

ntss

SAFETY • FIRE • ENVIRONMENT

DATA PROTECTION POLICY

EN ISO 27001

REVISION

Revision Description	Revision No	Revision Date
Initial Publication	0	20.04.2016
The policy has been amended in accordance with the new Turkish Personal Data Protection Law No. 6698 and its regulations.	1	17.07.2018
Incorrect definitions have been identified and corrected.	2	13.10.2018
The company address has been changed.	3	01.08.2019
Adjustments have been made in accordance with the membership information on the new website.	4	08.08.2019
The countries of the accreditation firms to which personal data is transferred have been detailed. The company address and telephone number have been updated.	5	28.04.2026

DATA PROTECTION POLICY

1. Purpose

As NTSS Eğitim ve Danışmanlık Ltd. Şti., it is our priority to process the personal data of natural persons, including our members, customers, visitors, suppliers and employees, in accordance with the Turkish Constitution and international conventions related to human rights in our country, and in particular in compliance with the Personal Data Protection Law No. 6698 ("KVKK"), and to ensure that the data subjects whose data are processed can effectively exercise their rights.

Accordingly, all processes related to the processing, storage and transfer of all personal data obtained through these channels during our operations, including but not limited to our employees, suppliers, customers, visitors, members and all users visiting our website, are carried out in accordance with the Data Protection Policy ("Policy") of NTSS Eğitim ve Danışmanlık Ltd. Şti.

Respecting the protection of personal data and the fundamental rights and freedoms of natural persons whose personal data are collected is the fundamental principle of our policy regarding the processing of personal data. Therefore, we carry out all our operations in which personal data are processed by paying attention to the rights protecting the privacy of private life, the confidentiality of communication, freedom of thought and belief, and the pursuit of effective remedies.

We take all administrative and technical protection measures required by the quality of the relevant data in order to protect personal data in accordance with the legislation and the latest technology.

This Policy explains the methods we follow regarding the processing, storage, transfer, deletion or anonymization of personal data shared during commercial or social responsibility activities, as well as similar processes within the framework of the principles set out in the KVKK**.**

2. Scope

All personal data processed by our Company are within the scope of the Policy, including our customers, visitors, business contacts, business partners, employees, suppliers, members and third parties.

The Policy applies during the processes related to the processing of all personal data held or managed by the Company; personal data have been addressed and designed in compliance with the KVKK, other applicable legislation related to personal data, and international standards in this field.

3. Definitions and Abbreviations

Specific terms and expressions, concepts, abbreviations, etc. stated in the Policy are briefly explained in this section.

NTSS means NTSS Eğitim ve Danışmanlık Ltd. Şti.

Explicit Consent means consent that is given based on information and expressed with free will regarding a specific subject. It means that it will not leave any doubt and is limited only to such processing activities.

Anonymization means making personal data in such a way that they cannot be associated with an identified or identifiable natural person under any circumstances, even by matching them with other data.

Employee means NTSS Personnel.

Data Subject (Personal Data Owner) means the natural person whose personal data are processed.

Personal Data means any information relating to an identified or identifiable natural person.

Special categories of personal data mean data relating to individuals' race, ethnic origin, political opinion, philosophical belief, religion, sect or other beliefs, appearance and clothing, membership in associations, foundations or trade unions, health, sexual life, criminal convictions and security measures, as well as biometric and genetic data.

Processing of personal data means any operation performed on personal data such as obtaining, recording, storing, preserving, altering, reorganizing, disclosing, transferring, taking over, making available, classifying or preventing the use of personal data, whether fully or partially by automatic means or by non-automatic means provided that they are part of any data recording system.

Data Processor means the natural or legal person who processes personal data on behalf of the Data Controller based on the authority given by the Data Controller.

Data Controller means the natural or legal person who determines the purposes and means of processing personal data and is responsible for the establishment and management of the data recording system.

KVK Board means the Personal Data Protection Board.

KVK Authority means the Personal Data Protection Authority in Türkiye.

