İHSAN DOĞRAMACI FOUNDATION AND SCHOOLS

Revised on June 22, 2020

POLICY ON THE PROCESSING, PROTECTION AND DESTRUCTION OF PERSONAL DATA

Effective as of October 7, 2016

CONTENTS

LEGISLATION, PURPOSE AND SCOPE

This Policy on the Processing - Protection and Destruction of Personal Data hereby has been prepared in compliance with the Constitution of the Republic of Turkey, the Law on the Protection of Personal Data date 7 April 2016 and number 6698 (referred to as the "Law" hereinafter) and other relevant laws in order to determine and declare the principles and obligations of our Institution in relation to the personal data of our students, potential students, parents, employees, visitors, potential employees, the persons and institutions with which we cooperate or which provide us services, and their employees, shareholders and authorities, and all third parties who share their personal data with us and/or contact us in any way that might lead to the sharing of personal data which are processed through automatic or non-automatic means or, provided that the process is a part of any data registry system, through automatic or non-automatic means.

This Policy hereby is published on the official website of our Institution and our schools.

I. OUR FUNDAMENTAL PRINCIPLES IN THE PROCESSING OF PERSONAL DATA

The procedures and principles applying to the processing of personal data stipulated in Article 4 of the Law are formulated parallel to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data number 108 and European Union's Data Protection Directive 95/46/EC.

Pursuant to the Law, the general principles to be complied with in the processing of personal data are as follows:

- Lawfulness and conformity with rules of bona fides.
- Accuracy and being up to date.
- Being processed for specific, limited, apparent and legitimate purposes.
- Being relevant with, limited to and proportionate to the purposes for which they are processed.
- Being retained for the period of time stipulated by relevant legislation or the purpose for which they are processed.

In this context, the principles applying to the processing of personal data are considered in the essence of all data processing operations by our Institution and it is accepted as an Institutional policy to carry out all data processing activities in line with these principles, as well as ethical values.

II. PROCESSING OF PERSONAL DATA

Personal Data

Personal data is all the information relating to any identified or identifiable person.

Processing of personal data is possible when at least one of the conditions laid down in article 5 of the Law is present.

Accordingly, the data of the data subject can be processed when one of the following conditions is met:

- The data subject has given his explicit consent,

- It is clearly provided for by the laws,
- It is mandatory for the protection of life or physical integrity of the person or of any other person who is bodily incapable of giving his consent or whose consent is not deemed legally valid,
- Processing of personal data belonging to the parties of a contract is necessary provided that it is directly related to the conclusion or fulfilment of that contract,
- It is mandatory for the controller to be able to perform his legal obligations,
- The data concerned is made available to the public by the data subject himself,
- Data processing is mandatory for the establishment, exercise or protection of any right,
- It is mandatory for the legitimate interests of the controller, provided that this processing shall not violate the fundamental rights and freedoms of the data subject.

The conditions under which personal data can be processed, that is, legal grounds for the processing of personal data, are limited by the Law and cannot be extended.

Personal Data of Special Nature

Personal data of special nature refers to the data which, if obtained by others, can lead to discrimination against or unfair treatment of the data subject.

Therefore, personal data of special nature must be protected more strictly than other personal data.

Personal data of special nature can be processed only with the explicit consent of the data subject or when certain conditions set out in the Law are met.

Personal data of special nature are defined in a limited way in the Law as data related to the 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, and the biometric and genetic data.

Personal data of special nature cannot be extended by comparison.

The Law also makes a distinction between personal data of special nature. Accordingly, the circumstances under which personal data of special nature related to health and sexual life without explicit consent and those in which the other personal data of special nature can be processed are regulated differently.

Pursuant to the Law, personal data of special nature can be processed without the explicit consent of the data subject in the following cases:

- Personal data of special nature excluding those related to health and sexual life can be processed only under the circumstances provided for in the Law,
- Personal data of special nature related to health and sexual life can be processed by any person or authorized public institutions and organizations that have confidentiality obligation, for the purposes of protection of public health, operation of preventive medicine, medical diagnosis,

treatment and nursing services, planning and management of health-care services as well as their financing.

