PERSONAL DATA RETENTION AND DESTRUCTION POLICY

Purpose

This Policy was drafted by Çanakkale Otoyol ve Köprüsü İnşaat Yatırım ve İşletme A.Ş. **("Company")** in accordance with the Turkish Law No. 6698 on the Protection of Personal Data, to determine the procedures and principles for the processing and protection as well as destruction and anonymization of personal data in accordance with the relevant legislation.

Scope

This Policy is applicable to all processing of personal data (of employees and interns, job candidates, suppliers' employees, supplier officials, news subjects and persons who submit complaints or demands regarding the project) by the Company where the processing is performed wholly or partly by automated means as well as to the processing other than by automated means of personal data which form part of a filing system.

This Policy may apply in full to all the aforementioned categories of data subjects while it could also be applied partially.

Foundations

This Policy is based on the Law No. 6698 on the Protection of Personal Data ("KVKK" or "Law"), the Regulation No. 30286 on the Data Controllers Registry and the Regulation No. 30224 on the Deletion, Destruction or Anonymization of Personal Data.

In the event of any inconsistencies between this Policy and the applicable legislation on the processing, protection and destruction of personal data, provisions of the Legislation shall prevail in application.

Definitions

For the purposes of this Policy, the following are to be understood and interpreted as:

a) **Recipient group:** Category of natural or legal person to whom personal data is transferred by data controller,

b) **Inventory:** Personal Data Inventory prepared by the Company in accordance with the legislation,

c) **Relevant user:** Persons (within or outside the organization of the data controller) who participate in the technical details of the storage, processing and protection under authorization and instructions received from the data controller,

d) **Destruction:** Erasure, destruction or anonymization of personal data,

e) **The Law:** The Turkish Law No. 6698 on the Protection of Personal Data dated 24 March 2016,

f) **Storage Media:** Any media on which personal data are stored, where the personal data are processed wholly or partly by automated means or processed by other means as part of a filing system,

g) **Personal data:** Any information relating to an identified or identifiable natural person,

h) **Data subject:** The natural person whose personal data are processed,

i) **Anonymization of personal data:** Rendering personal data impossible to link with an identified or identifiable natural person, even if matched with other data

j) Processing of personal data: Any operation performed upon personal data such as collection, recording, storage, retention, alteration, re-organization, disclosure, transferring, taking over, making retrievable, classification or preventing the use thereof, fully or partially through automatic means or provided that the process is a part of any data registry system, through non-automatic means,

k) Erasure of personal data: The process of making personal data inaccessible and reusable for the relevant users,

l) Destruction of personal data: The process of making personal data inaccessible, irretrievable and non-reusable by anyone,

m) The Board: Turkish Personal Data Protection Board,

n) The Authority: Turkish Personal Data Protection Authority,

o) Logging: The process followed to help obtain information on evidence of possible attacks, including steps to analyze, record, collect, merge, store originals for analysis and presentation of event recordings, in other words, logs; generated by information systems covering all critical networks and devices, which helps to obtain important information such as which channels the attack took place, the type of attack, and where the attack started,

p) Sensitive personal data: Personal data relating to race, ethnic origin, political opinion, philosophical belief, religion, sect or other belief, clothing, membership to associations, foundations or trade-unions, health, sexual life, convictions and security measures, biometric and genetic data,

q) Periodic destruction: Erasure, destruction or anonymization of the personal data, which shall be carried out when the conditions of processing set out by the Law are no longer met and also ex officio at the repeated intervals specified in the Policy,

r) Policy: This Personal Data Retention and Destruction Policy, which is accepted as the data responsible in accordance with the Law, which was made by the Company as data controller the basis for determination of maximum time required for the purpose of the processing of personal data and erasure, destruction or anonymization thereof,

s) Registry: The registry of data controllers maintained by the Authority (VERBİS),

t) Company: The company whose trade name is Çanakkale Otoyol ve Köprüsü İnşaat Yatırım ve İşletme A.Ş.,

u) Data processor: The natural or legal person who processes personal data on behalf of the data controller upon his authorization,

v) Data filing/registry system: The registry system which the personal data is registered into through being structured according to certain criteria,

w) Data controller: The natural or legal person who determines the purpose and means of processing personal data and who is responsible for establishing and managing the data registry system.

