GDPR Privacy Policy

Next4biz Privacy Policy regarding to General Data Protection Regulation (GDPR).

Next4biz Privacy Policy regarding to General Data Protection Regulation (GDPR)

Board's/Management's approval: Information Security, GDPR and Technology Committee ("Privacy Committee").
This policy is valid since 18.05.2018.
Last review date: 24.06.2022
The next review date: 24.06.2023

Scope:

The Privacy Committee is responsible for this policy. Next4biz collects and processes certain personal data. The persons whose personal data are collected and processed include customers, suppliers, business contacts, employees and other persons with whom we are in business relationships. This policy explains how such personal data must be collected, used and stored in a way to ensure compliance with the data protection standards of the company and with the laws. This policy applies to all employees. This policy supports our other policies involving the use of internet and email systems.

This policy demonstrates how we try to protect the personal data and how we make our employees understand the rules governing the use of personal data to which they have access in the course of performance of their jobs. The EU General Data Protection Regulation (GDPR) addresses the ethical treatment of personal data. The Regulation was introduced in EU law in 2016, valid since 25 May 2018.

Statutory Requirements:

A proper legal basis (or foundation) has been established for our data processing. No infringement is committed in transactions involving any personal data.

Legitimacy / Compliance with the Laws:

How the data processing affects the concerned persons and any negative effects of it have been evaluated. Personal data are collected and processed only in line with the service requirements and limited to the purpose. Necessary notifications regarding the collection of personal data are made.

Transparency:

We comply with the transparency obligations under the right to information. We have clearly established our purposes for data processing. We add the details of our purposes for data processing to the Information Document for Personal Data Processing. We regularly review our transactions and update our processing and our documents when necessary. If we plan to use any personal data for a new purpose outside a legal obligation or function as provided in the law, we first check if it is congruent with our original purpose or if we have obtained a special consent for the new purpose.

Data Minimization:

We collect personal data only to the extent we need them for our established purposes and process them in such design and detail that will be sufficient for the respective purpose. We periodically review the personal data we have processed and stored and at the request of the respective data owners and/or when the respective personal data are no longer needed for business purposes, we anonymize or destroy the personal data.

Special Categories of Personal Data: Our products and data processing needs regarding our services do not require processing of special categories of personal data including but not limited to racial or ethnic origin, political views or similar beliefs, trade union membership (or non-membership), physical or mental health or condition, criminal acts or related lawsuits of any individual. Your personal data are strictly checked in accordance with this policy.

Data Protection Law: The Data Protection Law stipulates how organizations, including Next4biz INC., must collect, use and store any personal data. These rules

apply regardless of whether any personal data are stored electronically or in paper or in other means of storage. In order to comply with the laws, we exercise utmost care for the legitimate collection, use, processing and safe storage of the personal information and for prevention of illegal disclosure of any personal information.

The Data Protection Law is supported with six important principles. These principles dictate that the following principles must be observed regarding the personal data:

1. Personal data are processed fairly and transparently in relation to the data subject.
2. Personal data are collected only for specified, explicit and legitimate purposes.
3. Caution is exercised to ensure that the collected personal data are sufficient and relevant in relation to the.
4. Caution is exercised to ensure that the personal data are accurate and up-to-date.
5. Personal data are not stored longer than necessary and processed by respecting the rights and freedoms of the data subjects. Personal data are protected by taking the necessary security measures.

Data control:

Having the required competency, the Committee periodically reviews the compliance with the above principles. It ensures that the contracts with the suppliers in the status of data processors comply with the requirements of the GDPR.

Accuracy and Level of Relevancy

It is ensured that all personal data are processed in accordance with the established purpose of processing and to the extent necessary for the business needs and service purposes. We do not process any personal data received for a single purpose for any other related purpose or purposes.

Data Security:

We protect your personal data against loss, misuse or abuse.

- If any personal data are stored in printed paper, we keep them in a safe place inaccessible by any unauthorized persons pursuant to our Clean Desk Policy.

- Printed data are destroyed in accordance with our ISO 27001 manual when they are no longer needed.
- Data stored in computers are protected with strong passwords changed regularly in accordance with our Password Policy.
- No data are stored in memory sticks pursuant to our USB Policy.
- Servers containing personal data are kept in a local and secure data center.
- Data is regularly backed up in accordance with the backup procedures of the company.

Commercial Purposes

The personal data we process fall into the scope that we can use for our commercial purposes.

The purposes involving the staff, administration, financial, regulatory, payroll and business development include the following commercial areas:

- Compliance with our statutory, regulatory and corporate governance obligations and practices – collection of information as part of any investigations instituted by any regulatory bodies or in connection with any legal proceedings or claims – Ensuring compliance with the business policies (such as policies involving the use of internet and email systems, etc.)
- Operational reasons such as recording of transactions, training and quality control, ensuring privacy of commercially sensitive information, security audit, credit scoring and control, etc. – Investigation of complaints – Checking of references and ensuring safe employment practices, monitoring and management of the access of the employees to the systems and facilities, and employee non-attendance, management and assessments – Monitoring of the behavior of employees, and disciplinary matters
- Marketing – improvement of services
- Personal data – Information related to identifiable individuals such as job applicants, present and former employees, agents, contract service providers and other personnel, clients, suppliers, marketing persons, etc. The personal data we collect may include the following: Information of any individual related to address and contact details, education, finance and solvency, credentials, training courses and skills, marital status, nationality, position, and CV.

