Security
Data Retention and Destruction Policy

Data Retention and Destruction Policy

Department: Information Security, GDPR and Technology Committee
This policy is valid since 01.08.2018.

Scope:

The committee* is responsible for this policy. The purpose of this Policy is to ensure the governance of Next4biz in terms of the Record Storage and Destruction Policy and to define how it shall manage its data (e.g., documents, archives and electronic records). This Data Retention and Destruction Policy has been prepared in compliance with the requirements of the relevant laws and regulations of the Republic of Turkey, in particular the Protection of Personal Data (Law No. 6698) as well as the General Data Protection Regulation applicable in the European Union and CCPA (California Consumer Privacy Act).

Any information and documents used internally; any data in functional use for the needs of the business; and any documents or electronic records containing any information derived from the existing data are not considered as important, unless they have been classified as “Necessary/Important/Sensitive” or personal data. Accordingly, any documents not classified as “sensitive are outside the scope of this policy.

* The committee is responsible for information security, data protection and steering.

Access, Storage and Destruction

Access:

Next4biz complies with the principles of protection of personal data in the processing of personal and all other data in accordance with its Privacy Policy. These principles relate to the following areas:

- Legal compliance;
- Transparency; and
- Traceability.

Access to the processed data in a legally compliant, transparent and traceable manner is the goal.

Record:

All information received and produced by the employees of Next4biz in the course of performance of their respective tasks and functions at the premises of Next4biz is deemed a record regardless of the transmission or storage environment, of the storage place or of the importance of the information. Next4biz also processes data in the capacity of data processor via various platforms where it provides its services. Any records and other documents such as record reports, letters, emails, graphics, data, manuscripts, customer transaction records, customer instructions, facility certificates, and letters, invoices, completed application forms, financial records, registration certificates, tender documents received from third persons fall into this scope.

Record Storage Period and Destruction

The storage period is determined according to the time that a record is needed for any commercial reasons, including the provision of a service, or according to the time specified in the applicable regulations. In respect of the records of natural and legal persons, the storage period starts with the starting of the respective service. Upon the cessation of the service, the periodic destruction process starts, unless otherwise stated in the respective contract. Apart from the processes set out in the Privacy Policy, as a data processor, Next4biz receives written requests from its customers and suppliers for anonymization of their data. These requests are evaluated by the Committee and the data are anonymized or deleted, as the case may be, in accordance with the respective contract.

Record Storage and Destruction Program

The Record Storage and Destruction Program is carried out by the operations department of Next4biz. In addition, periodic anonymization of the data as per the requirements of the relevant Personal Data Protection law is performed in accordance with the relevant procedure.

Next4biz keeps any collected and stored personal data as long as its obligations arising from the Law continue or for a period deemed appropriate for the purpose of fulfillment of its obligations and protection of its rights arising from the contracts. Upon the fulfillment or cessation of such obligations or at the request of the customer or the respective person as the data owner, the respective data in the systems of Next4biz are anonymized or deleted by taking the necessary measures to protect the integrity of the data in the systems.

Our company scans the data stored with the status of data controller in 6 (six) month time periods, complying with the periods recorded in our VERBIS processes. In case of data that needs to be deleted is revealed as a result of this scanning, anonymization is performed collectively.

Our corporate customers should retrieve their data via the respective Next4biz platform they have been using, before the expiry of the contract term. Within 30 calendar days (the period specified in the Data Protection Policy) after the termination of the service and the closure of the account, all the data of the customer is deleted and made inaccessible.

The purpose of the Storage and Destruction Policy is to provide guidance about the record storage and destruction protocol to all business segments whose records are kept in Next4biz.

Roles and Responsibilities

Roles:

All owners and/or responsible persons of company records evaluate their records and take the appropriate decision for the keeping and destruction of the records. For the purposes of implementation of this policy, the necessary compliance activities are carried out by the defined roles in accordance with their responsibilities.

Responsibilities:

Before the destruction of any documents or data, their nature and content are identified. Unless this examination has been done, no document may be destroyed. To this end, necessary physical and electronic examination and evaluation are done. This assessment is a task requiring competency and is performed by taking into account the complexity of the respective document.

The storage and backup processes involving the customer data processed by Next4biz are carried out at the data centers. The business continuity and disaster recovery plans are defined and executed.

Audit and Reporting

Data retention and disposal processes are audited by the relevant committee at designated intervals, and the results are reported to upper management. The reporting process is carried out to cover the type of records disposed, the method used, and the responsible parties.

Employee Awareness and Training

All employees are regularly informed about data retention and disposal policies and receive the necessary training. These training sessions aim to increase employees' awareness of legal obligations and company procedures.

Incident Management

Any incident that may occur in data retention or disposal processes must be immediately reported to the Information Security Committee. In the event of a violation, the necessary notifications are made in accordance with applicable legislation, and corrective/preventive measures are taken to prevent recurrence.