Privacy Policy

Contents

INTRODUCTION

Our Data Privacy Policy lays out strict requirements for processing personal data pertaining to clients, business prospects, business partners and employees. NRTT is committed to abide by data protection laws and to ensure the rules and principles of data protection are followed.

All NRTT employees are obligated to adhere to the Data Privacy Policy.

PROCESSING PRINCIPALS

FAIRNESS AND LAWFULNESS

When processing personal data, the individual rights of the data subjects must be protected. Personal data must be collected and processed in a legal and fair manner.

RESTRICTION TO A SPECIFIC PURPOSE

Personal data can be processed only for the purpose that was defined before the data was collected. Subsequent changes to the purpose are only possible to a limited extent and require substantiation.

DELETION

Personal data that is no longer needed after the expiration of legal or business process-related periods must be deleted. There may be an indication of interests that merit protection or historical significance of this data in individual cases. If so, the data must remain on file until the interests that merit protection have been clarified legally, or the corporate archive has evaluated the data to determine whether it must be retained for historical purposes.

CONFIDENTIALITY AND DATA SECURITY

Personal data is subject to data secrecy. It must be treated as confidential on a personal level and secured with suitable organizational and technical measures to prevent unauthorized access, illegal processing or distribution, as well as accidental loss, modification or destruction.

RELIABILITY OF DATA PROCESSING

Collecting, processing and using personal data is permitted only under the following legal bases. One of these legal bases is also required if the purpose of collecting, processing and using the personal data is to be changed from the original purpose.

CUSOMTER AND PARTNER DATA

DATA PROCESSING - CONTRACTUAL RELATIONSHIPS

Personal data of the relevant prospect, clients and business partners can be processed to establish, execute and terminate a contract. This also includes advisory services for a business partner under contract if this is related to the contractual purpose. Prior to a contract – during the contract initiation phase – personal data can be processed to prepare bids or purchase orders or to fulfill other requests of the prospect that relate to contract conclusion. Prospects can be contacted during the contract preparation process using the information that they have provided. Any restrictions requested by the prospects must be complied with.

DATA PROCESSING – ADVERTISING PURPOSES

If the data subject contacts NRTT to request information (e.g. request to receive information material about a service), data processing to meet this request is permitted.

Personal data can be processed for advertising purposes or market and opinion research, if this is consistent with the purpose for which the data was originally collected. The data subject must be informed about the use of his/her data for advertising purposes. If data is collected only for advertising purposes, the disclosure from the data subject is voluntary. The data subject shall be informed that providing data for this purpose is voluntary. When communicating with the data subject, consent shall be obtained from him/her to process the data for advertising purposes. When giving consent, the data subject should be given a choice among available forms of contact such as regular mail, e-mail and phone.

If the data subject refuses the use of his/her data for advertising purposes, it can no longer be used for these purposes and must be blocked from use for these purposes. Any other restrictions from specific countries regarding the use of data for advertising purposes must be observed.

CONSENT TO DATA PROCESSING

Data can be processed following consent by the data subject. The declaration of consent must be obtained in writing or electronically for the purposes of documentation. In some circumstances, such as telephone conversations, consent can be given verbally. The granting of consent must be documented.

DATA PROCESSING PURSUANT TO LEGAL AUTHORIZATION

The processing of personal data is also permitted if legislation requests, requires or allows this. The type and extent of data processing must be necessary for the legally authorized data processing activity, and must comply with the relevant statutory provisions.

DATA PROCESSING PURSUANT TO LEGITIMATE INTEREST

Personal data can also be processed if it is necessary for a legitimate interest of NRTT. Legitimate interests are generally of a legal (e.g. collection of outstanding receivables) or commercial nature (e.g. avoiding breaches of contract). Personal data may not be processed for the purposes of a legitimate interest if, in individual cases, there is evidence that the interests of the data subject merit protection, and that this takes precedence. Before data is processed, it is necessary to determine whether there are interests that merit protection.

USER DATA AND INTERNET

If personal data is collected, processed and used on websites or in applications, the data subjects must be informed of this in a privacy statement and, if applicable, information about cookies. The privacy statement and any cookie information must be integrated so that it is easy to identify, directly accessible and consistently available for the data subjects. If use profiles (tracking) are created to evaluate the use of websites and applications, the data subjects must always be informed accordingly in the privacy statement. Personal tracking may only be effected if it is permitted under national law or upon consent of the data subject. If tracking uses a pseudonym, the data subject should be given the chance to opt out in the privacy statement. If websites or apps can access personal data in an area restricted to registered users, the identification and authentication of the data subject must offer sufficient protection during access.