In this context, all the conditions applying to the processing of personal data are considered by our Institution in all personal data processing procedures, and it has been adopted as Institutional Policy to carry out data processing activities in observation of these conditions. However, as an institution providing education and teaching, our Institution may be required by virtue of its nature to process the health data (such as blood type, regularly used drugs, allergy history, chronic diseases, previous operations, etc.) of its students, teachers and employees directly or indirectly in a limited and moderate way as required by and limited to its activities through electronic or non-electronic methods.

III. TRANSFER OF PERSONAL DATA

A. Transfer of Personal Data inside Turkey

Article 8 of the Law provides that the personal data obtained to be processed in line with the general principles laid down in the Law can be transferred to third parties only with the explicit consent of the data subject.

The Law stipulates the same conditions for processing personal data and transfer of these data inside Turkey.

The article also specifies the conditions which must be met for transferring personal data to third parties without the explicit consent of the data subject.

However, the legal processing of personal data inside Turkey does not mean that they can be directly transferred. In other words, conditions stipulated in Articles 5 and 6 must be satisfied for transfer to take place.

In this context, one of the conditions laid down below must be met for the transfer of personal data:

- The data subject has given his explicit consent,
- It is clearly provided for by the laws,
- It is mandatory for the protection of life or physical integrity of the person or of any other person who is bodily incapable of giving his consent or whose consent is not deemed legally valid,
- It is mandatory to process the personal data of the parties to a contract, on condition that they are directly related to the drawing up and execution of the contract,
- It is mandatory for the controller to be able to perform his legal obligations,
- The data concerned is made available to the public by the data subject himself,
- Data processing is mandatory for the establishment, exercise or protection of any right,
- It is mandatory for the legitimate interests of the controller, provided that this processing shall not violate the fundamental rights and freedoms of the data subject.

Transfer of personal data of special nature can take place when the data subject has given his explicit consent and/or it is explicitly provided for by the laws, with the exception of personal data of special nature relating to health and sexual life, and when personal data relating to health and sexual life is concerned, transfer is possible by persons under an obligation of confidentiality or by authorized institutions and establishments for the purposes of protection of public health, protective medicine,

medical diagnosis, treatment and nursing services, planning and management of health-care services as well as their financing.

Personal data can only be data belonging to the real persons, while “data controller” and “data processor” can be both natural and legal persons.

Any natural or legal person carrying out a transaction on personal data must either be a data controller or a data processor, based on the purpose and method of data processing.

In this context, any data transfer between the persons in these two categories should comply with the regulations in the Article 8 of the Law.

B. Transfer of Personal Data Abroad

According to Article 9 of the Law, personal data may be transferred abroad when

- The data subject has given his explicit consent,
- The country is approved by the Board as “Adequate Country” and existence of the circumstances provided for in the second paragraph of Article 5 and the third paragraph of Article 6 of the Law,
- If the country is not approved by the Board as an “Adequate Country”, then data controllers in Turkey and abroad commit in writing to provide an adequate level of protection and the Board has authorized this transfer in the existence of the circumstances referred to in the second paragraph of Article 5 and the third paragraph of Article 6 of the Law).

The Law stipulates the same conditions for the processing of personal data and their international transfer. However, additional measures are imposed for the transfer of personal data abroad.

Personal data can be transferred abroad if the data subject has given his explicit consent.

When there is no explicit consent, the Law lays down different provisions for international transfer of personal data according to the presence of adequate data protection in the country of transfer.

1. If Adequate Protection is Provided

Personal data can be transferred abroad when;

It is clearly provided for by the laws,

- It is mandatory for the protection of life or physical integrity of the person or of any other person who is bodily incapable of giving his consent or whose consent is not deemed legally valid,
- Processing of personal data belonging to the parties of a contract is necessary provided that it is directly related to the drawing up or execution of that contract,
- It is mandatory for the controller to be able to perform his legal obligations,
- The data concerned is made available to the public by the data subject himself,
- Data processing is mandatory for the establishment, exercise or protection of any right,
- It is mandatory for the legitimate interests of the controller, provided that this processing shall not violate the fundamental rights and freedoms of the data subject.

