ONE WORLD DANIŞMANLIK EĞİTİM VE ARAŞTIRMA HİZMETLERİ LİMİTED ŞİRKETİ

PERSONAL DATA PROTECTION AND PROSSESING POLICY

CONTENTS

This text has been prepared in Turkish and English. In case of conflict between the English and Turkish versions; The Turkish version will be valid. Turkish Laws are valid for disputes regarding your personal data.

This text has been prepared in Turkish and English. In case of conflict between the English and Turkish versions; The Turkish version will be valid. Turkish Laws are valid for disputes regarding your personal data.

1. INTRODUCTION

For One World Danışmanlık Eğitim ve Araştırma Hizmetleri Limited Şirketi (“One World or the Company”), the privacy and security of your personal data are of great importance. For this reason, by this Policy of Personal Data Protection and Processing ("Policy"), the basic principles regarding how to comply with the regulations stipulated in the Personal Data Protection Law No.6698 ("KVKK") are determined.

2. OBJECTIVE

This Policy, has been prepared by the Company in order to ensure full compliance with the Personal Data Protection Legislation and to prevent violations of these regulations. The purpose of this Policy is explained below;

a. Setting rules and determining procedures for activities related to the Processing of Personal Data;
b. To determine the direct / indirect related persons and the duties and responsibilities of these persons within and outside the Company by ensuring compliance with the Data Protection;
c. To create the necessary system for the awareness of employees and business partners who will make the necessary arrangements for the Protection of Personal Data;
d. To ensure transparency by informing people whose personal data is processed by the Company such as employees, shareholders, officials, visitors, and employees of cooperating institutions and third parties.

3. IMPLEMENTATION OF THE POLICY AND RELATED LEGISLATION

The relevant legal regulations in force regarding the processing and protection of personal data will primarily be applied. In case of inconsistency between the current legislation and the Policy, our Company accepts that the current legislation will be applied.

The policy has been formed by embodying the rules set forth by the relevant legislation within the scope of Company practices.

4. ENFORCEMENT OF THE POLICY

This Policy issued by our Company is dated 01.03.2021. In case the whole or certain articles of the Policy are renewed, the issue date of the Policy will be updated.

The policy is published on our Company's website (www.oneworldconsulting.com) and made available to the relevant persons upon the request of the personal Data Owners.

5. DEFINITIONS

Personal Data: It is any information relating to an identified or identifiable natural person.

Processing of Personal Data: It refers to all kinds of operations performed on data through fully or partially automatic means of personal data or non-automatic means provided that it is a part of any data recording system including obtaining, recording, storing, preserving, changing, reorganizing, disclosing, transferring, taking over, making available.

This text has been prepared in Turkish and English. In case of conflict between the English and Turkish versions; The Turkish version will be valid. Turkish Laws are valid for disputes regarding your personal data.

Anonymization: It refers to the rendering of personal data that cannot be associated with an identified or identifiable natural person under any circumstances, even by matching with other data.

Data Controller: It refers to 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.

Data Processor: It refers to the natural or legal person who processes personal data on behalf of the data controller based on the authority given by the controller.

Third Party: Refers to a natural or legal person, public institution, organization or body other than the Data Owner, Data Controller, Data Processor and persons authorized to process personal data under the direct authority of the Data Controller or Data Processor.

Related Person/Data Owner: It refers to the real person whose personal data is processed.

Explicit Consent: It refers to the consent relates to a specified issue, declared by free will and based on information.

Personal Data Breach: It refers to the security breach that causes inadvertent or unlawful destruction, loss, change, unauthorized disclosure or access to Personal Data transferred, stored or processed.

Sensitive Personal Data: Personal data relating to the race, ethnic origin, political opinion, philosophical belief, religion, sect or other belief, clothing, membership of associations, foundations or trade-unions, information relating to health, sexual life, convictions and security measures, and the biometric and genetic data are deemed to be sensitive data.

The Institution: It refers to the Personal Data Protection Authority.

The Board: It refers to the Personal Data Protection Board.

Data Protection Legislation: It refers to all applicable laws regarding privacy and data protection, including but not limited to KVKK and related regulations and all applicable legislation, rules, regulations, binding administrative guidelines and their updated versions.