For definitions not included in this Policy, the definitions in the Law shall apply.

Personal Data Storage Media

The personal data of the data owners are securely stored by the Company in virtual and physical areas listed as following by the Company in accordance with the relevant legislation, in particular the provisions of KVKK, and in accordance with international data security principles:

a) Electronical data storage areas:
   1. Computers,
   2. Central servers,
   3. Shared / non-shared disk drives for storing data over the network,
   4. Cloud services,

b) Non-electronical data storage areas:

   1. Papers,
   2. Unit cabinets.

General Principles of Storage and Destruction of Personal Data

The Company is a Data Controller with an obligation to register on the Registry and it accepts, declares and undertakes that it is obliged to store the personal data it holds in accordance with the Inventory and to act in accordance with this Policy in order to delete, destroy or anonymize it when necessary.

The following principles apply to the storage and destruction of personal data:

a) The Company shall comply with the general principles set forth in Article 4 of the Law,
b) The Company accepts that having drafted this Policy is not sufficient proof that personal data has been deleted, destroyed or made anonymous in accordance with the legislation,
c) When storing, deleting, destroying or anonymizing the personal data, the Company shall comply with the security measures stated in Article 12 of the Law, the provisions of the relevant Legislation, Board decisions and the Policy,
d) The Company declares that it shall provide for the deletion, destruction or anonymization of personal data that the Company holds is that is processed fully or partially by automated means or processed by non-automatic means provided that it is part of a data filing/registry system in a compliant manner with this Policy and tools provided for by this Policy,
e) The Company shall record all transactions relating to the deletion, destruction and anonymization of personal data and shall retain such records for at least 3 (three) years, reserving other legal obligations.

Purposes of Personal Data Processing

Personal data are processed by the Company as Data Controller for the following purposes in accordance with Article 20 of the Constitution and Article 4 of the KVKK:

- ❖ Carrying out Selection and Placement Processes for Job Candidates / Trainees / Students
- ❖ Carrying out Application Processes for Job Candidates
- ❖ Conducting Employee Satisfaction and Engagement Processes
- ❖ Fulfillment of Obligations Arising from Employee Contracts and Legislation
- ❖ Audit / Ethics Activities
- ❖ Conducting Training Activities
- ❖ Compliance with the Legislation
- ❖ Execution of Finance and Accounting Activities
- ❖ Ensuring the Security of Physical Areas
- ❖ Execution of Assignment Processes
- ❖ Monitoring and Conducting of Legal Affairs
- ❖ Internal Audit / Investigation / Intelligence Activities
- ❖ Conducting Communication Activities
- ❖ Human Resources Process Planning
- ❖ Execution / Audit of Business Activities

- ❖ Conducting Workplace Health / Safety Activities
- ❖ Organization and Event Management
- ❖ Conducting Performance Evaluation Processes
- ❖ Execution of Risk Management Processes
- ❖ Retention and Archiving Activities
- ❖ Social Responsibility and Civil Society Activities
- ❖ Conducting of Contract Processes
- ❖ Tracking Requests / Complaints
- ❖ Ensuring the Security of the Data Controller's Operations
- ❖ Informing Authorized Persons, Institutions and Organizations
- ❖ Execution of Management Activities

Legal, Technical and Other Principles Requiring Destruction of Personal Data

Personal data of data subjects are destructed by the Company in accordance with legal, technical and other reasons and purposes including but not limited to;

- **a)** The general principles set out in Article 4 of the Law,
- **b)** On the request of the data subject,
- **c)** Termination of legal obligations,
- **d)** Legal, technical and other reasons.

