

NEEDS MAP

Data Protection Policy Document

Needs Map

Needs Map is a social cooperative that brings together those in need with individuals, institutions and organizations that want to support them. In this context, it collects and verifies needs from individuals, institutions and civil society organizations and facilitates the matching of these needs with appropriate support through its map-based technology. At the same time, it undertakes an important mission in bringing together real needs and resources in humanitarian aid activities.

Policy Statement

In line with the Data Security Policy, Needs Map aims to ensure the security of information assets, processes and locations in accordance with the principles of confidentiality, integrity and accessibility. With this policy, Needs Map is committed to the protection of personal data of all its stakeholders.

Data security breaches can harm the individuals supported and jeopardize the reputation of the institution. It is the legal responsibility of institutions to protect the personal information and data of the individuals supported. Actions such as data breaches, unauthorized access, unauthorized data sharing or data misuse by any person who contacts Needs Map are considered unacceptable behaviors at all times. Needs Map takes all complaints and concerns about data security breaches submitted to it seriously. All employees and managers are responsible for complying with this policy and reporting incidents, suspicions or breaches that threaten data security. Persons authorized by Needs Map are obliged to investigate data security breaches and take the necessary measures.

All members, founders, board of directors, employees, representatives, consultants, interns, project partners, stakeholders, service providers and volunteers of Needs Map are obliged to report any persons or incidents that they consider to be in violation of the Data Protection Policy to the focal person determined by Needs Map or to the e-mail address etik@ihtiyacharitasi.org .

1. Introduction

This policy has been prepared to ensure the protection of all personal data collected, processed and stored by Needs Map during its activities. Needs Map acts in accordance with the laws of the Republic of Turkey and relevant international standards in personal data protection processes. This policy applies to Needs Map employees, volunteers, beneficiaries, donors, project partners, service providers, consultants and third parties. Personal data means any information belonging to an identified or identifiable natural person, and sensitive data (special personal data such as health information, ethnic origin, religious belief, etc.) is also included in this scope. Within the scope of these rules, it is expected that the values produced will create a corporate culture. The Data Protection Policy Document is the public declaration of Needs Map.

2. Purpose

This policy has been prepared to ensure the protection of all personal data collected, processed and stored by Needs Map during its activities. Needs Map acts in accordance with the laws of the Republic of Turkey and relevant international standards in personal data protection processes. This policy applies to Needs Map's employees, volunteers, beneficiaries, donors, project partners, service providers, consultants and third parties. Personal data means any information belonging to an identified or identifiable natural person, and sensitive data (health information, ethnic origin, religious belief, etc.) is also included in this scope.

3. Scope

Needs Map's Data Protection Policy is valid for all members, founders, board of directors, employees, representatives, consultants, interns, project partners, stakeholders, service providers and volunteers, in any environment and in any situation, during or outside working hours.

4. Responsible Parties

While Needs Map founders, board of directors, employees, representatives, consultants, interns, project partners, stakeholders, service providers, and volunteers are responsible for the implementation of this policy; monitoring whether the policy is implemented or not, and the

procedures to be followed or actions to be taken if it is not implemented are the responsibility of the focal persons to be appointed by Needs Map.

This policy document contains the ethical values and principles that the parties and each employee, founder, board of directors, members, volunteers, interns, and all institutions and organizations that Needs Map works with must comply with. Needs Map founders, board of directors, employees, representatives, consultants, interns, project partners, stakeholders, service providers, and volunteers accept the obligation to act in accordance with this policy document based on the principle of honesty and sense of responsibility.

5. Data Protection Policy Basic Principles

Compliance with Law : Personal data is processed in accordance with the law and ethical rules.

Commitment to Purpose : Data is collected for specific and legitimate purposes and used only for those purposes.

Data Minimization : Only necessary data is collected and processed.

Accuracy and Timeliness : The accuracy of personal data is ensured and updated when necessary.

Storage Period Limitation : Data is stored only for as long as necessary and expired data is securely destroyed.

Security : Necessary technical and administrative measures are taken to ensure the security of personal data.

