Nils Munck Consult
GENERAL DATA PROTECTION POLICY

Contents

1 Purpose

Nils Munck Consult (NM-C, the Company) has implemented this General Data Protection Policy ("General Data Protection Policy") to establish minimum standards for the protection of any personal data when collected, processed, transferred, made available, stored and otherwise used when working on Nils Munck Consult Projects.

This General Data Protection Policy focuses on the legal requirements established by the General Data Protection Regulation ("GDPR") and implements the core principles of the GDPR.

2 Scope

Any person having access to personal data at Nils Munck Consult are obliged to comply with this General Data Protection Policy whenever they collect, process, transfer, make available, store or otherwise use personal data in connection with or in the context of cooperating with Nils Munck Consult.

3 Personal Data

Personal Data means data or information, whether true or not, about an individual who can be identified directly or indirectly from that data or information. Such data may include:

- Employee Personal Data, for example, master data (e.g. name, address, phone number, email address, citizenship, marital status), organizational data (e.g. org. unit, cost centre, personnel or identification number, employee manager), contractual data (e.g. employment status, contract type, average working hours), compensation and benefit information, employee attendance data (e.g. time records, paid time off), performance and talent information (e.g. CV, training, performance ratings, discipline), information contained in emails and other business communication;
- HCP Personal Data, for example, contact details, CRM activities, information contained in emails and other business communication, bank account details;
- Applicant Personal Data, for example, contact details, CV information, work and education history, skills;
- Website/Application User Personal Data, for example, IP-address or other online identifier, location data, log-file data, contact details;

4 Special Categories of Personal Data

Special Categories of Personal Data or also called sensitive data are Personal Data which may only be processed subject to specific requirements. Special Categories of Personal Data are:

- Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership;
- Genetic data;
- Biometric data (such as electronic fingerprint, iris scan or voice recordings);
- Data concerning health (such as employee's number of sick days, disability status or medical history, incontinency issues); and
- Data concerning an individual's sex life or sexual orientation.

5 Processing of Personal Data

Processing means any use or operation which is performed on Personal Data. That could be anything one can do with Personal Data, such as collection, recording, organization, structuring,

storage, adaptation or alteration, retrieval, consultation, usage, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction (hereinafter collectively "Processing").
Some examples of Processing of Personal Data:

- Communication with other individuals, such as sending and receiving emails;
- Obtain information on individuals and put such information into data bases;
- Log access to websites or track site visits of users.

6 Core Data Protection Requirements

The Company and anybody employed by the Company need to ensure that they always comply with the following Core Data Protection Requirements when Processing Personal Data:

6.1 Key Principles

Nils Munck Consult will ensure that Personal Data is

- Processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');
- collected for specified, explicit and legitimate purposes and not further Processed in a manner that is incompatible with those purposes, unless specifically authorized by law ('purpose limitation');
- adequate, relevant and limited to what is necessary in relation to the purposes for which they are Processed ('data minimisation');
- accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that Personal Data that are inaccurate, having regard to the purposes for which they are Processed, are erased or rectified without delay ('accuracy');
- kept in a form which permits identification of an individual for no longer than is necessary for the purposes for which the Personal Data are Processed, unless specifically authorized by law; ('storage limitation'); and if longer than 6 months only by specific permission by the individual.
- Processed in a manner that ensures appropriate security of the Personal Data, including protection against unauthorised or unlawful Processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

6.2 Consent or other Statutory Justification Ground

Nils Munck Consult shall only Process (including making available to others) any Personal Data where the relevant individuals have freely given through a specific, informed and unambiguous indication their consent to the Processing of their Personal Data, as the case may be, or where a statutory justification ground permits the Processing. The Processing of Sensitive Personal Data will typically require the explicit consent of the relevant individual.

6.3 Notice

Where applicable, Nils Munck Consult must notify individuals (prior to the Processing (including collection) of the Personal Data) with the following information:

- Identity of the Company responsible for the Processing of the Personal Data (including contact details);
- Contact details of the Nils Munck Consult Data Protection Officer (where applicable);

- Types of Personal Data being Processed;
- Purposes for the Processing of the Personal Data as well as the legal basis (consent or specific statutory justification ground) for the Processing of the Personal Data;
- Where the Processing is based on the overriding legitimate interest of Nils Munck Consult as statutory justification ground, details on such legitimate interests;
- Recipients or categories of recipients of the Personal Data, and, where applicable, international data transfers including reference to the appropriate safeguards for international data transfer and the means by which the individual can obtain a copy of them or where they have been made available;
- Retention period of the Personal Data;
- Individual's rights under applicable data protection law, which may include the right of access, the right of erasure, or the right to object;
- Right to withdraw consent at any time without affecting the lawfulness of Processing based on consent before its withdrawal;
- Right to lodge a claim with the competent supervisory authority;
- Whether the provision of Personal Data by the individual is a statutory or contractual requirement or a requirement necessary to enter into a contract, as well as whether the individual is obliged to provide the Personal Data and of the possible consequences of such Processing for the individual;
- Existence of automated decision-making, including profiling, and meaningful information about the logic behind involved, the significance and the envisaged consequences of such Processing for the individual (which must be given in a clear and transparent way).