Technical and Administrative Measures for Secure Storage of Personal Data and Prevention of Unlawful Processing and Access

The technical measures taken by the Company for the safe storage of personal data and the prevention of unlawful processing and access are listed below:

- **a)** Network security and application security are provided.
- **b)** Closed system network is used for personal data transfers through the network.
- **c)** Key management tools are implemented.
- **d)** Security measures are taken within the scope of procurement, development and maintenance of information technology systems.
- **e)** Security of personal data stored in the cloud is ensured.
- **f)** Authorization matrix has been established for employees.
- **g)** Access logs are kept regularly.
- **h)** Data masking is applied when necessary.
- **i)** Up-to-date anti-virus solutions are used.
- **j)** Firewalls are utilized.
- **k)** User account management and authorization control system is applied, and these are followed.
- **l)** Log records are kept without user intervention.
- **m)** Intrusion detection and prevention systems are used.
- **n)** Penetration tests are performed.
- **o)** Cyber security measures have been taken and their implementation is continuously monitored.
- **p)** Encryption is utilized.
- **q)** Portable memory, CD, DVD media are transferred to the data of special persons are encrypted.
- **r)** Data loss prevention software is used.

The administrative measures taken by the Company for the safe storage of personal data and the prevention of unlawful processing and access are listed below:

- **a)** Training and awareness studies are conducted at regular intervals on data security for employees.
- **b)** Corporate policies on access, information security, usage, storage and disposal have been prepared and implemented.

c) Confidentiality commitments are signed with third parties.
d) Employees who have been resigned or who have resigned from their jobs are removed from this field.
e) Signed contracts contain data security provisions.
f) Extra security measures are taken for personal data transferred via paper and the related documents are sent in confidential document format.
g) Personal data security policies and procedures have been established.
h) Personal data security issues are swiftly reported.
i) Personal data security is monitored.
j) Necessary security measures are taken for entering and exiting physical environments containing personal data.
k) The security of physical environments containing personal data against external risks (fire, flood etc.) is ensured.
l) The security of personal data environments is ensured.
m) Personal data processed are reduced as much as possible. (Data minimization)
n) Personal data is backed up and the security of the backed up personal data is also ensured.
o) Existing risks and threats are identified.
p) Data service providers are regularly audited for data security.
q) Service providers are provided awareness on data security.

Technical and Administrative Measures for Proper Destruction of Personal Data

Technical measures taken by the Company for the destruction of the personal data of the data subject in accordance with the relevant legislation are:

a) Utilizing up-to-date systems required for the destruction of personal data, taking of relevant confidentiality and information security measures,
b) Closure and removal of Relevant Users' authorizations in the scope of personal data to access, retrieve deleted data and/or reuse,
c) Irrevocable deletion of the personal data stored on the central servers and cloud systems,
d) In addition to these listed measures, using appropriate means of destruction for electronical storage media (physical de-magnetization, overwriting or anonymization) based on the nature of the media and the personal data concerned,
e) Application of deletion (masking, etc.), destruction (physical destruction) methods for the destruction of personal data stored on non-electronical media.

Administrative measures taken by the Company for the destruction of the personal data of the data subject in accordance with the relevant legislation are:

a) Regular implementation of the practices necessary for the destruction of personal data,
b) Maintenance of necessary equipment for the physical destruction of personal data stored on non-technical media.

Additional Measures for Storage and Destruction of Sensitive Personal Data

Technical measures taken by the Company for the proper storage and destruction of sensitive personal data in accordance with the relevant legislation are:

a) Protocols and procedures for personal data security have been determined and implemented.
b) When sensitive personal data is to be sent by e-mail, it is sent in encrypted form and only using KEP (Registered Electronic Mail) or corporate e-mail account.
c) Up-to-date encryption / cryptographic keys are used for sensitive personal data and are managed by different units.

Unit Assignments and Information for Storage and Destruction of Personal Data

A list including the titles and job descriptions of the personnel working in the Company units involved in the storage and destruction of the personal data can be found in ANNEX-1.

Storage and Destruction Periods

A list including the storage times and destruction of the personal data can be found in ANNEX-2.

Periodic Destruction

Periodic destruction of personal data is set to occur every 12 (twelve) months, except for the periods indicated in the list of applicable storage and destruction times annexed to this Policy according to the categories of personal data processed by the Company.

