Data Privacy Policy

NNIT GROUP

Classification: PUBLIC
Version: 3

2021-09-23

Conscience driven. Value adding

Table of Contents

Author: HLGD
Approved by: BKJO, PNFA, KSAE, RICL, JHHM, FORS, KLLO

1 Purpose and Scope

1.1 Purpose

As an IT Service provider it is essential to NNIT to respect and protect data privacy. On behalf of our customers and within the NNIT group we process data on a regular basis - a substantial portion of which is Personal Data.

This Data Privacy Policy sets out the standards and the principles, which NNIT collects, uses, stores and processes Personal Data. This Data Privacy Policy is based on the European Union General Data Protection Regulation 5419/16 (GDPR).

Personal Data must be processed in accordance with these standards and principles as well as in accordance with the instructions and requirements set out by NNIT's customers, in order to ensure the safety of the data and the integrity of the individual data subjects concerned by any processing carried out by NNIT or on behalf of others.

NNIT's processing of Personal Data must always adhere to applicable data privacy legislation; primarily the GDPR.

1.2 Scope

This Data Privacy Policy is a minimum standard applicable to all entities and employees of the NNIT group. Local management in the NNIT entities is responsible for the implementation of any local regulatory requirements.

NNIT will safeguard its Customers' data, including Personal Data, with the same diligence and care as its own data.

The following definitions used in this Privacy Policy are:

Term	Definition
Data Controller	A natural or legal person (entity), public authority or any other body which alone or jointly determines the purposes and the means of the processing of Personal Data. The Data Controller is the main responsible entity for data privacy compliance, including inter alia compliance with applicable national and EU law.
DPO	Data Protection Officer. See Section 3 and 6.

Term	Definition
Data Processing	Data processing is a central term in data privacy. It is very broadly understood and will apply in most instances where personal data is used in any way or form. Any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction, is considered data processing.
Data Processor	A Data Processor is a natural or legal person, public authority, agency or any other body which processes Personal data on behalf of a Data controller.
Data Subject	An identified or identifiable natural person (as opposed to a legal person) to whom Personal Data can be linked. In the context of this Data Privacy Policy the Data Subjects will typically fall into these categories: • Persons whose data are processed by NNIT's customers in the course of their business (e.g. their customer data). • NNIT's customers' employees (e.g. employees in the customers' IT departments interacting with NNIT employees or systems). • NNIT employees. • Representatives of suppliers or partners.
Data Transfer	Disclosure, transmission of or making Personal Data available in any way or any form, including the mere access, to third parties.
EU Model Clauses	The EU model clauses are a set of standard contractual terms adopted by the European Commission. The EU Model Clauses constitute a standard data transfer agreement which allows Data Transfer to entities located outside the EU/EEA.
GDPR	EU Regulation 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).
NNIT	The NNIT Group as a whole or an individual entity in the NNIT Group as the case may be. NNIT entities are all wholly owned and controlled subsidiaries of the parent company in the NNIT Group, NNIT A/S incorporated in Denmark.

Term	Definition
Personal Data	Any information, which can be linked to an identified or identifiable natural person. Such an identification link can be either direct or indirect. This makes it a very broad category of data, which is applicable in almost all instances where data is included as element of IT deliverables.
QPoint	Quality Management in IT: NNIT's quality management system.
Sensitive Personal Data	A subset of Personal Data that encompasses the following data: • Racial and ethnical background • Political, religious or philosophic persuasion • Union affiliation • Medical records • Data concerning health • Data concerning sex life • Genetic and biometric data

2 Data Privacy Standards

2.1 Principles of Data Processing

NNIT has adopted the following principles of Data Processing, which shall always apply when NNIT is the Data Controller:

- Data Processing must have a legal basis.
- Data Processing must adhere to good privacy and industry practices.
- The Data Processing must be done with a clear purpose.
- The Data Processing must not extend beyond the purpose.
- Appropriate organizational and technical security measures must be applied in the Data Processing in order to prevent unlawful or unauthorized access, disclosure or destruction.
- The accuracy and authenticity of Personal Data must be ensured.
- Access must be restricted to ensure compliance with the principles set out above.
- Data Processing must be based on documented agreements between the Data Controllers and the Data Processors.
- International Data Transfers must be carried out in accordance with the EU Model Clauses or similar arrangements giving the Data Subjects the same degree of protection as if the Data Processing were carried out within the EU/EAA.

