Scope

The purpose of this policy is to establish the governance of Next4biz Information Technologies with respect to its Data Retention and Disposal Policy and to define how it manages its data (e.g., documents, archives, and electronic records).

This policy has been prepared taking into consideration Law No. 6698 on the Protection of Personal Data (KVKK), GDPR, ISO 27001, ISO 27701 and ISO 22301 standards, VERBİS obligations, customer contracts, and applicable industry regulations.

Types of Data and Records Within Scope

This policy covers documents, archives, and electronic records. It also covers the following types of data and systems:

The policy also covers cloud services, log records, databases, backups, email systems, customer data held on the SaaS platform, and API records.

Data Classification and Security Controls

Appropriate security controls are applied according to the classification of the information.

Access

We use cookies in accordance with legal regulations to improve our services and your experience on our site. Click 'Accept All' to allow all cookies, 'Reject All' to refuse optional cookies, or manage your preferences in settings.

SETTINGS REJECT ALL ACCEPT ALL

The following access security principles are also applied:

Within the scope of access security, the principle of least privilege and need-to-know access are applied; segregation of duties (SoD) is observed, authorizations are regularly reviewed, and authentication and multi-factor authentication (MFA) controls are used.

Data Records

All information generated or received by Next4biz personnel while performing various activities or functions within the scope of Next4biz products and services is considered a record, regardless of the transmission or storage medium, storage location, or importance. In addition, Next4biz processes data through the platforms on which it provides services in its capacity as a data processor.

Data Retention Period and Disposal

The retention period refers to the period during which a record is required for business reasons and the services provided, or must be retained under applicable regulatory requirements. For records belonging to natural persons, legal entities, or other companies, the retention period begins with the provision of the service. Periodic disposal processes are carried out upon termination of the service, unless otherwise specified in the contracts.

Retention periods are defined in the Data Retention and Disposal Inventory.

In addition to the processes set out in the KVKK Policy, Next4biz, acting as a data processor, receives written data anonymization requests from the organizations it serves and from its suppliers. These requests are submitted to the Committee for evaluation, handled in accordance with the relevant contracts, and the necessary anonymization or deletion is performed.

We use cookies in accordance with legal regulations to improve our services and your experience on our site. Click 'Accept All' to allow all cookies, 'Reject All' to refuse optional cookies, or manage your preferences in settings.

Under the KVKK, disposal is carried out by applying one of the following methods: deletion, destruction, or anonymization.

Data Retention and Disposal Program

The Data Retention and Disposal Program is implemented for company operations. In addition, periodic anonymization procedures required under the KVKK regulations are defined in the relevant procedure.

Our Company retains the personal data it collects and stores for the duration of its obligations arising from applicable laws or for the periods legally required to fulfill its contractual obligations and protect its rights. Once the relevant purpose or obligation has been fulfilled or ceases to apply, or upon a request submitted through our customer or directly by the relevant data subject, the request is promptly addressed on a case-by-case basis with respect to the specific personal data, while ensuring that the integrity of the Company's data is not compromised.

Every six (6) months, our Company reviews the data retained in its capacity as a data controller, in accordance with the retention periods recorded in our VERBİS processes. If, as a result of this review, data requiring disposal is identified, such data is anonymized collectively.

Periodic disposal activities are recorded and made available for inspection when required.

Customer Data and Data Processor Role

Corporate customers whose contractual service period has ended should retrieve their historical data through the Next4biz platform to which they had access before the contract termination date in order to avoid data loss.

We use cookies in accordance with legal regulations to improve our services and your experience on our site. Click 'Accept All' to allow all cookies, 'Reject All' to refuse optional cookies, or manage your preferences in settings.

At the end of the 30 calendar-day period following termination of the service and closure of the account, as defined in the KVKK Policies, all processed data belonging to the relevant organization is deleted and rendered inaccessible.

In addition to this process, the following measures are implemented:

As part of this process, the customer is provided with the opportunity to transfer its data to an external environment; early deletion is performed upon the customer's request, the process for removing data from backups is carried out, and records of deletion activities are maintained.

Roles

All owners and/or responsible persons of company data assess their records and make appropriate decisions regarding data retention and disposal. For the implementation of this policy, the necessary compliance activities are carried out through defined roles and responsibilities.

The roles within the scope of this policy are as follows:

The roles within the scope of this policy are Data Subject, Data Controller, Data Processor, Information Security, System Administrators, Business Unit Owners, KVKK Committee, and Technology Committee.

Responsibilities

The nature and content of any document or data considered for disposal shall be identified. No document shall be disposed of without prior review. Disposal is carried out following the necessary physical and/or electronic examination and assessment.

We use cookies in accordance with legal regulations to improve our services and your experience on our site. Click 'Accept All' to allow all cookies, 'Reject All' to refuse optional cookies, or manage your preferences in settings.

Data restoration from backups is carried out in a controlled manner. Access to backup environments is restricted to authorized personnel.

Audit and Reporting

Data retention and disposal processes are audited by the Information Security Committee at defined intervals, and the results are reported to senior management. The reporting process covers the type and method of disposed records and the responsible persons.

These audits are conducted as part of internal audits, independent audits, customer audits, and certification audits.

Employee Awareness and Training

All employees are informed about data retention and disposal policies at regular intervals and receive the necessary training. The training aims to increase employees' awareness of legal obligations and company procedures.

New employees receive training as part of their onboarding. Training attendance records are maintained.

Incident and Breach Management

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

The breach management process includes the following steps:

We use cookies in accordance with legal regulations to improve our services and your experience on our site. Click 'Accept All' to allow all cookies, 'Reject All' to refuse optional cookies, or manage your preferences in settings.

Information is labeled with one of the following classification levels:

- Public
- Internal Use / Service Specific
- Protected Information / Confidential
- Highly Confidential / Sensitive

Technical Security Measures

The following technical security measures are implemented:

Technical security measures include encryption, MFA, logging, DLP, backup, access control, antivirus and malware protection, patch management, and vulnerability management.

Cloud Services

The following matters are taken into consideration when using cloud services:

When using cloud services, the hosting of customer data, data location, subcontractors, cloud security, and encryption are taken into consideration.

Log Management

The following matters are monitored as part of log management:

As part of log management, access logs, admin logs, audit trails, log retention periods, and log integrity are monitored.

Reference Documents

We use cookies in accordance with legal regulations to improve our services and your experience on our site. Click 'Accept All' to allow all cookies, 'Reject All' to refuse optional cookies, or manage your preferences in settings.

- Backup Policy
- Business Continuity Policy
- Incident Response Procedure
- Data Retention and Disposal Inventory

We use cookies in accordance with legal regulations to improve our services and your experience on our site. Click 'Accept All' to allow all cookies, 'Reject All' to refuse optional cookies, or manage your preferences in settings.