Destruction of Personal Data Upon Demand by a Data Subject

When the person requests the deletion or destruction of his personal data by applying to the Company pursuant to Article 13 of the Law;

- **a)** If there are no legal bases applicable for processing the personal data; the Company deletes, destroys or anonymizes the personal data subject at the data subject's request. The Company concludes the request within 30 (thirty) days at the latest and informs the data subject.
- **b)** If there are no legal bases applicable for processing the personal data and the data has been transferred to third parties, the Company notifies the relevant third party within 10 (ten) days at the latest and ensures that the necessary transactions are carried out by the third party.
- **c)** If a legal basis is still applicable to the processing of the personal data, data subject's request may be denied by the Company, provided that it notifies the data subject in writing or electronically of the decision as well as the justification under Art 13, paragraph 3 of the Law within 30 (thirty) days at the latest.

Validity

This Policy as drafted by the Company entered into force as of the date of publication on the Company's website.

In case of any inconsistencies between the provisions of KVKK and other relevant Legislation and this Policy, the provisions of KVKK and other relevant Legislation shall prevail.

ANNEX-1: ASSIGNMENT OF UNITS AND INFORMATION

Job descriptions and the titles of the employees and the units involved personal data protection are provided in the table below.

The information below only covers the job descriptions of the personnel involved in protection of personal data and all these personnel bear the duty of ensuring compliance with the storage periods of personal data concerning the processes included in the job descriptions.

TITLE	**UNIT**	**JOB DESCRIPTION**
Contract and Admin Director	Management	Responsible for taking and implementing the administrative decisions necessary for compliance with the legislation.
HR & Administration	Contract and Admin Department	Responsible for ensuring that the employees act in accordance with KVKK and other related legislation, for conducting training and awareness activities on the legislation and compliant processing of personal data by the employees.
Head of IT	Contract and Admin Department	Responsible for ensuring the security of personal data stored on electronic media in accordance with the legislation and the implementation of technical measures taken by the Company.
Lawyer / Legal Counsel	Legal Department	Responsible for conducting internal periodic and/or random audits for the Company's and its employees' compliance with KVKK.
Workplace Doctor - HR & Administration	Contract and Admin Department	Responsible for the processing and destruction of health data (sensitive personal data) of employees.
HR & Administration	Contract and Admin Department	Responsible for the destruction of personal data stored in non-electronical storage media (paper, unit cabinets, archives) and preparing reports after destruction.

ANNEX-2: TABLES OF STORAGE AND DESTRUCTION PERIODS

The storage and destruction periods of the data processed by the Company are determined based on the data categories in the Inventory based and are as given in the table below.

TABLE A – PROCESSING OF PERSONAL DATA OF EMPLOYEES AND INTERNS

PERSONAL DATA CATEGORY	**PROCESSED PERSONAL DATA IN THE CATEGORY**	**RETENTION PERIOD**	**DESTRUCTION PERIOD**
Identification	Name-surname, parents' names, date and place of birth, marital status, identity card serial number, T.C.K.N. (Turkish identity number), passport information etc.	10 years after the conclusion of business relations	Within 6 Months After Expiration of Storage Period
Communication/Contact Info	E-mail address, contact address, telephone no	10 years after the conclusion of business relations	
Personnel Files	Payroll information, disciplinary investigations, job entry-exit document records, CV/résumé information, performance evaluation reports etc.	10 years after the conclusion of business relations	
Legal Transactions	Information contained in correspondence with judicial authorities	10 years after the conclusion of business relations	
Physical Area Security	Surveillance camera recordings	2 years after the acquisition of the data	
Transaction Security	IP address, web site access information, password and password information, etc.	2 years after the acquisition of the data	
Occupational Experience	Diploma information, courses attended, vocational training information, certificates, transcript information etc.	10 years after the conclusion of business relations	
Audio-visual Recordings	Photographs and camera recordings (except for records falling in the scope of Physical Area Security data), audio recordings	10 years after the acquisition of the data	
Military Service Status	Document obtained for recruitment processes and creation of personnel files for male candidates and used for leave planning	10 years after the conclusion of business relations	
Health Data	Blood type information, disability status, personal health data, use of medical devices/prostheses	15 years after the conclusion of business relations	
Criminal Conviction and Security Measures	Criminal record	10 years after the conclusion of business relations	