When personal data of special nature are concerned, if the transfer country has an adequate level of protection, personal data with the exception of data relating to health and sexual life can be transferred

abroad if it is clearly provided for by the laws, while personal data relating to health and sexual life can be transferred to countries with sufficient protection without the explicit consent of the data subject by persons under an obligation of confidentiality or by authorized institutions and establishments for the purposes of protection of public health, protective medicine, medical diagnosis, treatment and nursing services, planning and management of health-care services as well as their financing.

2. Transfer to Countries without Adequate Protection

- Fulfillment of at least one of the requirements listed in the Articles 5 and 6 of the Law,
- Written commitment of the data controllers in Turkey and the relevant country to provide sufficient protection,
- Board approval

are required.

In this context, our Institution has established an Institutional principle to act in accordance with the provisions listed above and on condition that the requirements are met, personal data can be transferred to all governmental and private institutions and organizations allowed and/or required by statutory provisions, İhsan Doğramacı Bilkent University and Schools, schools and our program partners at home and abroad, persons and firms which offer us services and/or which we direct you to use their services, persons and institutions whose services we use or with whom we cooperate to carry out our operations, persons, firms and our units and personnel who can take measures and make the necessary interventions particularly in relation to health problems, other third persons who are responsible for and support us in taking security measures such as safeguarding your personal data, preventing unauthorized access and unlawful processing, and all third persons who are related to the activities of our Institution in a limited and moderate way.

IV. DATA CHANNELS

Personal data can be collected by our Institution in any oral, written, non-electronic or electronic medium through, but not limited to, channels such as school application and registration forms, our websites and your e-mails, mobile applications, collected forms, health reports, all types of software, programs, systems, applications, and platforms, as well as all digital and online media and systems not limited to those stated above, contracts, applications, forms, proposals, sound and video recordings, cookies used by our computers to recognize you in website visits etc. by student affairs and registration units and other school employees, administrative and academic units, secretariat, reception and security offices, our school and program partners in Turkey and abroad, and transportation bus company and other companies which provide us services.

V. DATA PROCESSING PURPOSES

The purposes and legal bases of processing and transfer of your personal data include, besides fulfillment of legal and contractual obligations, carrying out the relations between the school and students, updating contact information, opening and follow-up of student and parent registrations, provision of all our services, conducting the registration and ensuing procedures, meeting financial requirements including invoicing, enabling relevant units to contact you and ensuring your satisfaction in general, identifying your needs, guaranteeing the legal and physical safety of our institution, our students and yours, continuation of education and other services in line with the demands of the legislation, contracts and technology, improvement of our services, undertaking promotional activities, carrying out analyses,

management of all records and documents in line with the purpose of processing, establishing and maintaining communication between our Institution and graduates and carrying out the required operations and procedures not limited to the foregoing, establishing communication, fulfillment of data storage, reporting and information obligations provided for by the legislation, relevant regulatory institutions and other authorities, ensuring your use of schools and programs in Turkey and abroad and meeting other requirements laid down in the legislation.

VI. OUR OBLIGATIONS

A. Obligation to Inform

The law gives data subject a right to be informed about by whom, for what purposes and for which legal reasons/basis their data are to be processed, for what purposes and to whom the data may be transferred, and these issues are addressed under the obligation to inform of the controller.

Accordingly, as data controller, our Institution has assumed the obligation to inform and accepted it as Institutional Policy to act in accordance with its obligations to inform data subjects about

- The identity of the controller and of his representative, if any,
- The purpose of data processing,
- To whom and for what purposes the processed data may be transferred,
- The method and legal reason of collection of personal data,
- Other rights referred to in Article 11.

In this context, our obligation to inform can be accessed through the http://www.obi.bilkent.edu.tr address.

