.

8. Contractors undertake to delete any data provided to netgo group after fulfillment of the agreed cooperation project or after termination of the contractual relationship, as well as upon non-conclusion, without being requested to do so. If the data must be retained for longer periods for legal reasons, it must be deleted after the statutory retention period has expired. Appropriate proof of deletion must be provided to netgo group upon request. Confidential information contained in files that are routinely stored electronically or stored due to disaster recovery processes does not have to be deleted if this would only be possible with disproportionate effort. Confidential information obtained in this way must continue to be treated confidentially.

9. In the event of a breach of the above provisions by the Contractor, netgo group may demand the immediate surrender of all confidential information provided, including copies of all copies, transcripts of any kind, etc., or to demand proof that it has been rendered unusable. Contractors are fully liable for misuse and disclosure of the data provided.

10. Should individual provisions mentioned herein be or become invalid or void in whole or in part, this shall not affect the validity of the remaining provisions mentioned herein. The invalid or void provision shall be replaced by a valid provision which netgo group and the Contractors would have agreed in order to achieve the same result. This applies accordingly to missing components.

3.2.4 Handling of work equipment

1. When working on netgo group systems, only the work equipment provided (in particular hardware/software) may be used. Exceptions may only be allowed after examination and approval by the person responsible for the respective technical system in which the commissioned measure is implemented.

2. Upon an urgent need to connect external IT equipment to the data network (e.g. Ethernet / WLAN or other IT system interfaces of netgo group) due to a justified, proven exception, the Contractor undertakes to ensure that:

    - All third-party systems used (host including all virtual machines on the host) have a recognized antivirus scanner with up-to-date virus signatures and are operated free of malware.
    - The operating system has an up-to-date status (with active support from the manufacturer/distributor) and, above all, an up-to-date operating system patch status.
    - No hacking tools or unlicensed hacked software components are used that could have a negative impact on business processes. These include, among others, network sniffer or other software.
    - Simultaneous further networking, e.g. via mobile radio, must not be possible via the external system.
    - The third-party system must be presented, checked and approved by netgo's contact person as described above. This must be done before each use, as the general conditions of the software environment may have changed.
    - No vulnerable software may be installed on the third-party system.

3. The Customer's security instructions must be observed.

4. If there is a justified need, the use of email accounts and Internet access via netgo's own domain can be granted. A user ID will be provided for this purpose. The private use of email and the Internet by the Contractor's employees is prohibited. Work equipment of netgo group may only be used for the contract fulfillment.

- External accounts are explicitly recognizable by a separate identifier.
- Sending emails to all users in the address book at the same time is also prohibited.
- A firewall –which includes a spam and virus scanner and an Internet address filter– is operated to ensure network data security. Internet access, including private access, is logged and can be monitored.
- Downloads of software are only permitted within the scope of order fulfillment.

3.3 Access to netgo buildings/rooms

Physical access to work locations of netgo group is only granted after registration and in the presence of netgo employees. Exceptions must be specified in writing. Access must be applied for and granted in accordance with the respective regulations of the location.

Access to security zones, in particular personnel and management areas and computer centers, must be documented and must be accompanied by netgo personnel or contact persons.

3.4 Data security

3.4.1 Access to the Customer's data

Pursuant to the "principle of minimum assignment of authorizations", Contractors may only be assigned authorizations required to fulfill the order. Authorizations may only be used for activities deemed necessary for fulfilling the order and have been agreed with project management. netgo reserves the right to log the Contractor's accesses and to evaluate them on an ad hoc basis.

Remote access may still be authorized. The scope and types of use are regulated in the system-specific specifications or explicitly agreed with the Contractor. However, netgo reserves the right to prevent the remote access provided without prior notice if there is a justified operational interest.

3.4.2 Data exchange procedures

netgo group data may only be exchanged in encrypted form via the IT infrastructure provided by netgo.

3.4.3 Handling of mobile data carriers

The use of mobile data carriers is strictly prohibited. Should it nevertheless be necessary, agreed encryption must always be used. If necessary, only USB sticks provided are to be used. Exceptions must be documented. External data carriers may not be used.

3.4.4 Data backup of project planning statuses

Project planning statuses are to be stored by the Contractor and in a secure and agreed environment.

3.4.5 Data storage with the Contractor

The Contractor must prove which of its employees have access to the Customer's data.

The Contractor undertakes to take suitable and appropriate technical and organizational measures to protect netgo's data. netgo reserves the right to carry out an inspection of these measures at the Contractor's premises and to demand improvements at its reasonable discretion.

3.5 Prohibition of own non-commissioned recordings

Any recordings not authorized by the contractual relationship are prohibited. Handwritten notes and photos are also deemed records.

3.6 Reporting obligations of the Contractor

If the Contractor becomes aware of breaches of information security requirements (including those of third parties) or other risks for the Customer and its assets or its customers, the Contractor undertakes to notify netgo group's Information Security Officer (ISO) immediately without being prompted.

4 Confirmation of the information security requirements

I hereby confirm bindingly for the Contractor that I have taken note of and understood this document "Supplier Information Security Guidelines" and that the Contractor will comply with the guidelines and ensure that vicarious agents also comply with them or will ensure compliance by the persons entrusted by me with the fulfillment of the order.

Name (role)	Date	Signature

5 Period of validity

This document is binding from the start of the supplier or service provider relationship with netgo