KVK Law means the Personal Data Protection Law No. 6698 published in the Official Gazette No. 29677 dated 7 April 2016.

Policy means the Data Protection Policy of NTSS for the protection and processing of personal data.

DPO means the Data Protection Officer.

4. Roles and Responsibilities

Board: The Board is responsible for the overall oversight of determining and

operating reporting, review and sanction mechanisms in case of non-compliance with the Policy, rules and regulations.

Executive Board: The Data Protection Policy has also been approved by the Executive Board.
It is the authorized approval mechanism for the establishment of the Policy, its implementation and ensuring its update when necessary.

The Board of Directors is responsible for taking the necessary measures to ensure that the companies from which services are received, as well as the employees involved, comply with the Policy.

All non-conformities, risks, and matters requiring improvement related to the Policy are regularly reviewed and reported to the Executive Committee for evaluation.

Data Protection Officer: The Data Protection Officer shall be responsible for the preparation, development, implementation and updating of this Policy. The Policy shall be evaluated in terms of update and improvement needs when necessary. The registration of the document prepared in the KVK Authority portal (VERBİS) is the responsibility of the Data Protection Officer.

5. Legal Obligations

Our obligation of transparency: Pursuant to the KVK Law, as the Data Controller, our legal obligations regarding the protection and processing of personal data are listed as follows:

When we collect personal data as the Data Controller, we are obliged to inform the Data Subject on the following matters:

a. For what purpose your personal data will be processed,

b. Information about our identity and, if any, the identity of our representative,

c. For what purpose and for what reasons your processed personal data may be transferred,

d. Our method of data collection and its legal basis,

e. Rights arising from the law,

As a Company, we ensure that this Policy is publicly available, clear, understandable and easily accessible.

Our obligation to ensure data security: As the Data Controller, we take the administrative and technical measures stipulated in the legislation to ensure the security of the personal data held by us. The obligations regarding data security and the measures taken are detailed in Sections 9 and 10 of this Policy.

6. Classification of Personal Data

Personal Data: Personal Data means any information relating to an identified or

identifiable natural person.

The protection of personal data applies only to natural persons; information regarding legal entities that does not contain information about natural persons is outside the scope of personal data protection. Therefore, this Policy does not apply to the data of legal entities.

Special Categories of Personal Data: These are data relating to individuals' race, ethnic origin, political opinion, philosophical belief, religion, sect or other beliefs, appearance and clothing, membership in associations, foundations or trade unions, health, sexual life, criminal convictions and security measures, as well as biometric and genetic data.

7. Processing of Personal Data

We process personal data in accordance with the following principles;

Fair and lawful processing: We process personal data fairly and lawfully, under our obligation of transparency and disclosure.

Ensuring that personal data are accurate and up to date when necessary: In order to ensure that the processed data are accurate and up to date, we take the necessary measures in our data processing procedures. We allow a Data Subject to update their own data and to apply to us for the correction of any inaccuracies in the processed data.

Processing for specific, explicit and legitimate purposes: As a Company, we process personal data in accordance with the legislation within clearly defined and legitimate purposes determined to carry out our activities within the ordinary course of commercial life.

Personal data are relevant, limited and proportionate to the purposes for which they are processed: We process personal data relevant to the specified purposes, in a clear, explicit, limited and proportionate manner.

We prevent the processing of personal data that are irrelevant or not required to be processed. Therefore, unless there is a legal obligation, we do not process special categories of personal data or, where necessary, we obtain explicit consent on the matter.

Retention of personal data in accordance with legal regulations and our legitimate commercial interests: Certain provisions in the legislation require the retention of personal data for a specified period. For this reason, we retain the personal data we process from time to time in accordance with the applicable legislation or for the period necessary for the purpose of processing the personal data.

In the event that the storage period stipulated in the legislation expires or the purpose of processing ceases to exist, we delete, destroy or anonymize the personal data. Our principles and procedures regarding retention periods are detailed in Article 9.1 of this Policy.