When NNIT acts as a Data Processor on behalf of its customers, NNIT will endeavor to ensure the above principles to the extent this is comprised by the instructions provided to NNIT and concluded between NNIT and its customers.

2.2 Legal basis for Data Processing

When acting as a Data Controller NNIT must ensure that its Data Processing is based on one of the following legal grounds:

- The Data Subject's consent, which must be freely given, explicit and informed.
- The Data Processing is necessary for the performance of contractual obligations between NNIT and the Data Subject.
- The Data Processing is necessary to ensure compliance with NNIT's legal obligations.

- The Data Processing is in the vital interest of the Data Subject.
- The Data Processing is necessary due to a public interest.
- The Data Processing is necessary to pursue legitimate interests of NNIT or a third party and when this interest is not contravened by the rights and freedoms of the Data Subject.

Further, when acting as a Data Controller with respect to Sensitive Data, NNIT must ensure that the Data Processing is based on one of the following legal grounds:

- The Data Subject's consent, which must be freely given, explicit and informed; or when the Data Subject is not able to consent, in order to safeguard the Data Subject's vital interests.
- The Data Processing is necessary for complying with or exercising rights on the applicable employment, social security and social protection law.
- The Data Processing is necessary for medicinal or diagnostic purposes.
- The Data Subject has publicized the information (however, NNIT must in this regard still adhere to the other applicable data privacy standards including this Data Privacy Policy, and in particular ensure that there is a legal basis).
- The Data Processing is necessary in order to exercise legal rights or claims of NNIT.
- The Data Processing is specifically permissible or otherwise required under local law.

2.3 Right of Information and Objection

Data Subjects shall have the following rights set out in this Section 2.3, which must be exercised in accordance with the procedure in Section 6 below. The obligations of NNIT differ depending on NNIT's role as either Data Controller or Data Processor acting on behalf of a third party Data Controller.

NNIT as Data Controller:

When NNIT is the Data Controller, NNIT will (to the extent reasonably possible) provide the Data Subjects with the following information insofar it is necessary for the Data Subject to exercise its rights under the GDPR, local law and this Data Privacy Policy:

- The identity of the Data Controller (that is, the relevant NNIT entity).
- The purpose and the legal basis of the Data Processing, including the legitimate interests pursued by NNIT when the legal basis is a legitimate interest.

- The recipients of the data.
- Data Transfers to entities outside the EU/EEA and the legal basis for such transfers.
- The Data Subject's right to complain as set out in Section 6 below.

The specific Data Processing activities carried out by NNIT are described in further detail in the privacy notices issued by NNIT either on the NNIT website or communicated to the Data Subjects in relation to specific Data Processing activities.

Data Subjects shall have, upon request, the following rights with respect to the Data Processing:

- Right of Access (confirmation to the data subject that Personal Data is processed, access in form of a copy of the data relating to the Data Subject).
- Right of Rectification (the right to change data)
- Right to be Forgotten (the right to have data deleted)
- Right to Restriction of Processing (right to have certain processing activities suspended)
- Right to Data Portability (right to have data delivered in a machine-readable format)
- Right to Objection (right to have certain processing activities limited).
- Right to Limit Automated Decision-making.
- Right to withdraw consent (if the processing is based on consent as the legal basis)

All such requests shall be made according to the procedure in Section 6 below. The rights may be subject to conditions or restrictions in certain instances, depending on such circumstances as the Data Processing, the purpose, the legal basis and the retention requirements.

NNIT as Data Processor:

When NNIT acts as Data Processor on behalf of a third party Data Controller, the obligation to inform the Data Subject rests with the said Data Controller. When a request from a Data Subject concerns a third party Data Controller, NNIT does not have any legal basis (inter alia due to obligations of confidentiality) to divulge information to the Data Subject. NNIT will therefore forward such requests without undue delay to the Data Controller and assist the Data Controller (to the extent reasonably possible) in complying its obligations with the Data Subject.

