

It is recommended that our Corporate Customers pay attention to the following issues in terms of data security and compliance with laws and regulations within the scope of personal data protection, customer secrets and sensitive data while managing customer information, process design, authorization and configuration or using the application;

1. An “Information/Privacy Notice” must be included in every instance of contact with the customer (issue owner).

While collecting customer information or issues with a web form, the link of the corporate Information/Privacy Notice regarding processing personal data must be included on the form, and the purpose for using the collected data must be stated.

2. If a promotional/marketing campaign email or sms is to be sent to customers, permission must be obtained.

If the messages for promotional/marketing or campaign/advertising purposes will be sent to customers via e-mail or SMS, communication permission must be obtained for the relevant communication channel. Communication permissions should be saved in a database with history and kept up to date. For whatever purpose permission has been obtained, it should not be sent other than for that purpose.

When sending emails and sms via Next4biz CRM, it must be sent with up-to-date permission information. For this purpose;

Communication permission information should be transferred to Next4biz CRM and kept up to date in this environment.

Up-to-date permission information must be queryable by Next4biz CRM via web services to be provided by the company.

3. E-mail and sms campaign messages sent to the customers should include an unsubscribe link for not receiving a new message.

The ability to opt out of lists in email campaigns should be given to customers. If customers don't want to receive messages, they can remove the communication permission by clicking on the unsubscribe link.

4. An authorization matrix that defines authorizations and roles according to the task descriptions must be prepared. In the authorization matrix, the relevant users must be granted access to areas with personal data solely for the purposes of their duties and responsibilities.

A role/authorization matrix must be prepared according to the criticality of personal data for accessing the custom data fields for every search, issue, or customer in addition to searches of customer information and access authorizations.

Definitions on Next4biz must be made according to this matrix, which must be checked periodically before and after use. Authorizations must be granted "only to the extent necessary and only to the relevant party or authority."

5. The data collected on the Next4biz application must not be shared with irrelevant departments or 3rd parties.

The business units or business partners that will receive personal or relevant information are defined with automatic workflows and manual forwarding. Assigning user permissions for form and related fields must be executed due to the need to know the principal and authorization matrix. No forwarding or workflow must be defined outside of the intended purpose. This data must not be transferred to external environments by means of email, etc.

6. In order to prevent the misuse of the personal data stored in the Next4biz application, users must be reminded periodically.

Additionally, regular notifications must be made within your organization and to your suppliers, and the relevant contracts must include these provisions.

7. Information notices can be prepared to serve as an announcement and knowledge base for users and shared within the application.

Announcement Text Example: Personal data created and collected must only be used for the purpose of managing customer information, responding to requests,

and executing business processes. The data cannot be transferred to external environments or used for other purposes.

8. Custom data fields to be created on the Next4biz interface must be defined in accordance with the principles of “proportionality” and “data minimization.”

The creation of unnecessary data fields must be prevented while managing customer information, responding to requests, and executing business processes.

9. Special categories of personal data (sensitive data) cannot be collected and processed within the Next4biz application.

As per relevant legislation in your country (GDPR in EU and CCPA in the USA, Law No. 6698 in Türkiye), the special category of personal data includes the data subject's race, ethnicity, political opinions, philosophical beliefs, religion, sect or other beliefs, appearance or clothing, memberships to associations, foundations or trade unions, medical conditions, sexual life, criminal convictions and security measures, and biometric and genetic data.

- a. Data fields that allow a special category of personal data must not be created on the Next4biz application.
- b. Necessary warnings must be defined on the interface so that users or customers do not upload special categories of personal data to the Next4biz application.

In issue forms, label-type data fields must be created with the addition of the relevant descriptions. Similarly, these information notices must be used for file upload fields.

Text Example: Please do not enter/upload personal data such as health information, criminal record, political opinions, etc., in this field.

- c. Your organization, users, and suppliers must not enter information related to a special category of personal data, and the necessary notifications must be made periodically.
- d Upon receiving an email or a customer issue containing a special category of personal data, the said data must be promptly deleted by the relevant users within the organization.

9. Necessary warnings must be defined on the interface so that sensitive data related to customers' such as financial account or payment information is not uploaded to the Next4biz application.

10. Inessential personal data must not be included in automatic or manual notification message templates and messages sent via email or SMS.

11. The "Privacy Notice" and the purpose for sending the email must be added as a disclosure notice at the end of emails.

Text Example: This email has been sent to you for informational purposes in response to the issue you have submitted. If you haven't submitted any issues to our company and this email does not concern you, please send us an email at [\[email protected\]](#) (your corporate email address).

12. While using support services of Next4biz, screenshots, documents, etc., with personal data or any data which is not necessary for the solution must not be uploaded to applications and environments that do not require personal data, such as help desk, email, etc.

Personal data that is not required for the resolution of support requests must not be submitted or uploaded to the help desk on the Next4biz application.

Security measures such as anonymization and encryption must be taken for the information files required for the resolution of the issue.

You must periodically inform your employees and suppliers on this matter.

13. You can meet the personal data anonymization requests of your customers via the Next4biz API or the Help Desk.

You can use the API method for the anonymization of personal data. Alternatively, you can submit your request to the Next4biz support team by logging an issue with the help desk. No personal data is permitted in anonymization requests; there must be technical information and/or a data pattern addressing this data.

Anonymized data cannot be restored. This is why anonymization in records such as complaints, processes, etc., must be handled within the corporation to ensure the fulfillment of operational continuity and legal responsibilities.

14. The methods under the Information Security Category in the Next4biz Help Desk Knowledge Base must be used and checked periodically.

Next4biz Help Desk Knowledge Base: Information Security Category

- *How can I manage passwords?*
- *How can I manage authorizations?*
- *Which authorizations affect access to customer data?*
- *How can I grant limited authorization for issue-related searches?*
- *How can I limit customer search functionality?*
- *How can I enable IP restrictions for users?*
- *What should I consider when using the Help Desk?*
- *Two-Step Authentication in the Login Process*
- *Confidential Issue Management*
- *Authorization of Customer Data Fields*
- *How Can I Manage Customer Custom Fields?*
- *How Can I Manage Issue Custom Fields?*

15. Outsourcing

If a subcontractor or outsourcing is involved in the processing of personal data, Next4Biz must be informed, necessary agreements must be made, and compliance with legal requirements, contracts, and technical infrastructure must be ensured, with approval obtained before proceeding.