Purposes for processing personal data: As NTSS, we process personal data for the purposes listed below:

- To carry out our Training and Consultancy activities,
- To provide support services within the scope of contracts and service standards,
- To determine the preferences and needs of our members/visitors and to shape and update the services we offer accordingly,
- To ensure the fulfillment of our legal obligations as required or dictated by legal regulations,
- To conduct market research and statistical studies,
- To evaluate job applications,
- To ensure communication with persons who have a business relationship with the Company,
- Marketing,
- To provide our members and customers with recommendations about our newsletters, new trainings and programs,
- Compliance management,
- Vendor/supplier management,
- Legal reporting,
- Billing,
- To carry out the necessary reporting for the certification of our customers who receive training through the e-learning platform and whose customer details are shared with accreditation bodies,
- To manage membership processes through social networks,
- To ensure corporate communication,
- To provide personalized suitable job postings and employment-related information.

Processing of special categories of personal data: Special categories of personal data are processed by us by taking the administrative and technical measures prescribed by law and determined by the KVK Board, and if explicit consent has been obtained or where required by legislation.

Special categories of personal data related to health and sexual life may be processed for the purposes of protecting public health, preventive medicine, medical diagnosis, treatment and care services, as well as planning and management of healthcare

services and the financing of such services by individuals or authorized institutions. Organizations are under an obligation of confidentiality; therefore, such data other than those of our employees are not processed by us. Such data belonging to our employees may be processed by persons authorized by law.

Processing of personal data collected through cookies: We use cookies to improve the way we operate and for the use of our web pages. In addition, we use certain cookies to remember the preferences you make on our websites, thereby providing you with an enhanced and personalized experience.

The resumption of training on the e-learning platform at any time it is stopped is carried out through such cookies.

We may collect your personal data through cookies available on our digital platforms; we may process, transfer or store the data we collect.

Processing of personal data for human resources and employment purposes: In order to evaluate job applications, we process, store and transfer your personal data contained in your CV, diploma and other documents that you share with us during your application process as a job candidate. The processing, transfer and storage of personal data shared as a job candidate fall within the scope of this Policy.

The Personal Data of an employee are processed and stored in accordance with this Policy as well as the Social Security Institution (SGK) legislation.

Processing of personal data collected under other memberships via www.ntss.com.tr: In order to become members via **www.ntss.com.tr**, visitors share the following information and register in the system;

- Name,
- Surname,
- Email address,
- GSM phone number,
- Nationality,
- Identification number,
- Date of birth,
- Position,
- Address

The deletion, destruction or anonymization of personal data on this platform is covered under Article 9 of this Policy.

Processing of personal data collected within the scope of electronic learning (e-Learning) training services via www.ntss.com.tr: Electronic learning (e-

Learning) trainings are sold via www.ntss.com.tr by credit card or bank transfer.

In addition to these, members who make payments by credit card share their credit card information. NTSS receives services from İyzico, an institution approved by the Banking Regulation and Supervision Agency (BDDK), for transactions related to credit cards. The collected financial information is processed for the purposes of the sales process in relation to the purchased products and services. In case of purchase through the digital portal, www.ntss.com.tr transfers the member's financial information to the İyzico system for the execution of the transaction, and the cardholder's card security is ensured through 3D secure.

Details of the information transferred for payment purposes:

- Cardholder's Name and Surname
- Credit Card Number,
- Expiry date,
- CVV2,
- Or bank account details

During the purchase, information such as the member's billing and payment details (name, surname, billing address), invoices sent to members and copies of bank receipts of payments received from members, payment number, invoice amount, invoice number, invoice notification date are obtained. These data are processed to manage the billing process, accounting, after-sales services, communication, marketing, audit, control, and transactions carried out with payment service providers. During the purchase, the member's financial information is transferred to legal entities such as banks or credit card companies for the execution of the transaction. Credit card information is not stored in the www.ntss.com.tr databases.

The above data are shared and transferred with third parties in accordance with Article 8 of this Policy.

The deletion, destruction or anonymization of personal data on this platform is covered under Article 9 of this Policy.

