Personal Data Protection Law (PDPL) Information Text

We, as SAINTADVISER, respect and attach importance to the privacy of our client private lives. Therefore, we would like to share with you the information text we have prepared in our capacity as Data Controller in accordance with the Personal Data Protection Law No. 6698 ("the PDPL"), in order to protect fundamental rights and freedoms in the use of personal data.

In this text, you can obtain information about the purpose for which your personal data will be processed within the scope of the PDPL, to whom and for what purpose your processed personal data may be transferred, the collection of your data, the legal cause and other rights.

You can apply for us at any time you wish and learn the purpose of using your personal data, and with which entities and for what purpose they are shared, or you can send e-mail about the "Policy for the Protection and Processing of Personal Data" anytime to info@saintadviser.com.

Purposes of Processing Your Personal Data

You, as our client, may transmit to us your personal data, special categories of personal data(name, surname, company name, e-mail address, country name, company sector, city name) via channels such as e-mail or website, verbally, in writing, or through electronic media. We process these data you have transmitted to us, in order to provide with you better and safer services.

Without your explicit consents, your personal data and special categories of personal data will not be used for any purposes other than those mentioned above, and will not be shared with or transferred to third parties, with the exception of legal obligations and public institutions/ organizations.

Based on your explicit consents, your personal data may be shared with our affiliates in the Country or abroad, our directly or indirectly associated companies, our joint ventures, or with the public institutions or organizations authorized to request for such data due to a legal necessity, and with the entities, suppliers, authorized vendors and other business partners in the Country or abroad, with whom we are contracted as required by our activities, provided that the adequate measures are taken.

Collection of Your Personal Data

In compliance with the legislation in force, your personal data may be collected verbally, in writing or in electronic environment via channels such as our Company, our shareholders, our group companies, our affiliates, our agencies, or our solution partners with whom we cooperate or have a contractual relationship.

Storage of Your Personal Data

When you share your personal data with our Company, you should know that the accuracy and keeping of these data up-to-date are important for the rights you have within the scope of the Personal Data Protection Law No. 6698, and with regard to the other relevant legislation. In case of providing inaccurate or false information, the responsibilities and liabilities to arise therefrom entirely lie on you. You can report to the address (info@saintadviser.com) any changes and/or updates regarding your personal data you have shared with us.

Erasure, Destruction or Anonymization of Your Personal Data

Your personal data processed for the purposes mentioned in this information text will be erased, destroyed, or continued to be used by us through anonymization, when the purpose requiring the processing ceases to exist or at the expiration of the periods determined by the laws.

Protection of Your Personal Data

Our Company takes all kinds of technical and administrative measures necessary to protect personal data against unauthorized access and against loss, misuse, disclosure, alternation or destruction of these data. In the event that personal data are damaged or acquired by third parties as a result of possible attacks on our website and network system, our Company will immediately notify this circumstance to you and the Personal Data Protection Board.

Rights of the Data Subjects

You have the right to apply for our Company and thus, have the right to:

A. Learn whether or not your personal data are processed;

B. Request for relevant information, if your personal data have been processed;

C. Learn the purposes of processing your personal data and whether or not those data are used in compliance with the purposes;

D. Know the third parties in the Country or abroad, to whom your personal data are transferred;

E. Request for rectification in case your personal data have been processed incompletely or inaccurately;

F. Request for erasure or destruction of your personal data;

G. Request that the operations carried out under the subparagraphs (d) and (e) of article 11/1 of the PDPL be notified to the third parties to whom your personal data are transferred;

H. Object to occurrence of any results that are to your detriment through analysis of your processed data exclusively by automated systems;

I. Request for compensation of the damages in case you incur damages due to the unlawfully processing of your personal data.

You can send e-mail about your requests regarding your above-mentioned rights by completing the "Information Application Form" signed with your wet signature. Your applications will be replied as soon as possible or in no later than 30 days after they are received by our Company, depending on their contents. The applicants may be requested to submit any other relevant information and documents.

Policy For The Protection And Processing Of Personal Data

1. Objective

The objective of this Policy is:

- to describe the methods adopted for the protection of personal data and personal data processing activities in compliance with the Personal Data Protection Law No. 6698 ("the PDPL") in all kinds of activities carried out by FALLING ACTION LLC. ("the Firm"), and
- to ensure transparency by informing all persons whose personal data are processed by the Firm, particularly the Firm's administrative officials, personnel, customers, personnel candidates, suppliers, visitors, the employees of the entities the Firm cooperates with and third parties about the principles adopted and the systems established by the Firm for the protection of personal data.