6.4 Collection and Retention

The use of the Personal Data must be limited to only those activities which are necessary to fulfil the identified purpose(s) for which the Personal Data was collected and which are compatible with the purposes identified in the Notice (point 6.3 above), and delete / anonymize Personal Data once the stated purposes have been fulfilled and legal obligations met.

6.5 Confidentiality

All Employees at the Company must be committed to keeping any Personal Data confidential and not to disclose any Personal Data to unauthorized third parties.

6.6 Disclosure to Service Providers

Service providers may have access to Personal Data. In this case, Company must ensure that such access is limited to those Personal Data that is absolutely necessary, that the service provider is diligently chosen, considering in particular the technical and organizational security measures provided by the Service Provider or even adherence to a recognized Code of Conduct for data protection or an approved Certification for data protection, and where applicable that appropriate data processing clauses contained in a relevant service agreement or a separate data processing agreement is in place.

6.7 Data Minimization Principle

The Processing of Personal Data must be adequate, relevant and limited to what is necessary in relation to the purpose for which they are Processed.

6.8 Data Subject's Rights
The individuals whose Personal Data is processed by the Company may have certain rights against the Company to request (1) access to their Personal Data, (2) rectification of their Personal Data, (3) erasure of their Personal Data, (4) restriction of Processing of their Personal Data, (5) portability of their Personal Data, (6) objection to the Processing of their Personal Data (including object to profiling), and (7) objection to automated decision making (including profiling).

6.9 Security / Safeguards
Nils Munck Consult will take reasonable measures to ensure that Personal Data in the Company's possession and control is protected against loss, unauthorized access, use, destruction, modification or disclosure and ensure that appropriate technical and organisation security safeguards are in place to protect Personal Data appropriate to the level of risk and sensitivity of the data. Taking into account state-of-the-art, costs, nature, scope, context and purposes of data Processing as well as the rights and freedoms of the individuals, this will include in particular the pseudonymization and encryption of Personal Data, measures to ensure confidentiality, integrity, availability and resilience, measures to restore the Personal Data in a timely manner in the event of an incident, and processes for regularly testing, assessing and evaluating the effectiveness of the security measures.

6.10 Data Transfer
Personal Data must not be transferred to countries that do not provide an adequate level of data protection from a European data protection law perspective ("Restricted Countries").

6.11 Data Protection Impact Assessment
Whenever Nils Munck Consult develops or considers a new Processing activity, in particular implementing a new technology or IT system (such as applications, software, databases, features), or changing any existing Processing activities, the owner of such Processing activity is responsible to comply with the Data Protection Regulations.

6.12 Data Protection by Design and by Default
When developing or considering a new Processing activity, in particular implementing a new technology or IT system, or changing any existing Processing activities, appropriate technical and organizational security measures must be considered prior to implementation. By default, only Personal Data which is necessary for the intended purpose may be Processed.

6.13 Keeping Documentation up-to-data
When developing or considering a new Processing activity, in particular implementing a new technology or IT system, or changing any existing Processing activities, the owner of the Processing activity shall inform the Nils Munck Consult Data Protection Officer and shall provide the Data Protection Officer with all necessary information in order to keep the related data protection documentation (such as notices, records of processing activities, data processing and data transfer agreements) up-to-date.

6.14 Records of Processing Activities
The data Processing activities must be documented in a record of processing activities. Nils Munck Consult Data Protection Officer is responsible for the completeness and accuracy of the records of processing activities.

6.15 Awareness and Training
All Employees shall receive Data Privacy Awareness Training to become familiar with this General Data Protection Policy, and any relevant supplementing policies, standards, instructions and guidelines.

6.16 Security Breach
All Employees are required to familiarize themselves and comply with the Nils Munck Consult IT Security Information Breech notification procedure.

7 Questions
Any questions relating to the General Data Protection Policy should be directed to:

nm@nilsmunck-consult.com

8 Follow-up of this Policy
This policy is followed up through a quarterly risk assessment. The procedure for the risk assessment is described in the Nils Munck Consult Risk Assessment and Treatment Policy.

9 Changes compared to Last Revision
This is Version 1 of the policy.

Nils Munck,

Founder and CEO

May 17th, 2018