6. Special Procedures for Beneficiaries and Children in Data Processing

Needs Map applies special procedures in data processing regarding beneficiaries and children:

Clarification and Information: Beneficiaries and children are clearly informed before personal data is collected.

Consent and Permission: The explicit consent of the relevant person is obtained for the processing of personal data. In transactions involving children, permission is obtained from legal guardians.

Data Security: Special security measures are implemented to protect the data of beneficiaries and children.

6.1 While Collecting Data from Beneficiaries and Children;

- All activities should be described in detail.
- Verbal and written permissions and signatures of adults must be obtained.
- Children should be provided with information that is relevant to their age group when personal data is collected, so that they can understand what will happen to their Personal Data and what rights they have.
- The process of obtaining permission from all individuals should be left to the free will of the individual and no pressure should be exerted.
- Data must be stored and kept securely.
- Employees must also take care of their own data security.
- Employees must maintain a high level of protection and safekeeping of phones, computers and all data they receive from beneficiaries.
- Detailed information about verbal consent form, explicit consent form, consent form, participant form, informative forms, brochures, and toll-free call center numbers should be shared with beneficiaries and all individuals contacted during the activities.
- Employees must be aware of and share the right of beneficiaries to withdraw information they have provided.
- The reliability of the documents should be regularly audited and reported by the audit board and/or legal experts.
- In cases where photography is required for reporting or social media purposes during activities, verbal and written consent is obtained from the beneficiaries. For children, images should be taken after verbal consent is obtained from the child and written consent from the parent; however, the child's face should not be visible and their identity should not be revealed.

7. Responsibility in Data Processing

Needs Map acts responsibly in personal data processing processes.

Data Controller: Needs Map is primarily responsible for the protection of personal data and fulfills the legal and technical requirements during the processing of personal data.

Employees and Volunteers: All employees and volunteers of Needs Map are informed about the protection of personal data and act in accordance with this policy.

8. Processing of Personal Data

Personal data is processed in order for Needs Map to carry out its activities, in line with legal obligations or contractual requirements. Personal data includes operations such as collection, recording, storage, modification, transfer, disclosure, anonymization and destruction.

Sensitive Data: Sensitive data such as health information, psychological evaluation, personal history arising from protection risks are processed only with explicit consent and in accordance with security measures.

Donor Information: Donor data is processed only for the specified purposes and the confidentiality of this data is protected.

Project Partners: Data belonging to project partners are processed for the purpose of effective execution of projects and the consent of the relevant data owner is obtained when sharing them.

9. Transfer of Personal Data

Personal data is shared with institutions and organizations within Türkiye within the legal framework and with the consent of the relevant person. Needs Map takes the necessary measures to ensure the security of data in such data transfers.

10. Data Storage and Destruction

Personal data collected is stored only for as long as necessary. Needs Map periodically reviews its data storage processes and securely destroys data when necessary.

Storage Period: Personal data is stored for the periods stipulated in the relevant legal regulations.

Destruction Procedure: When the data retention period expires, these data are deleted, destroyed or made anonymous by Needs Map.

11. Data Security and Protection Measures

Needs Map takes all necessary technical and administrative measures to ensure the security of personal data.

Access Permissions

Username and Password Protection

- Access to personal data is only possible through usernames and passwords that comply with strong password policies.
- User passwords are updated periodically.

Sharing Data and Authorization

- Personal data can only be viewed and shared by authorized personnel.
- Consent is obtained from the relevant individual before data is shared, and it is used solely for specified purposes.
- Personal data is shared only within the framework of legal regulations and institutional policies.
- No data is shared with third parties without the explicit consent of users.
- Users are informed and their consent is obtained before any data is processed.
- The privacy policy is made available for users to access transparently.

Access Revisions and Restrictions

- Permissions are regularly reviewed, and only necessary access rights are granted.
- Access for users whose roles have ended is revoked immediately.

Cybersecurity

Monitoring User Activities

- All user activities on systems where personal data is processed are logged and regularly reviewed.
- The system automatically alerts in case of suspicious activities.