Personal data collected within the scope of electronic learning (E-Learning) training services via www.ntssakademi.com: E-Learning trainings are provided to our customers via www.ntssakademi.com. After logging in, once the sales transactions are completed, user information is copied to this environment from www.ntss.com.tr.

In this environment, all training activities of students are recorded; logins and logouts to the website are recorded, including tests and their results. Such information may be made accessible to accreditation bodies abroad if requested by organizations that issue certificates related to the provided training or that may require reporting.

The deletion, destruction or anonymization of personal data on this platform is covered under Article 9 of this Policy.

Exceptional cases where explicit consent is not required for the processing of personal data: In the following exceptional cases arising from the law, we may process personal data without obtaining explicit consent:

a. Where it is explicitly provided for by laws,

b. Where it is necessary to process the personal data of the parties to a contract, provided that it is directly related to the establishment or performance of a contract,

c. Where data processing is necessary for the establishment, exercise or protection of a right,

d. Where data processing is necessary for the legitimate interests of the data controller, provided that it does not harm the fundamental rights and freedoms of the Data Subject,

e. Exceptional cases where special categories of personal data may be processed without the explicit consent of the Data Subject are addressed in Article 7 of this Policy.

8. Transfer of Personal Data

Transfer of personal data domestically: NTSS acts in accordance with the decisions and regulations determined by the KVK Law and accepted by the KVK Board regarding the transfer of personal data.

Without prejudice to the exceptional cases specified in the legislation, personal data and special quality data cannot be transferred to other natural or legal persons without the explicit consent of the Data Subject.

In exceptional cases stipulated by the KVK Law and other legislation, data may be transferred to authorized administrative or judicial bodies or institutions without the explicit consent of the Data Subject, in the manner and subject to the limitations prescribed by the legislation.

In addition, in the exceptional cases stipulated by the legislation, in the situations detailed in Article 7.9 of this Policy and in cases related to special categories of personal data listed in Article 7 of this Policy, transfer may be made without seeking explicit consent.

By taking the measures prescribed by the KVK Board and the relevant legislation, special categories of personal data related to the health and sexual life of the Data Subject may be processed without seeking explicit consent, by persons under an obligation of confidentiality or by authorized institutions and organizations, for the purposes of protecting public health, preventive medicine, medical diagnosis, treatment and care services, as well as planning and management of healthcare services and their financing.

Transfer of personal data abroad: As a rule, personal data cannot be transferred abroad without the explicit consent of the Data Subject. However, in cases specified in one of the exceptional situations in Article 7 of this Policy, if the third parties located

abroad are in a country announced by the KVK Board as providing adequate protection, personal data may be transferred abroad without explicit consent.

In cases where they are located in countries without adequate protection, Data Controllers in Türkiye and abroad must put in writing that adequate protection is ensured and the permission of the KVK Board must be obtained.

Transfer of personal data abroad for the purpose of providing our services and marketing activities: Subject to certificates approved by international accreditation bodies, the names and other personal information of our students who successfully complete our face-to-face or e-Learning platform trainings are shared with accreditation bodies located in the United Kingdom and the United States of America for the issuance of certificates.

The names and other personal information of students who will take exams after the trainings will be shared with accreditation institutions in the United Kingdom and the United States of America.

Agencies and organizations to which personal data are transferred

Personal Data;

a. Training Accreditation Companies,

b. Legally authorized international institutions and organizations,

c. Private legal entities authorized by law

are transferred in accordance with the principles and rules detailed above.

Measures we take regarding the lawful transfer of personal data

Technical measures: Measures to protect your personal data include, but are not limited to, the following:

a. We make internal technical arrangements for the processing and storage of personal data in accordance with the legislation,

b. We establish technical infrastructure to ensure the security of the databases where your personal data will be stored,

c. We monitor the established technical infrastructure processes and carry out audits,

d. We determine procedures regarding the reporting of the technical measures we take and audit processes,

e. We periodically update and renew technical measures,

f. Risky situations are re-evaluated and necessary technological solutions are produced,

g. We use virus protection systems, firewalls and similar software and hardware security products and establish security systems in parallel with technological developments,

h. We employ staff specialized in technical matters.