2. Scope

This Policy covers all personal data which pertain to the persons whose personal data are processed automatically or non-automatically -provided that they constitute a part of any data recording system- by the Firm in the Firm's processes, particularly the personal data of the Firm's administrative officials, personnel, customers, personnel candidates, suppliers, visitors, the employees of the entities the Firm cooperates with and third parties.

3. Authorities and Responsibilities

In the fulfillment of the requirements regarding the destruction of data as specified by the Law, the Regulation and the Policy within the Firm; all employees, outsourced service providers and everyone storing and processing personal data in another way at the entity are responsible for the fulfillment of these requirements.

Each business unit is obliged to store and protect the data generated in its own business processes.

The relevant manager and the team to be designated by the relevant manager shall decide on destructions that will affect business processes and cause data integrity to deteriorate, data loss and occurrence of results contrary to the statutory provisions, taking into consideration the type of the related personal data, the systems in which it is included and the business unit performing the data processing.

The responsibility for the transactions, such as receiving or admitting on behalf of the data controller the correspondences with and the notifications from the Personal Data Protection Authority, and registration with the registry, lies on the data controller's contact person.

4. Definitions and Abbreviations

Firm: FALLING ACTION DANIŞMANLIK VE REKLAMCILIK SANAYİ VE TİCARET LİMİTED ŞİRKETİ.

Explicit Consent: Consent which is related to a specific matter, based on information and expressed with free will.

Relevant/Authorized User: With the exception of the persons or units that are responsible for the technically storage, protection and backing up of data; persons who process personal data in line with the authorization they obtained or the instruction they received from the data controller or within the data controller's organization.

Destruction: Erasure, destruction or anonymization of personal data.

Law/PDPL: The Personal Data Protection Law No. 6698.

Recording Medium: All kinds of mediums containing personal data processed automatically, completely or in part, or non-automatically provided that they constitute a part of any data recording system.

Personal Data: All kinds of information related to an identified or identifiable natural person.

Processing of Personal Data: All kinds of operations carried out on the data, such as obtaining, saving, storing, protecting, modifying, editing, describing, transferring, receiving, making available, classifying or blocking the use of the personal data automatically, completely or in part, or non-automatically provided that they constitute a part of any data recording system.

Anonymization of Personal Data: Rendering personal data non-associable with an identified or identifiable natural person under any circumstances, even by matching with other data.

Erasure of Personal Data: Rendering personal data inaccessible and non-reusable for the relevant/authorized users under any circumstances.

Destruction of Personal Data: The operation of rendering personal data inaccessible, unrecoverable and non-reusable by anyone under any circumstances.

Board/PDP Board: Personal Data Protection Board.

Special Categories of Personal Data: Data related to individuals' race, ethnicity, political opinions, philosophical beliefs, religion, sect or other beliefs, appearance; association, foundation or trade union memberships, health, sexual life, criminal convictions and security measures, and individuals' biometric and genetic data.

Periodic Destruction: The operation of erasure, destruction or anonymization to be performed -as specified in the Policy for the Storage and Destruction of Personal Data- ex-officio

in repetitive intervals in case all the personal data processing conditions referred to in the Law cease to exist.

Data Subject/Relevant Person: A natural person whose personal data is processed.

Data Processor: A natural or legal person who processes personal data on behalf of a data controller, by virtue of the authority granted to that natural or legal person by that data controller.

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

By-Law: By-Law on the Erasure, Destruction or Anonymization of Personal Data, published in the Official Gazette on 28 October 2017.

5. Policy for the Protection and Processing of Personal Data

By the Policy, the Firm sets forth concretely the measures necessary for and the processes applied to the protection and processing of personal data. The Firm acknowledges that it shall comply with the legislation in force, in cases where there is an inconsistency between this Policy and the relevant laws and by-laws, or in case the Policy is not up-to-date in line with the updated legislation. This Policy shall be updated in accordance with the amendments to the Law, the By-Law and the legislation.