EMPLOYEE DATA

DATA PROCESSING FOR THE EMPLOYMENT RELATIONSHIP

In employment relationships, personal data can be processed if needed to initiate, carry out and terminate the employment agreement. When initiating an employment relationship, the applicants' personal data can be processed. If the candidate is rejected, his/her data must be deleted in observance of the required retention period, unless the applicant has agreed to remain on file for a future selection process.

In the existing employment relationship, data processing must always relate to the purpose of the employment agreement if none of the following circumstances for authorized data processing apply.

If it should be necessary during the application procedure to collect information on an applicant from a third party, the requirements of state and local laws must be observed. In cases of doubt, consent must be obtained from the data subject.

There must be legal authorization to process personal data that is related to the employment relationship but was not originally part of performance of the employment agreement. This can include legal requirements, collective regulations with employee representatives, consent of the employee, or the legitimate interest of the company.

DATA PROCESSING PURSUANT TO LEGAL AUTHROIZATION

The processing of personal employee data is also permitted if national legislation requests, requires or authorizes this. The type and extent of data processing must be necessary for the legally authorized data processing activity, and must comply with the relevant statutory provisions. If there is some legal flexibility, the interests of the employee that merit protection must be taken into consideration.

CONSENT TO DATA PROCESSING

Employee data can be processed upon consent of the person concerned. Declarations of consent must be submitted voluntarily. Involuntary consent is void. The declaration of consent must be obtained in writing or electronically for the purposes of documentation. In certain circumstances, consent may be given verbally, in which case it must be properly documented. In the event of informed, voluntary provision of data by the relevant party, consent can be

assumed if national laws do not require express consent. Before giving consent, the data subject must be informed in accordance of this Data Privacy Policy.

DATA PROCESSING PURSUANT TO LEGITIMATE INTEREST

Personal data can also be processed if it is necessary to enforce a legitimate interest of NRTT. Legitimate interests are generally of a legal (e.g. filing, enforcing or defending against legal claims) or financial (e.g. valuation of companies) nature. Personal data may not be processed based on a legitimate interest if, in individual cases, there is evidence that the interests of the employee merit protection. Before data is processed, it must be determined whether there are interests that merit protection. Control measures that require processing of employee data can be taken only if there is a legal obligation to do so or there is a legitimate reason. Even if there is a legitimate reason, the proportionality of the control measure must also be examined. The justified interests of the company in performing the control measure (e.g. compliance with legal provisions and internal company rules) must be weighed against any interests meriting protection that the employee affected by the measure may have in its exclusion, and cannot be performed unless appropriate. The legitimate interest of the company and any interests of the employee meriting protection must be identified and documented before any measures are taken. Moreover, any additional requirements under law must be considered.

TELECOMMUNICATIONS AND INTERNET

Telephone equipment, e-mail addresses, intranet and internet along with internal social networks are provided by the company primarily for work-related assignments. They are a tool and a company resource. They can be used within the applicable legal regulations and internal company policies. In the event of authorized use for private purposes, the laws on secrecy of telecommunications and the relevant national telecommunication laws must be observed if applicable.

There will be no general monitoring of telephone and e-mail communications or intranet/ internet use. To defend against attacks on the IT infrastructure or individual users, protective measures are implemented for the connections to the NRTT network that block technically harmful content or that analyze the attack patterns. For security reasons, the use of telephone equipment, e-mail addresses, the intranet/internet and internal social networks can be logged. Evaluations of this data from a specific person can be made only in a concrete, justified case of suspected violations of laws or policies of NRTT.

TRANSMISSION OF PERSONAL DATA

Transmission of personal data to recipients outside or inside NRTT is subject to the authorization requirements for processing personal data under the Reliability of Data Processing section. The data recipient must be required to use the data only for the defined purposes.

If data is transmitted to a recipient outside of NRTT to a third country this country must agree to maintain a data protection level equivalent to this Data Privacy Policy. This does not apply if transmission is based on a legal obligation. A legal obligation of this kind can be based on the laws of the domiciliary country of NRTT transmitting the data. In the alternative, the laws of the domiciliary country of NRTT can acknowledge the purpose of data transmission based on the legal obligation of a third country.

If data is transmitted by a third party to NRTT, it must be ensured that the data can be used for the intended purpose.

