May 2018

PRIVACY POLICY

Policy for processing and protection of personal data.

The data protection policy applies to Nordigo ApS and other companies in the Group, hereinafter referred to as Nordigo. The policy must help to ensure and document that Nordigo protects all personal data in accordance with the terms of the Personal Data Regulation. The policy also informs about the processing and use of the registered personal data.

1. Record of processing of personal data

Nordigo handles personal information about:

- Employees
- Customers
- Suppliers

The listing below is an overview of the processing for which the company is responsible. Personal data is the basis for Nordigo´s ability to conclude employment, customer and supplier contracts.

2. Purpose and legality of processing

Personal data is processed and archived in connection with:

- Personnel administration including recruitment, employment, resignation and payroll
- Main data for customers as well as marketing, orders, service and sales
- Main data for suppliers as well as requisitions and purchases

We only use the personal information for the purposes mentioned and we only collect the information necessary to fulfill the purpose.

3. Storage and erasure

Nordigo has introduced the following general guidelines for storing and erasing personal data:

- Personal data is stored in physical folders.
- Personal data is stored in IT systems and on server drives.
- Personal data will be stored for as long as necessary for the purpose of processing.
- Personal data of employees are deleted five years after termination of employment.
- Personal data on applicants who have applied based on advertisement are deleted after recruitment of a new employee; Unsolicited applications are deleted immediately.

4. Data security

Nordigo has implemented the following security measures for the protection of personal data:

- Only employees who have a work-related need for access to the registered personal data have access to it either physically or through IT systems with rights management.
- All computers have a password and employees must not give their passwords to others.
- Computers must have firewall and antivirus software installed that is going to be regularly updated.
- Personal data is properly deleted by phasing out and repairing IT equipment.
- USB-sticks, external hard drives etc. with personal data must be stored in a locked drawer or cupboard.
- Physical folders are placed in a locked office or in a locked cupboard.
- Personal data placed in physical folders are deleted by shredding the papers.
- Personal data that are to be sent by e-mail to an external recipient is sent as a secure-encrypted e-mail.
- All employees are instructed in the processing and protection of personal data.

5. Disclosure

Personal data about employees can be disclosed to public authorities e.g. tax and pension companies as well as Danløn in connection with payroll payments.

6. Processors

Nordigo exclusively uses processors providing sufficient guarantees to implement appropriate technical and organizational security measures in such a manner that processing will meet the requirements of this Regulation.

7. Rights

Nordigo looks after the rights of the data subject including the right of access, withdrawal of consent, rectification and erasure, and inform the data subject of the processing of personal data by the company. The data subject has the right to appeal to the Data Protection Agency.

8. Violation of personal data security

If personal data security has been violated, Nordigo will report the violation to the Data Protection Agency as soon as possible and within 72 hours. The Data controller* of the company is responsible for this. The report describes the violation, which groups of persons it concerns and what consequences the violation can have for these people, as well as how Nordigo has corrected or will rectify the violation. If the violation entails a high risk for those persons Nordigo is processing personal information about, we will notify them. Nordigo documents all violations of personal data security. Should there be any discrepancy with Danish laws and regulations, these are the ones that apply.