Data Storage:

Personal data are not stored and processed for other purposes than the intended purpose and for no longer than necessary for business and legal purposes for the period defined by law. The required data storage period is established by taking into account the reasons for obtaining the personal data, depending on the conditions of each case, in compliance with our data storage policy. For details, please see our Data Retention and Destruction Policy.

International Transmission of Data:

It is ensured that personal data is stored in safe environments, in the data centers of our third-party business partners when and to the extent necessitated by the services provided by the company.
The personal data is not transmitted to any other location for any purpose.
Any other transmissions are done by prior approval of the Committee.

Data Protection Risks:

The principles and roles set out in the policy help protection of Next4biz against any data security risks, including the following ones:

- Breach of privacy.
- Any undefined data processing processes.

Responsibilities:

- All persons and entities working for or with Next4biz have the responsibility to ensure proper collection, storage and treatment of the data. Each team processing the personal data ensures the treatment and processing of the data in compliance with this policy and the data protection principles.
- The Information Security, GDPR and Technology Committee is ultimately responsible for ensuring that Next4biz fulfills its legal obligations.

The Information Security, GDPR and Technology Committee acts as the data protection officer. The responsibilities for the cloud data center whose services are used and the roles and responsibilities involving the marketing activities are assigned and reviewed by the Committee. The Committee is in charge of the following areas:

- Update the management about the data protection responsibilities, risks and problems.
- Review all data protection procedures and related policies in accordance with an agreed schedule.
- Arrange training courses and information briefs for the persons covered by this policy.
- Address any data protection problems reported by the employees and other persons covered by this policy.
- Address the requests from any individuals to see the personal data kept by Next4biz about the respective individual (also called “subject access requests”).
- Review and approve the contracts made with any third parties who may process the sensitive data of the company.

Responsibilities for the Cloud Data Center whose Services are Used

- Make sure that all systems, services and equipment used for data storage meet acceptable security standards.
- Make regular checks and scans to make sure that the security hardware and software operate properly.
- Evaluate any third-party services the company considers to use to store and process its data.

Responsibilities of the Marketing Manager:

- Approve the data protection notices attached to any means of communication such as emails and letters.
- Address any data protection inquiries from journalists and other media organizations.
- Work with any other staff members when necessary in order to make sure that any marketing initiations comply with the data processing principles.

General Employee Guidelines:

Only employees who need to provide service and/or reach the business purpose can have access to the data covered by this policy. When access to any confidential information is required, an approval process is executed. Next4biz provides the necessary information to the employees that will help them understand their

responsibilities related to the processing of the data. The employees keep all the data secure by taking reasonable measures and pursuing the information security guidelines.

Data Storage:

These rules define how and where the data must be stored in a safe manner. Any problems involving the safe storage of the data are directed to the IT manager or the data protection officer. When the data are stored in hardcopy, they are kept in a secure place where any unauthorized persons cannot see them aligned with clean desk policy. These guidelines also apply any data stored electronically in general but are printed out for any reason. Any data outputs are destroyed in a secure manner when they are no longer needed. Electronically stored data is protected against unauthorized access, accidental erasing and malicious attacks. The data is protected with strong passwords which are changed regularly and are not shared between the employees. The data are stored only in defined drivers and servers and uploaded only to approved cloud information services. Data are backed up at the required intervals. The backups are tested regularly in accordance with the standard backup procedure of the company. All servers and computers containing personal data are protected by approved security software and firewalls.

Data Subject Access Requests

All individuals being the subject of the personal data kept by Next4biz can

- Inquire which personal data of them are kept by the company and why;
- Inquire how they can have access to their personal data;
- Request information about how their personal data are kept up-to-date;
- Request information about how the company fulfill its data protection obligations;
- Request to rectify, to restrict processing or to erase his/her personal data.

If an individual contacts the company requesting this information, it is called the data subject access request. Any subject access requests from any individuals are forwarded to the respective data controller via its registered email account, if any. The data controller should provide the requested information within 30 days. Before delivering any information, the data controller must verify the identity of the person making the subject access request. The Personal Data Protection Law permits the

disclosure of any personal data to any law enforcement authority without the consent of the data subject under certain circumstances. Under such circumstances, Next4biz will process the relevant personal data within the limits allowed by the law.

Data anonymization and destruction process upon requests will be considered due to relevant legislation and for the data in status of “data controller”. Periodic data destruction is executed for the personal data in status of data controller.

For the status of “data processor” the relevant data controller will be responsible for data destruction.

This Statement does not apply to instances where we merely process data on behalf of corporate clients who are data controllers for their benefit, such as when we act as only a data processor.

Giving/Obtaining of Information:

Next4biz aims to make sure that the individuals know and understand that their personal data are processed. To this end, Next4biz has issued a privacy notice stating

- How the personal data are used and
- What the individual’s (data subjects) rights as to the use of their personal data.

You can read the privacy notice at

https://www.next4biz.com/legal/Legal-Security-Policies-privacy-policy.html