2.4 Access restrictions and Controls

NNIT has adopted the following definition of access and restrictions extending to all systems and types of data including Personal Data.

- Access to data must be limited to the personnel resources that need to have the access to perform their services.
- For specific types of data specific restrictions may apply which prevent or limit the access to locations outside the EU/EAA or even to specific countries in the EU/EAA and such access restrictions must be reflected in NNIT's service design.

2.5 Security

In order to safeguard Personal Data and to ensure and enforce the access restrictions set out in Section 2.4 above, appropriate technical and organizational security measures must always be taken to prevent the accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure of or access to data.

Compliance relies on a combination of technical and organizational security measures:

- Technical access management and technical security
- Procedures and rules
- Control and traceability ensuring enforceability, documentation and the possibility to investigate possible breaches.

2.6 Data Transfers

NNIT has a global presence, including major operations centers in Denmark, the Czech Republic, China and the Philippines. NNIT therefore engages in Data Processing in the capacity as Data Controller and as Data Processor to third party Data Controllers (NNIT's customers) in different countries and with Personal Data from different countries of origin. NNIT is fully committed to ensuring that such Data Transfers have the requisite level of protection.

When engaging in Data Transfer whereby access to data is provided from one entity to another and where the receiving entity is located outside the EU/EEA, such Data Transfer requires a specific legal basis.

For Data Transfers involving NNIT data, i.e. data where one NNIT entity is Data Controller and another is the Data Processor, EU Model Clauses have been adopted between the NNIT entities.

For data transfers involving customer data, i.e. data where a customer is the Data Controller and an NNIT entity is the Data Processor or sub-processor, EU Model Clauses must be entered into between the customer entities acting in the capacity of Data Controllers and the relevant NNIT entities.

3 Governance

In order to ensure the effective implementation of and compliance with the Data Privacy Policy in the NNIT Group, NNIT has adopted the following governance:

The NNIT DPO is responsible for overseeing overall compliance with data privacy, including the Data Privacy Policy, as well as issuing guidance and counselling on matters of data privacy.

NNIT Legal provides legal business support, including in cooperation with the DPO, on matters concerning data privacy, in particular in relation to contractual matters.

NNIT Line of Business (LoB) – have the day-to-day operational responsibility for ensuring compliance with the Data Privacy Policy and NNIT's duties and obligations as a Data Processor.

NNIT HR is responsible for NNIT's compliance with the Data Privacy Policy when NNIT acts as a Data Controller, collecting and processing data about NNIT employees and applicants.

Other departments within NNIT are responsible for the compliance with the Data Privacy Policy and NNIT's responsibilities as Data Controller for the data collected, used and processed by these departments.

As part of the overall commitment to quality within the NNIT organization, NNIT Quality & Security (Q&S) monitors and enforces compliance across NNIT.

Employees and external consultants with access to NNIT systems are required to be trained, stay updated, adhere to policies, processes and procedures in QPoint when in contact with Personal Data.

All NNIT employees will undergo mandatory data privacy training and all NNIT employees will on an annual basis be obligated to read, understand and approve the NNIT Data Privacy Policy.

4 Reporting of violations

4.1 Reporting of violations

Any breaches of the Data Privacy Policy are handled in accordance with NNIT's existing procedures for non-conformity in QPoint.

In addition to the ordinary internal lines of communication that can be used to report violations, NNIT has extended the scope of our whistleblower service to accommodate violations of this Data Privacy Policy and applicable data privacy law.

4.2 Breach notification

When a privacy data breach occurs where NNIT is Data Processor, NNIT will inform the Data Controller regarding the incident without undue delay.

When a privacy data breach occurs where NNIT is Data Controller, NNIT will inform the Supervisory Authorities and where applicable the Data Subjects in accordance with the requirements set out in the applicable data privacy law.

5 Oversight

5.1 Self-Assessment

NNIT conducts continuous self-assessment of the Data Privacy Policy.