Personal Data Processing Inventory: Personal Data Processing activities that Data Controllers carry out depending on their business processes; The purposes of Personal Data Processing refers to the inventory that they have created by associating with the data category, the recipient group and the data owner group, and elaborated by explaining the maximum period required for the purposes for which the Personal Data is processed, the Personal Data foreseen to be transferred to foreign countries and the measures taken regarding data security.

6. FIELD OF APPLICATION, PERSONAL DATA OWNERS AND PERSONAL DATA CATEGORIES

This Policy will find application in the regions where the Company operates.

This text has been prepared in Turkish and English. In case of conflict between the English and Turkish versions; The Turkish version will be valid. Turkish Laws are valid for disputes regarding your personal data.

The application area of the policy is the processing of personal data belonging to the following Data Owners:

- Natural Person Clients, Consultants
- Company officials
- Shareholders
- Business Partner Shareholders, Officials, Employees
- Candidates of Employment
- Business Partners or Possible Customers
- Visitors
- Third Parties

The following information can be counted as personal data;

- Identity Information (name, surname, TR ID number, place of birth, date of birth, etc.)
- Contact Information (Phone number, address, e-mail address etc.)
- Information of family members and relatives (personal data about family members (e.g. spouse, mother, father, child) and relatives of the personal data owner in order to protect the legal interests of the data owner within the framework of the operations carried out by the Company business units)
- Resumes

This Policy does not cover all possibilities and / or legal requirements that may arise regarding the subject of the Policy and does not foresee and / or replace all special regulations / legal requirements that may be made. For this reason, legal advice should be obtained from the Data Controller when necessary.

This Policy may be updated periodically to reflect changes in the relevant legislation and / or internal policies.

7. DETAILS OF DATA CONTROLLER, REPRESENTATIVE AND DATA PROCESSOR

Data Controller is our Company and its registered office is at Maslak Mah. Maslak Meydan Sk. No: 1 Beybi Giz Plaza Kat 25, 34485 Sarıyer / İstanbul. The Data Controller has appointed Ozlem Mangir as the Data Controller Representative.

Data Controller Representative (“DCR”) contact address is Ozlem Mangir at info@oneworldconsulting.com.

8. PRINCIPLES TO BE APPLIED IN THE PROCESSING OF PERSONAL DATA

The principles to be considered during the processing of personal data are listed under the headings below.

8.1 Compliance with Law and Good Faith

The Company must act in accordance with the law and honesty within the scope of the processing of personal data. In this context, by applying the principles of proportionality and necessity in the processing of personal data, the Company should process only the necessary amount of personal data at a level that is in accordance with the data processing purposes.

This text has been prepared in Turkish and English. In case of conflict between the English and Turkish versions; The Turkish version will be valid. Turkish Laws are valid for disputes regarding your personal data.

8.2 Being Accurate and Updated When Needed

The Company should ensure that the personal data they are processing are accurate and up-to-date and take the necessary measures accordingly.

8.3 Processing for Specific, Clear and Legitimate Purposes

The Company should process personal data for specific, clear and lawful reasons. Within this scope, the purpose for which personal data will be processed should be determined and these purposes should be submitted to the information of the Data Owners before the personal data is processed.

8.4 Being Related, Limited and Measured for the Purpose of Processing

The Company should process personal data in a way that is suitable for the realization of the specified purpose and avoids the processing of personal data that are not needed or not are related to the realization of the purpose.

8.5 Being Stored for the Period Stipulated in the Relevant Legislation or For the Period Required for the Purpose for which they are Processed

The Company should keep personal data only for the periods stipulated by law or limited to the purpose for which they were processed. Within this scope, if a period is specified for the storage of personal data in the relevant legislation, this period should be followed. If a period of time has not been determined, personal data should be kept for the period required for the purpose for which they were processed.

9. PROCESSING OF PERSONAL DATA AND SENSITIVE PERSONAL DATA

9.1 Processing of Personal Data

The Company carries out its personal data processing activities in accordance with the data processing conditions set forth in Article 5 of the KVKK. Within this scope, personal data processing activities are carried out in the presence of the personal data processing conditions listed below.

a. Having the Explicit Consent from the Personal Data Owner

In cases where other data processing conditions do not exist or are not applicable, in accordance with the general principles set out in Article 5 of the KVKK, the personal data of the data owner can be processed by the company with the free will of the data owner, having sufficient information about the personal data processing activity, without any hesitation and only if s/he gives her consent limited to that transaction.

b. Personal Data Processing Activity Being Explicitly Stipulated by Laws

If there is an explicit regulation in the laws regarding personal data processing, personal data processing activity may be carried out by the Company limited to the relevant legal regulation.