5.1.1. Ensuring the security of personal data

The Firm takes all kinds of technical and administrative measures necessary to ensure the appropriate level of security required for the protection of personal data.

The Firm takes measures for the following matters prescribed by article 12/1 of the PDPL:

- Preventing unlawful processing of personal data,
- Preventing unlawful access to personal data,
- Ensuring protection of personal data.

The measures taken by the Firm to ensure the security of personal data are detailed in the sections below.

5.1.2. Administrative Measures

In order to ensure data security, the Firm employs knowledgeable and experienced persons and provides its personnel with the necessary information security awareness and trainings on the protection of personal data.

The Firm takes the necessary administrative measures in order to ensure the security of personal data and carries out inspections on whether the employees work in accordance with these measures. The company defines accesses and authorizations in accordance with the legal compliance requirements determined on a business unit basis, and at a level that will not cause disruption to business processes. The Firm defines the rules on accessing personal data and the authorizations to access personal data by the employees working in the information technology units. The employees are informed that they shall not disclose the personal data -they have accessed- to others in violation of the provisions of the PDPL and that they shall not use those personal data for any purposes other than the processing purposes and that these responsibilities shall survive even after they resign, retire from or leave the office. In this direction, necessary commitments are obtained from the employees. Regarding the sharing of personal data with third parties, a framework contract shall be signed with the persons with whom personal data will be shared, or the Firm shall ensure data security under the provisions it will add into the contracts. The third parties with whom personal data are shared accept the provisions that they shall take necessary security measures to protect personal data and that they shall ensure the compliance with these measures in their own organizations. In case it is found that the processed personal data are obtained by others through illegal ways despite the measures taken, the data controller's contact person shall notify this issue to the relevant person and the PDP Board. It shall be investigated how personal data are obtained by others. In order to eliminate the weakness that it has identified, the Firm shall implement the necessary administrative measures, and take technical measures in case of need.

5.1.3. Technical Measures

The Firm carries out the internal checks necessary for the systems established. The Firm operates the processes of conducting risk analysis, data classification, information security risk assessment and business impact analysis within the scope of the systems established. In line with these processes, technical measures are taken in accordance with the developments in technology. Infrastructure investments are made, as compatible with developing technology.

The Firm ensures the installation of software and hardware containing anti-virus systems and firewalls. The Firm uses the versions of its systems for which the necessary security measures are taken against current and known vulnerabilities. The Firm ensures that the authorizations to access personal data, granted to the employees in the information technology units, are kept under control.

The physical spaces, storing the personal data being processed in the Firm, are protected by taking the necessary physical security measures against theft and loss.

The passwords, which are used for access to the areas such as systems, applications, databases, etc. containing personal data, are generated through a complex algorithm, and the systems force the use in this way.

The Firm makes the definitions of access and authorization in accordance with the legal compliance requirements determined on a business unit basis. The Firm checks the compliance of the accesses with the authorizations. The Firm reports to the relevant parties the information obtained as a result of checking the security of the systems.

The points that pose a risk are identified and the necessary technical measures are taken accordingly.

5.1.4. Inspections carried out for the sustainability of personal data protection

The Firm carries out necessary inspections and have necessary inspections carried out in compliance with article 12 of the PDPL.

The Firm regularly carries out penetration tests on the systems for technical vulnerabilities that may occur in the systems. The systems are monitored regularly by the information technology units. Furthermore, system trace records are monitored to ensure security against cyber-attacks. Necessary technical and administrative measures are taken for the findings identified by monitoring the systems and the data generated by the warning systems, as well as by the inspections on the management systems.

5.1.5. Measures taken in case of unauthorized disclosure of personal data

In case of unauthorized disclosure of personal data processed in compliance with article 12 of the PDPL, the Firm shall inform the relevant data subject and the PDP Board about the issue.

If deemed necessary by the PDP Board, this circumstance may be announced on the website of the PDP Board or by any other method.

5.1.6. Measures implemented to ensure the protection of personal data by third parties

The Firm ensures that the sanction articles for preventing unlawful processing of personal data, for preventing unlawful access to personal data and for ensuring protection of data are mutually inserted in the contracts concluded with third parties by the Firm. Confidentiality agreements are signed before sharing information with third parties. Necessary information is provided to third parties in order to raise awareness.