Updates and Security Patches

- Systems and software are regularly updated, and the latest security patches are applied.
- All applications used by users are subjected to security audits.

Precautions for Data Sharing

- Data is shared only via secure communication protocols (e.g., HTTPS).
- If data is shared via email or messaging, files are encrypted.

Malware Scanning

- Data storage areas are regularly scanned, and files containing malware are removed from the system.

Traffic and Activity Monitoring

- Traffic and activities of users accessing the system are continuously monitored.
- The system automatically blocks excessive or abnormal traffic.

Physical Security

Data Storage Areas

- Personal data is stored in physically secure environments.
- Data centers are protected with security measures that allow access only to authorized personnel.

Backup and Recovery Plan

- Personal data is regularly backed up.
- Recovery plans are in place for unforeseen circumstances.

12. The purpose of KVKK, as stated in the Personal Data Protection Law:

<https://www.kvkk.gov.tr/Icerik/4185/6698-Sayili-Kisisel-Verilerin-Korunmasi-Kanununun-Amaci-ve-Kapsami>

- To protect the fundamental rights and freedoms of individuals in the processing of personal data,
- To regulate (discipline) the obligations of real and legal persons who process personal data and the procedures and principles they will comply with,
- Protecting the privacy of individuals (privacy of private life),

- Ensuring personal data security

can be listed as follows.

Personal Data Protection Law; Personal Data Protection Law No. 6698 was accepted in the Turkish Grand National Assembly on 24 March 2016.

12.1 Within the Scope of KVKK

- The importance and obligations of the data controller
- Principles of processing personal data,
- The issues of deletion, destruction or anonymization of personal data are defined.

13. Notification and Reporting Mechanisms

In case of a data privacy violation, the reporting and security procedures of Needs Map (İH) must be put into effect. All members, founders, board of directors, employees, representatives, consultants, interns, project partners, stakeholders, service providers and volunteers of Needs Map are obliged to immediately report any data privacy violations or concerns. Needs Map is committed to ensuring that reporting mechanisms are accessible, confidential and in compliance with legal regulations regarding the protection of personal data. Reported violations will be handled in accordance with the principles of confidentiality and security, and in the event of a violation, the necessary technical and administrative measures will be taken.

All members of Needs Map, founders, board of directors, employees, representatives, consultants, interns, project partners, stakeholders, service providers and volunteers can report their suspicions about data privacy violations through a confidential reporting mechanism. A confidentiality-protecting reporting line and notification mechanism will be established, which all stakeholders can easily apply to when there is a suspicion of data privacy violation. This mechanism will be designed in accordance with security and confidentiality principles, all violations will be meticulously examined and necessary measures will be taken.

Notifications can be made via e-mail to etik@ihtiyacharitasi.org or to the focal persons determined by the Needs Map.

If a person associated with this policy makes a complaint verbally, the focal person must notify the focal person in writing of the information that the person making the verbal report has consented to be shared, and the focal person must follow the process.

In all cases, individuals to whom this policy applies are obliged to evaluate and take into consideration any victimization, retaliation or false accusations that may arise as a result of the notification, and to implement the relevant procedure in cases where it is detected.

14. Training and Capacity Strengthening

Needs Map organizes periodic trainings to regularly inform all employees, volunteers and related parties about acting in accordance with data privacy policies and to provide the necessary awareness. These trainings ensure that responsibilities and obligations regarding data protection are understood, the capacity of related parties is strengthened and the procedures to be followed in case of policy violations are clarified. Training programs are designed and continuously updated to include best practices regarding data security, privacy violations, reporting processes and current legal regulations.

15. Review and Revision

Needs Map reviews its data privacy policies at regular intervals and updates them when necessary. Any changes made to the policy are communicated to all stakeholders in a timely manner and their feedback is received. Stakeholder opinions and suggestions are taken into consideration to ensure that the policy is implemented more effectively and inclusively. Revision processes are carried out in accordance with relevant legal regulations and international data protection standards.