This text has been prepared in Turkish and English. In case of conflict between the English and Turkish versions; The Turkish version will be valid. Turkish Laws are valid for disputes regarding your personal data.

c. Failure to Obtain the Explicit Consent of the Data Owner Due to Actual Impossibility and Being Obligatory to Process Personal Data

In cases where the personal data owner cannot explain his consent or his consent is not valid, if it is necessary to process personal data in order to protect the life or body integrity of the persons, data processing activities are carried out by the Company in this context.

d. The Personal Data Processing Activity Is Directly Related to the Establishment or Performance of a Contract

Provided that it is directly related to the establishment or performance of a contract, the processing of personal data belonging to the parties and employees of the contract is necessary, the Company carries out data processing activity.

e. Processing Personal Data to Fulfill Legal Obligation

The Company will be able to process the personal data of the data owner in order to fulfill its legal obligations as the data controller.

f. Data Owner Makes Own Personal Data Public

Personal data that is made public by the relevant person herself/himself (not limited to LinkedIn, Kariyer.net; publicly disclosed in any way) is processed by the company in accordance with the purpose of publicization.

g. Being Obligatory of Data Processing for Establishment, Use, or Protection of a Right

In the event that the processing of personal data is mandatory for the establishment, exercise or protection of a right, personal data processing activities are carried out by the Company in accordance with this obligation.

h. Being Obligatory of Data Processing for Legitimate Interest

Provided that it does not harm the fundamental rights and freedoms of the personal data owner, data processing can be carried out if data processing is mandatory for the legitimate interests of the Company.

9.2 Processing of Sensitive Personal Data

Special attention is paid to the processing of personal data of sensitive data that have the risk of creating discrimination when unlawfully processed by the company. Within this scope, sensitive personal data are processed by the Company in accordance with Article 6 of the KVKK.

10. TRANSFER OF PERSONAL DATA

The Company can transfer personal data and sensitive personal data of the personal data owner to third parties in accordance with the 8th Article of the KVKK by taking the necessary security measures in line with the legal personal data processing purposes.

This text has been prepared in Turkish and English. In case of conflict between the English and Turkish versions; The Turkish version will be valid. Turkish Laws are valid for disputes regarding your personal data.

By the company, according to KVKK Article 9, in the case KVK Board adequate protection where it has been declared a foreign country or the absence of adequate protection, adequate protection of those responsible for the data in and in the foreign countries, Turkey has pledged in writing and KVK where the Board ' permission or be transferred personal data to foreign countries by obtaining explicit consent of Relevant Persons, processed personal data can be stored in domestic / international storage servers.

11. ENLIGHTENMENT OF PERSONAL DATA OWNERS

The Company carries out the necessary processes to ensure that Data Owners are informed during the acquisition of personal data, in accordance with Article 10 of the KVKK and the Communiqué on the Procedures and Principles for Fulfilling the Responsibility of Enlightenment.

Within this scope, the following information is available in the Enlightenment Forms submitted to the Data Owners by the Company:

- The title of our Company as the Data Controller and the identity of its representative,
- For what purpose the personal data of Data Owners will be processed by the company,
- To whom and for what purpose the processed personal data can be transferred,
- Method and legal reason for collecting personal data,
- Rights of personal Data Owner

12. FINALIZATION OF REQUESTS OF PERSONAL DATA OWNERS

Personal Data Owners can use their rights in the KVKK regarding their data by applying in writing or by other methods determined by the Board.

The rights Data Owners have as follows:

- Learning whether personal data is processed,
- Requesting information if personal data has been processed,
- Learning the purpose of processing personal data and whether they are used appropriately for their purpose,
- To know the third parties to whom personal data are transferred domestically or abroad,
- To request correction of personal data in case of incomplete or incorrect processing and to request notification of the transaction made within this scope to third parties to whom personal data are transferred,
- To request the deletion or destruction of personal data in the event that the reasons requiring its processing disappear, despite the fact that it has been processed in accordance with the provisions of the law and other relevant laws, and to request notification of the transaction made within this scope to third parties to whom personal data has been transferred
- Object to the occurrence of a result against the person himself by analysing the processed data exclusively through automated systems
- To request the compensation of the damage in case of damage due to the processing of personal data illegally

This text has been prepared in Turkish and English. In case of conflict between the English and Turkish versions; The Turkish version will be valid. Turkish Laws are valid for disputes regarding your personal data.