Administrative measures: Measures to protect your personal data include, but are not limited to, the following:

a. We establish policies and procedures for access to personal data within the Company by Company and affiliate employees.

b. We inform and train our employees on protecting and processing personal data in accordance with the law.

c. In the contracts we make with our employees and/or the Policies we establish, we record the measures to be taken in case personal data are processed by Company employees in violation of the law.

d. We audit the personal data processing activities of the data processors we cooperate with.

9. Retention of Personal Data

Retention of personal data for the period stipulated by the relevant legislation or required for the purpose of processing: Provided that the retention periods stipulated in the legislation are reserved, we retain the personal data we process for the period necessary for the purpose of processing.

When we process personal data for multiple purposes, once the purposes of processing cease to exist or upon the request of the Data Subject, if there is no obstacle in the legislation regarding the deletion of the data, the data will be deleted, destroyed or stored by being anonymized. We follow the legal provisions and decisions of the KVK Board regarding destruction, deletion or anonymization.

Technical measures

a. We establish technical infrastructures for the deletion, destruction or anonymization of personal data and audit mechanisms.

b. We take the necessary measures to ensure the secure storage of personal data, c. We employ technical experts.

c. We create business continuity and emergency plans against potential risks and develop systems for their implementation.

d. We establish security systems in line with technological developments related to the storage of personal data.

Administrative measures:

a. We raise awareness by providing consultancy to our employees on technical

and administrative risks related to the storage of personal data,

b. In cases where we cooperate with third parties regarding the storage of personal data, we include the necessary provisions in the contracts made with the companies to which personal data are transferred, regarding the implementation of security measures by those parties for the secure storage of personal data.

10. Security of Personal Data

Our obligations regarding the security of personal data: We take administrative and technical measures based on technological opportunities and implementation costs.

- prevention of unlawful processing,
- prevention of unlawful access,
- ensuring lawful retention.

Measures we take to prevent the unlawful processing of personal data: We carry out and ensure the performance of the necessary audits within the Company. We train and inform our employees on the lawful processing of personal data. Operations carried out by the Company are specifically evaluated by all business units, and as a result of these evaluations, personal data specific to the commercial activities carried out by the relevant units are processed.

In cases of cooperation with third parties for the processing of personal data, the contracts made with the companies processing personal data include provisions stating that the persons processing personal data will take the necessary security measures.

In the event of unlawful disclosure of personal data or a data breach, we notify the KVK Board of this situation and carry out the examinations required by the legislation and take the necessary measures.

Technical and administrative measures taken to prevent unlawful access to personal data

a. In order to prevent unlawful access to personal data,

b. We employ personnel with technical expertise,

c. We periodically update and renew technical measures,

d. We establish access authorization procedures within the Company,

e. We determine procedures regarding the reporting of the technical measures we take and audit processes,

f. We establish data recording systems used within the Company in compliance with the legislation and carry out periodic audits,

g. We create emergency response plans against potential risks and develop systems for their implementation,

h. We provide training and information to our employees on access to personal data and authorization,

i. In cases where cooperation is carried out with third parties for activities such as the processing of personal data, the contracts made with the companies providing access to personal data include provisions stating that persons with access to personal data will take the necessary security measures,

j. We establish security systems in line with technological developments to prevent unlawful access to personal data.

Measures we take in case of unlawful disclosure of personal data: We take administrative and technical measures to prevent the unlawful disclosure of personal data and update them in accordance with our relevant procedures. If we detect unlawful disclosure of personal data, we establish systems and infrastructures to inform the Data Subject and the KVK Authority.

Despite all administrative and technical measures taken, in the event of unlawful disclosure, this may be announced on the website of the KVK Authority or by another method if deemed necessary by the KVK Board.