TABLE B – PROCESSING OF PERSONAL DATA OF JOB CANDIDATES

PERSONAL DATA CATEGORY	PROCESSED PERSONAL DATA IN THE CATEGORY	RETENTION PERIOD	DESTRUCTION PERIOD
Identification	Name-surname, parents' names, date and place of birth, marital status, identity card serial number, T.C.K.N. (Turkish identity number), passport information etc.	2 years after the acquisition of the data (date of application to job ad or direct application via e-mail)	Within 6 Months After Expiration of Storage Period
Communication/Contact Info	E-mail address, contact address, telephone no		
Personnel Files	Payroll information, disciplinary investigations, job entry-exit document records, CV/résumé information, performance evaluation reports etc.		
Occupational Experience	Diploma information, courses attended, vocational training information, certificates, transcript information etc.		

TABLE C – PROCESSING OF PERSONAL DATA OF SUPPLIERS' EMPLOYEES

PERSONAL DATA CATEGORY	PROCESSED PERSONAL DATA IN THE CATEGORY	RETENTION PERIOD	DESTRUCTION PERIOD
Identification	Name-surname, parents' names, date and place of birth, marital status, identity card serial number, T.C.K.N. (Turkish identity number), passport information etc.	10 years after the conclusion of business relations	Within 6 Months After Expiration of Storage Period
Audio-visual Recordings	Photographs and camera recordings (except for records falling in the scope of Physical Area Security data), audio recordings		
Health Data	Blood type information, disability status, personal health data, use of medical devices/prostheses		

TABLE D – PROCESSING OF PERSONAL DATA OF SUPPLIER OFFICIALS

PERSONAL DATA CATEGORY	PROCESSED PERSONAL DATA IN THE CATEGORY	RETENTION PERIOD	DESTRUCTION PERIOD

Identification	Name-surname, parents' names, date and place of birth, marital status, identity card serial number, T.C.K.N. (Turkish identity number), passport information etc.	10 years after the conclusion of business relations	Within 6 Months After Expiration of Storage Period
Communication/Contact Info	E-mail address, contact address, telephone no		

TABLE E – PROCESSING OF PERSONAL DATA OF NEWS SUBJECTS

PERSONAL DATA CATEGORY	**PROCESSED PERSONAL DATA IN THE CATEGORY**	**RETENTION PERIOD**	**DESTRUCTION PERIOD**
Identification	Name-surname, parents' names, date and place of birth, marital status, identity card serial number, T.C.K.N. (Turkish identity number), passport information etc.	10 years after the acquisition of the data	Within 6 Months After Expiration of Storage Period
Communication/Contact Info	E-mail address, contact address, telephone no		
Audio-visual Recordings	Photographs and camera recordings (except for records falling in the scope of Physical Area Security data), audio recordings		

TABLE F – PROCESSING OF PERSONAL DATA OF PERSONS WHO SUBMIT COMPLAINTS OR DEMANDS REGARDING THE PROJECT

PERSONAL DATA CATEGORY	**PROCESSED PERSONAL DATA IN THE CATEGORY**	**RETENTION PERIOD**	**DESTRUCTION PERIOD**
Identification	Name-surname, parents' names, date and place of birth, marital status, identity card serial number, T.C.K.N. (Turkish identity number), passport information etc.	10 years after the conclusion of the project construction period	Within 6 Months After Expiration of Storage Period
Communication/Contact Info	E-mail address, contact address, telephone no		
Audio-visual Recordings	Photographs and camera recordings (except for records falling in the scope of Physical Area Security data), audio recordings		

ANNEX-3: TABLE OF UPDATES

Changes to this Policy up to this date are listed in the table below.

UPDATE DATE/VERSION CODE	**SCOPE OF UPDATES**
20.01.2020	Policy publication date