NNIT conducts on at least a yearly basis a self-assessment based on data and information gathered specifically for the self-assessment (e.g. questionnaires or internal lessons learned) and the input derived from audits conducted as well as any registered complaints or non-conformities.

Furthermore NNIT continues to monitor developments in legislation and regulatory practices, including in particular changes in data privacy practices adopted by the Supervisory Authorities and the relevant bodies in the EU.

The self-assessment process is anchored in the Governance set out in Section 3 above and is coordinated by the DPO.

5.2 Risk Identification

Risk identification is an integral part of the security measures set out in Section 2.5 above as well as the overall IT services management and quality management in NNIT, and is comprised of the following elements:

- Confidentiality (if information is revealed to unauthorized persons).
- Integrity (if data is changed by unauthorized persons).
- Availability (if system/data is not accessible during a given period).
- Information Classification.

Based on the above, appropriate measures and controls are established in order to reach an acceptable level of confidentiality, integrity and availability.

NNIT's procedures in Qpoint for security and incident reporting applies to all employees in NNIT working with supplying and maintaining compliance of IT services, systems and data. Service specific risk identification can be provided as part of the services to customers.

5.3 Audit

NNIT audits the compliance with the Data Privacy Policy as part of the processes in QPoint for audits applicable to all aspects of NNIT's business and operation.

Internal Audit:

On a regular basis NNIT conducts internal audits of compliance with this Data Privacy Policy. The internal audits are conducted by NNIT Quality & Security department. The internal audit applies to NNIT's Data Processing in the capacity as Data Controller and Data Processor.

External Audit:

NNIT commits to external audits of its Data Processing, both in the capacity as Data Controller and Data Processor. The external audits may vary depending on the nature of the audit (i.e. does the audit concern NNIT as a Data Controller or NNIT as a Data Processor on behalf of third parties), as well as the contractual obligations between NNIT and its customers. Consequently, NNIT is subject to the following types of external audits:

- Customer audits, which are conducted by the customer on an ad hoc basis and pursuant to local legislation.
- Independent system audits: Audits performed on the basis of a customer requirement based on a specified scope (e.g. ISAE 3402).
- Agency audits: Audits or inspections conducted by Supervisory Authorities or other regulatory bodies.
- Standardization body audits: Audits pursuant to certifications by international standardization bodies (e.g. ISO).

6 Complaints

The following sets out NNIT's commitment to address complaints or requests for information from Data Subjects concerning Data Processing carried out by NNIT.

Complaints can be directed to the NNIT DPO:

NNIT A/S
Att.: NNIT DPO
Østmarken 3A
DK-2860 Søborg
Denmark
Tel: +45 7024 4242
Email: privacy@nnit.com

The NNIT DPO will initiate an investigation and ensure that any complaints from data subjects will be investigated thoroughly and that the data subject will receive an appropriate and timely reply.

Direct complaints against NNIT – NNIT acting as Data Controller:

Direct complaints will be handled in accordance with the complaints procedure in Qpoint and if necessary raised as a non-conformity in accordance with the procedure for non-conformity.

Where necessary, NNIT will take corrective action to ensure that the principles in this Data Privacy are complied with.

Indirect Complaints – NNIT acting as Data Processor on behalf of a third party

NNIT will inform the relevant Data Controller and forward the complaint without undue delay and if the complaint concerns NNIT, assist the Data Controller (to the extent reasonably possible).

Direct complaints to the Supervisory Authority

Data Subjects are entitled to complain to the Supervisory Authority.

7 Change log

7.1 Discontinued Change log

Effective Date	Version	Change description	Author
2019-02-28	2.1	In part 3. Taxonomy related to new organization This version is modified by PAZR on behalf of PXK CR 3694	PAZR
2018-05-25	2	Revision to reflect GDPR CR 3480	PXK
2017-11-01	1	New document	PXK

7.2 Document information

This document is part of a record in QPoint, identified via the information below. Always use QPoint to access NNIT QMS documents.

QPoint Document ID:	33516
Document title:	NNIT Data Privacy Policy