11. Rights of the Data Subject

Under our obligation of transparency, we inform the Data Subject and establish the systems and infrastructure related to this notification. We make the necessary technical and administrative arrangements to enable the Data Subject to exercise their rights regarding their personal data.

The Data Subject has the following rights regarding their personal data:

a. To learn whether their personal data are processed,

b. To request information if their personal data have been processed,

c. To learn the purpose of processing personal data and whether they are used in accordance with their purpose,

d. To know the third parties to whom personal data are transferred domestically or abroad,

e. To request the correction of personal data if they are incomplete or incorrectly processed,

f. To request the deletion or destruction of personal data in case the reasons requiring the processing of personal data cease to exist,

g. To request that the correction, deletion or destruction operations mentioned above be notified to third parties to whom the personal data have been transferred,

h. To object to the emergence of a result against the person by analysing the processed data exclusively through automated systems,

i. To request compensation for the damage in case of loss due to the unlawful processing of personal data.

Exercise of rights related to personal data: The Data Subject may submit their request regarding their personal data through a separate method determined by the KVK Authority or by sending it in writing with a wet signature to the address "Beştepe Mah. Nergiz Sok. Via Flat İş Merkezi Ofis No: 27-28 Yenimahalle /ANKARA- TÜRKİYE".

In the application made by the Data Subject regarding the exercise of the above-mentioned rights and containing explanations regarding the use of such requests, the requested matter must be clear and understandable; the request must relate to the applicant themselves, or if another person is acting on behalf of the applicant, they must be specifically authorized in this regard and such authorization must be documented; additionally, the application must include personal information and the address details of the applicant, and identity documents must be attached to the application for identity verification.

Such requests shall be made individually, and requests from unauthorized third parties regarding the review of personal data will not be accepted.

Evaluation of the application

Response period for the application: Requests regarding personal data will be responded to free of charge within 30 (thirty) days at the latest in any case, or based on the tariff rate to be published by the KVK Board, depending on the nature of the request.
Additional information and documents may be requested during the application or during its evaluation.

Our right to reject the application: Applications related to personal data will be rejected by providing the reasons under the following conditions:

a. Processing of personal data for purposes such as research, planning and statistics by anonymizing them with official statistics,

b. Processing of personal data for artistic, historical, literary or scientific purposes or within the scope of freedom of expression, provided that privacy is not violated, personal rights are not infringed, or a crime is not committed,

c. Processing of personal data that have been made public by the Data Subject,

d. The application is not based on a specific reason,

e. The application contains a request contrary to the applicable legislation,

f. Non-compliance with the application procedure.

Procedure for the evaluation of the application: Requests must be submitted in writing, with a wet signature or electronic signature and via KEP, or identified by other methods determined by the KVK Board together with documents identifying the applicant, and thus the implementation of this Policy may commence.

If the request is accepted, the relevant action will be taken and notification will be made in writing or electronically. If the request is rejected, the applicant will be informed in writing or electronically by stating the reasons.

Right to file a complaint with the Personal Data Protection Board: In case of rejection of the application, if the response is found insufficient or no response is given in due time, the applicant shall have the right to apply to the KVK Board within 30 (thirty) days from the date of the response and in any case within 60 (sixty) days from the date of application.

12.Publication and Authorization of the Document

This Policy will be maintained in two different media, printed copy and electronic environment.

13.Update Period

This Policy will be reviewed at least once a year and, if necessary, will be updated in accordance with the principles set out in the Document Management Procedure.

14.Validity

This Policy shall be deemed valid after it is published on the Company's website.

15. Termination

When the termination resolution is accepted, unsigned copies of this Policy shall be retained for 5 years with a wet signature.

For questions regarding this Policy, contact details:

NTSS Eğitim ve Danışmanlık Ltd. Şti.

Adres: Beştepe Mah. Nergiz Sok. Via Flat İş Merkezi Ofis No: 27-28 Yenimahalle /ANKARA- TÜRKİYE

E-posta: dpo@ntss.com.tr

Tel: +90 (312) 911 55 66

APPROVED BY

ASUMAN ERKUL