The requests regarding the use of the rights mentioned above can be made via the Application Form that can be accessed from the link www.oneworldconsulting.com

- in written and wet signed form by registered mail or through a notary public at Maslak Mah. Maslak Meydan Sk. No: 1 Kat 25 Beybi Giz Plaza, 34485 Sarıyer / İstanbul address
  or
- With your secure electronic signature within the scope of Electronic Signature Law No. 5070 or with your mobile signature, or by using the e-mail address previously notified to the data controller and registered in the data controller's system, it must be sent to Ozlem Mangir at info@oneworldconsulting.com

13. CASES EXCLUDING THE RIGHTS OF PERSONAL DATA OWNERS REQUIRED BY LEGISLATION

In accordance with Article 28 of the KVKK, personal data owners will not be able to assert their rights in the following matters.

- Processing of personal data is necessary for the prevention of crime or for criminal investigation,
- Processing of personal data that has been publicized by Related Person/Data Owner
- The processing of personal data is necessary for the execution of supervision or regulation duties and for disciplinary investigation or prosecution by the authorized and authorized public institutions and organizations and professional organizations having the status of public institutions, based on the authority granted by the law,
- Processing of personal data is necessary for the protection of the economic and financial interests of the State regarding budget, tax and financial issues.

According to paragraph 1 of Article 28 of the KVKK, in the following cases, the data will be out of the scope of the Law, and the requests of the data owners will not be processed in terms of these data.

- Processing of personal data by real persons within the scope of activities related to him or his family members living in the same residence, provided that they are not given to third parties and obligations regarding data security are complied with.
- Processing personal data for purposes such as research, planning and statistics by making them anonymous with official statistics.
- Processing of personal data for artistic, historical, literary or scientific purposes or within the scope of freedom of expression, provided that they do not violate national defense, national security, public security, public order, economic security, privacy of private life or personal rights or constitute a crime.
- Processing of personal data within the scope of preventive, protective and intelligence activities carried out by public institutions and organizations authorized by law to ensure national defense, national security, public security, public order or economic security.
- Processing of personal data by judicial authorities or execution authorities regarding investigation, prosecution, trial or execution proceedings.

This text has been prepared in Turkish and English. In case of conflict between the English and Turkish versions; The Turkish version will be valid. Turkish Laws are valid for disputes regarding your personal data.

14. LIABILITY TO ENSURE THE SECURITY OF PERSONAL DATA

The Company takes the necessary technical and administrative measures to ensure the appropriate level of security in order to prevent the unlawful processing of the personal data they process and the unlawful access to the data and to ensure the preservation of the data.

Some of these measures are listed below.

- Training and raising awareness of employees regarding the legislation on the protection of personal data
- Taking technological technical measures to prevent access to systems and locations where personal data are stored and periodically updating the measures taken
- Periodic reporting of the technical measures taken, producing technological solutions for security risks
- Installing related software and systems, including software and hardware, including virus protection systems and firewalls
- In cases where personal data is subject to transfer, adding records to the contracts concluded with the persons to whom the personal data is transferred, stating that the party to whom the personal data is transferred will fulfil its obligations to ensure data security.

15. STORAGE PERIOD OF PERSONAL DATA

In case it is stipulated in the relevant laws and regulations, the company keeps personal data for the period specified in these regulations. If a period of time is not regulated in the legislation regarding how long personal data should be stored, personal data is processed for a period that requires the Company to process it in accordance with the practices of the Company and depending on the activity carried out while processing that data of practicing its commercial life. Then personal data is deleted, destroyed or is made anonymous.

If the purpose of processing personal data has ended and the retention periods determined by the relevant legislation and the Company have reached the end; personal data can only be stored in order to provide evidence in possible legal disputes or to assert the relevant right related to personal data or to establish a defense. In this case, the stored personal data is not accessed for any other purpose, and access to relevant personal data is provided only when it is required to be used in the relevant legal dispute. Here too, after the aforementioned period expires, personal data are deleted, destroyed or anonymized.