B. Obligations regarding Data Security

Pursuant to Article 12 regulating data security of the Law, our Institution as data controller is obliged to

- Prevent unlawful processing of personal data,
- Prevent unlawful access to personal data,
- Ensure the retention of personal data
- Ensure the destruction of personal data, when necessary.

Data controller should take all necessary technical, software, hardware and administrative measures to provide a sufficient level of security in order to fulfill its obligations.

If the data is processed by a natural or legal person on behalf of the data controller, the controller shall be jointly responsible with these persons for taking the necessary measures.

The Law also requires the data controller to be audited regarding data security.

The data controller is required to conduct necessary auditions or have them conducted in his own institution or organization in order to implement the provisions of the Law.

Therefore, the controller can conduct this audition himself or through a third party.

On the other hand, data controllers and processors cannot disclose the personal data they collected to others and cannot use them for purposes incompatible with those for which they were collected in breach of the provisions of the Law. This obligation shall be valid even after the end of the controllers' and processors' term. Otherwise, data controllers or data processors who act to the contrary shall be held personally responsible.

Finally, if the processed personal data are obtained unlawfully by third parties, the data controller shall notify the data subject and the Board without delay. The Board, can announce such breach, when necessary, on its official website or through other methods it deems appropriate.

In this context, our Institution takes the principles regarding data security into account in all its operations, takes the maximum care to ensure data security, and establishes it to do so as its Institutional policy.

C. Obligation to Respond to Data Subject Access Requests

Data controllers should respond to requests submitted by data subjects in writing or through other means identified by the Institution regarding the implementation of the Law free of charge and within 30 (thirty) days, based on the nature of the request.

However, if the request necessitates a responding fee, the data controller can charge the requestor a fee set by the Board. If the requestor fails to fulfill his/her obligation to pay the concerned fee, it is at the discretion of our Institution to cover the fee or not to respond to the request.

If the data controller accepts the request or refuses it with justification, he informs the data subject in writing or electronically.

If the request is accepted, the data controller does whatever is necessary to fulfill the request.

If the request is made due to a fault by the data controller, any fee collected should be repaid to the data subject.

In case the request is refused, the response is found insufficient or the request is not responded to within the set time period, the data subject can file a complaint to the Board within 30 (thirty) days after the receipt of the data controller's response and in any case within 60 (sixty) days after the date of making the request.

In this context, it has been determined as our Institutional policy to fulfill the obligations to respond to the data subjects' requests.

D. Obligation to Erase, Destroy or Anonymize Personal Data upon the Disappearance of the Reason of Processing

Erasure of Personal Data is the process of making personal data inaccessible and unusable for all relevant users.

Data controller is responsible for taking all the technical, software, hardware and administrative measures to render the erased personal data inaccessible and unusable for all relevant users of personal data.

Destruction of Personal Data refers to the process of rendering personal data inaccessible, irretrievable and unusable by anyone in any case.

Data controller is responsible for taking all the technical, software, hardware and administrative measures related to the destruction of personal data.

Anonymization of Personal Data is rendering personal data impossible to link with any identified or identifiable natural person even by matching them with other data. In order for personal data to be anonymized, they must be made irrelevant to identified or identifiable natural persons in spite of the use of appropriate techniques in terms of the registry medium and the relevant field of activity such as retrieving and matching personal data with another data by controller, receiver or receiver groups.

Data controller is liable for taking any technical, software, hardware and administrative measures for anonymization of personal data.

Erasure, destruction or anonymization of personal data, although they were processed in line with the legislation, upon disappearance of the reasons of processing ex officio or upon the request of the data subject is accepted as our Institutional policy, and destruction processes [1] are presented below.

E. Obligation to Abide by Board Decisions

If the Board determines the existence of a data breach upon a complaint or ex officio, the Board resolves to ask the data controller to settle the breach and notifies all concerned parties of its decision. The data controller must fulfil the decision notice without undue delay and within thirty days of receipt.