CONFIDENTIALITY OF PROCESSING

Personal data is subject to data secrecy. Any unauthorized collection, processing, or use of such data by employees is prohibited. Any data processing undertaken by an employee that he/she has not been authorized to carry out as part of his/her legitimate duties is unauthorized. The "need to know" principle applies. Employees may have access to personal information only as is appropriate for the type and scope of the task in question. This requires a careful breakdown and separation, as well as implementation, of roles and responsibilities. Employees are forbidden to use personal data for private or commercial purposes, to disclose it to unauthorized persons, or to make it available in any other way. NRTT must inform their employees at the start of the employment relationship about the obligation to protect data secrecy. This obligation shall remain in force even after employment has ended.

PROCESSING SECURITY

Personal data must be safeguarded from unauthorized access and unlawful processing or disclosure, as well as accidental loss, modification or destruction. This applies regardless of whether data is processed electronically or in paper form. Before the introduction of new methods of data processing, particularly new IT systems, technical and organizational measures to protect personal data must be defined and implemented. The technical and organizational measures for protecting personal data are part of NRTT's overall Information Security management and must be adjusted continuously to the technical developments and organizational changes.

DATA PROTECTION CONTROL

Compliance with the Data Privacy Policy controls is the responsibility of the *Director of Operations and IT* and other company units with audit rights or external auditors hired. The results of the data protection controls must be reported to the *Chief Strategy Officer*. On request, the results of data protection controls will be made available to the responsible data protection authority. The responsible data protection authority can perform its own controls of compliance with the regulations of this Policy, as permitted under national law.

DATA PROTECTION INCIDENTS

All employees must inform their supervisor, or the *Director of Operations and IT* immediately about cases of violations against this Data Privacy Policy or other regulations on the protection of personal data (data protection incidents).

In cases of

- improper transmission of personal data to third parties,
- improper access by third parties to personal data, or
- loss of personal data

RESPONSIBILTIES AND SANCTIONS

Management staff are responsible for data processing in their area of responsibility and for ensuring that organizational, HR, and technical measures are in place so that any data processing is carried out in accordance with data protection. Compliance with these requirements is the responsibility of the relevant employees. If official agencies perform data protection controls, the *Director of Operations and IT* must be informed immediately. The relevant executive bodies must inform the *Director of Operations and IT* as to the name of their data protection coordinator. Organizationally speaking, in agreement with the *Director of Operations and IT*, this task can be performed by a data protection coordinator for multiple entities. The data protection coordinators are the contact persons on site for data protection. They can perform checks and must familiarize the employees with the content of the data protection policies. The relevant management is required to assist the *Director of Operations and IT* and the data protection coordinators with their efforts. The departments responsible for business processes and projects must inform the data protection coordinators in good time about new processing of personal data. For data processing plans that may pose special risks to the individual rights of the data subjects, the *Director of Operations and IT* must be informed before processing begins. This applies to extremely sensitive personal data. The managers must ensure that their employees are sufficiently trained in data protection. Improper processing of personal data, or other violations of the data protection laws, can be criminally prosecuted and result in claims for compensation of damage. Violations for which individual employees are responsible can lead to sanctions under employment law.

DEFINITIONS

- Consent is the voluntary, legally binding agreement to data processing.
- Data protection incidents are all events where there is justified suspicion that personal data is being illegally captured, collected, modified, copied, transmitted or used. This can pertain to actions by third parties or employees.
- Data subject under this Data Privacy Policy is any natural person whose data can be processed. In some countries, legal entities can be data subjects as well.
- Under law, further data categories can be considered highly sensitive or the content of the data categories can be structured differently. Moreover, data that relates to a crime can often be processed only under special requirements under law.
- Personal data is all information about certain or definable natural persons. A person is definable for instance if the personal relationship can be determined using a combination of information with even incidental additional knowledge.
- Processing personal data means any process, with or without the use of automated systems, to collect, store, organize, retain, modify, query, use, forward, transmit, disseminate or combine and compare data. This also includes disposing of, deleting and blocking data and data storage media.
- Data Controller is the legally independent company of NRTT, whose business activity initiates the relevant processing measure.
- Third countries under the Data Protection Policy are all nations outside the European Union/EEA. This does not include countries with a data protection level that is considered sufficient by the EU Commission.
- Third parties are anyone apart from the data subject and the Data Controller.
- Transmission is all disclosure of protected data by the responsible entity to third parties.