16. REQUIREMENTS AND TECHNIQUES FOR DELETING, DESTRUCTING AND ANONYMIZING PERSONAL DATA

16.1 Conditions

Although the Company has been processed in accordance with the provisions of the relevant law as regulated in Article 138 of the Turkish Criminal Law and Article 7 of the KVKK, in case the reasons for processing are eliminated, the Company deletes, destroys or anonymizes personal data in the first periodic destruction process following the date when the obligation to destroy or anonymize occurs. The Company deletes, destroys or anonymizes personal data

This text has been prepared in Turkish and English. In case of conflict between the English and Turkish versions; The Turkish version will be valid. Turkish Laws are valid for disputes regarding your personal data.

when the Company will decide upon the own decision or upon the request of the personal Data Owner. The period of time for periodic destruction is 6 (six) months.

16.2 Deletion and Destruction Techniques of Personal Data

The most common deletion or destruction techniques used by the company are listed below:

a. Physical Destruction

Personal data can also be processed in non-automatic ways, provided that it is part of any data recording system. While such data is deleted/destroyed, a system of physical destruction of personal data in a way that cannot be used later is applied.

b. Secure Deletion Software

While the data is deleted/destroyed that processed in fully or partially automatic ways and stored in digital environments; methods for deleting data from the relevant software in a way that cannot be recovered again are used.

c. Sending to a Specialist for Secure Deletion

In some cases, the company may contract with an expert to delete personal data on its behalf. In this case, the personal data are securely deleted / destroyed by the expert on this subject so that they cannot be recovered again.

16.3 Techniques for Anonymizing Personal Data

Anonymization of personal data means making personal data unacceptable to an identified or identifiable natural person, even by matching it with other data.

The most commonly used anonymization techniques by the company are listed below.

a. Masking

Data masking is a method of making personal data anonym by extracting the basic identifying information of personal data from the data set.

b. Aggregation

With the data aggregation method, many data is aggregated and personal data cannot be associated with any person.

c. Data Derivation

With the data derivation method, a more general content is created than the content of personal data and it is ensured that personal data cannot be associated with any person.

d. Data Shuffling, Permutation

With the data shuffling method, it is ensured that the values in the personal data set are mixed and the connection between values and individuals are not possible.

17. PERSONAL DATA PROCESSING INVENTORY

The Company has created a personal data inventory even if it is not liable in accordance with the Data Controllers Registry Regulation issued by the Personal Data Protection Authority. In this data inventory, there are data categories, source of data, data processing purposes, data processing process and recipient groups to which the data is transferred.

18. DATA VIOLATION

The Company complies with all legal obligations to inform Data Owners or official authorities about security breaches that will result in accidental or unlawful destruction, loss, alteration, unauthorized disclosure of personal data or access to data. Some methods and procedures ("Data Breach Management Procedure") have been determined by the Company in order to prevent the repetition of the same event in order to detect, report and improve the consequences of any possible Personal Data Violation.

19. REPORTING

All kinds of risks, violations, control errors, including danger, risk, negligence / abuse of duty, or any behavior that may cause misapplication, which may lead to the Company's liability due to non-compliance with the legislation on Personal Data regulated by this Policy, should be reported to the following addresses:

1. One World Compliance Officer, Tim Bright, tim.bright@oneworldconsulting.com;

and / or

2. Data Controller Representative, Ozlem Mangir, info@oneworldconsulting.com;

In case a breach of Personal Data and / or control error causes a possible crisis, as stated in the Data Breach Management Procedure; the crisis management team will be involved and take primary responsibility in the management process.

In addition to these, the persons making a report within the scope of this Policy will be protected from any sanction; because the Company takes anti-sanction measures to protect notifiers from harmful consequences such as termination of employment, demotion, unwanted transfer or behaviors that can be defined as “mobbing”.

20. INSPECTION SYSTEM

In accordance with the company rules, each violation of this Policy is proportionally sanctioned according to the severity of the relevant violation and the applicable legal legislation, contractual provisions and company standard procedures.

The Company reserves the right to report any violation to the relevant Judicial and Administrative Authorities.

This text has been prepared in Turkish and English. In case of conflict between the English and Turkish versions; The Turkish version will be valid. Turkish Laws are valid for disputes regarding your personal data.