VII. THE RIGHTS OF DATA SUBJECT

In the framework of Article 11 of the Law, the data subject has the right to apply to the data processor at any time to

- To learn whether his personal data are processed or not,
- To request information if his personal data are processed,
- To learn the purpose of the processing of his data and whether this data is used for intended purposes,
- To know the third parties to whom his personal data is transferred at home or abroad,
- To request the rectification of the incomplete or inaccurate data, if any,
- To request the erasure or destruction of his personal data which is processed inaccurately or incompletely,
- To request notification of the third parties to whom his personal data has been transferred of the rectification, erasure or destruction operations,
- To object to the processing, exclusively by automatic means, of his personal data, which leads to an unfavorable consequence for the data subject,
- To request compensation for the damage arising from the unlawful processing of his personal data.

Our Institution has accepted to act in accordance with the rights of data subjects as its Institutional policy, and data subjects can submit their requests regarding the rights indicated above by writing to the e-mail address [2] …… or sending a letter with a return receipt request to the …….. postal address.

VIII. DESTRUCTION OF PERSONAL DATA

A. Reasons Requiring Destruction

Personal data are erased and destructed by our Institution upon the request of the data subject or erased, destructed or anonymized ex officio in cases where

- Legislative provisions serving as the basis of processing are amended or abolished,
- The purpose for which the data is processed or retained has disappeared,
- Data subject withdraws his explicit consent when the personal data is processed only on the basis of the data subject's explicit consent,
- The Board accepts the data subject's request to have his personal data erased or exterminated in the framework of his rights under the article 11 of the Law,
- The data subject files a complaint to the Board in case that our Institution refuses the data subject's request to have his personal data erased, destructed or anonymized, the data subject finds the given response insufficient or our Institution fails to respond to the request in the time period provided for by the Law, and the Board endorses the data subject's complaint,
- The maximum time period for which personal data should be retained is exceeded and there is no condition to justify retention of personal data for an extended period of time (in this case, our Institution will be able to continue retaining all kinds of personal data without destructing them and without adhering to the stated period of time or the stated maximum period of time).

B. Methods of Destructing Personal Data

1. Erasure of Personal Data

Personal Data on Servers

Of the personal data on servers, those for which the required period of retention has ended are erased by the system administrator by revoking the access authorization of relevant persons.

Personal Data in the Electronic Medium

Of the personal data in the electronic medium, those for which the required period of retention has ended are rendered inaccessible and unusable by other employees (relevant users) except the database administrator.

Personal Data in the Physical Medium

Of the personal data in the physical medium, those for which the required period of retention has ended are rendered inaccessible and unusable by other employees except the unit administrator in charge of the document archives.

Additionally, these data are rendered unreadable by blotting out/erasing.

Personal Data on Portable Media

Of the personal data kept in flash-based storage media, those for which the required period of retention has ended are kept in secure media by being assigned a password by the system administrator who is the only person given access authorization.

2. Destruction of Personal Data

Personal Data in the Physical Medium

Of the personal data in paper medium, those for which the required period of retention has ended are destructed irreversibly by being shredded in paper shredders.

Personal Data in Optic / Magnetic Media

If optic media and magnetic media are used, of the personal data in these media those for which the required period of retention has ended are subjected to physical destruction procedures like melting, burning or pulverization. Additionally, magnetic media is processed in a special device which exposes it to a powerful magnetic field and renders the data unreadable.

Anonymization of Personal Data

Anonymization of personal data is rendering personal data impossible to link with any identified or identifiable natural person even by matching them with other data.

In order for personal data to be anonymized, they must be made irrelevant to identified or identifiable natural persons in spite of the use of appropriate techniques in terms of the registry medium and the relevant field of activity such as retrieving and matching personal data with another data by controller or third parties.

3. Retaining Data for the Period of Time Provided for in the Relevant Legislation or Required for the Purpose of Processing

Our Institution retains personal data only for the period of time provided for in the relevant legislation or required for the purpose of processing. In this framework, our Institution first determines whether a certain time period is stipulated in the legislation for the retention of personal data and abides by the given period, if there is one. If the Legislation does not specify a certain period, our Institution retains personal data for the time period required for their processing. At the end of the concerned period or when the purposes for processing disappear, personal data are erased, destructed or anonymized by our Institution.