5.1.7. Measures implemented for the protection of special categories of personal data

It is necessary to take adequate measures for special categories of personal data both due to their characteristics and since they may cause victimization of or discrimination among individuals. Certain personal data, which have the risk of causing victimization of or discrimination among individuals when processed unlawfully, are determined to be "special categories of personal data" by article 6 of the PDPL.

Data related to race, ethnicity, political opinions, philosophical beliefs, religion, sect or other beliefs, appearance; association, foundation or trade union memberships; health, sexual life, criminal convictions and security measures, and biometric and genetic data are special categories of personal data.

The Firm takes the measures necessary in the protection of the data which are determined to be "special categories of personal data" by the PDPL and are processed lawfully. In the technical and administrative measures taken to protect personal data, sensitivity is shown for special categories of personal data.

The Firm will process special categories of personal data, provided that the adequate measures to be determined by the PDP Board are taken. The data subject's explicit consent shall be obtained, before processing his/her special categories of personal data. In the absence of the data subject's explicit consent, his/her personal data may be processed by virtue of the authorization granted by the laws in accordance with the following criteria:

~ A data subject's special categories of personal data, other than his/her health and sexual life, may be processed in the cases expressly allowed by the laws; and

~ A data subject's special categories of personal data related to his/her health and sexual life may be transferred to and processed by competent institutions and organizations or persons who are under the confidentiality obligation, for the purposes of protecting the public health, conducting preventive medicine, medical diagnosis, treatment and nursing services and for the planning and management of healthcare services and their financing.

5.1.8. Creating awareness to ensure the protection of personal data

Necessary information is provided to and trainings are organized for the business units and their effectiveness is measured, in order to expand the awareness for ensuring that personal data are prevented from unlawful processing, unlawful access and for ensuring that personal data are under protection. "The Policy for the Protection and Processing of Personal Data" is published on the website of our Corporation. The employees of our Corporation are informed about this Policy.

In case of an amendment to the relevant laws, by-laws or legislation, the policies are revised and then, they are re-announced to the employees.

5.2. Principles for the processing of personal data

Article 4/2 of the PDL determines the principles for the processing of personal data. The Firm processes personal data in compliance with these principles.

The processing of personal data is performed in accordance with the following principles:

- Lawfulness and compliance with the rules of objective good faith.
- Accuracy, and up-to-dateness when needed.
- Processing for certain, clear and legitimate purposes.
- Compliance with the principle of proportionality and being limited to and in connection with the processing purposes.
- Retention until expiration of the period stipulated by the relevant legislation or necessary for the processing purposes.

5.3. Conditions for the processing of personal data

A substantial part of the data handled by the Firm as a public corporation is processed by the Firm by exercising the powers mandatory to be exercised for the protection of public order and due to legal necessities. Pursuant to article 5/2 of the PDPL, in cases where:

- data processing is expressly permitted by the laws;
- it is mandatory to process personal data in order to protect the life or physical integrity of an individual or another person where the individual's consent is not deemed legally valid or the individual is incapable of giving explicit consent because of de facto impossibility;
- it is necessary to process personal data pertaining to the parties of a contract, provided that this is directly related to the conclusion or performance of such contract;
- it is mandatory to process personal data in order for the data controller to fulfill its legal obligations;
- the relevant person has made his/her data public;
- data processing is mandatory for the establishment, exercise or protection of a right; or
- processing of data by the data controller is mandatory for its legitimate interests, provided that the fundamental rights and freedoms of the relevant person are not harmed; the Firm may process such personal data without seeking explicit consent.

For the cases other than those listed above, the Firm processes personal data only after obtaining explicit consents of the data subjects.

5.4. Destruction of personal data

The personal data obtained by the Firm will be destroyed by the Firm in line with the requests of the personal data subjects, due to legal necessities and if the use of personal data is not mandatory for the protection of public order. The personal data pertaining to the data subjects shall be destroyed based on the decision to be taken by the Corporation, when the requirements for continuing the service, fulfilling legal obligations, planning employee rights and fringe benefits cease to exist.

5.5. Transfer of personal data to the persons in the Country

With respect to the sharing of personal data with third parties, the Firm meticulously complies with the conditions set out in the PDPL, provided that the provisions contained in other laws are reserved. Within this framework, personal data are not transferred to third parties in the absence of the data subject's explicit consent. However, in the existence of one of the following conditions set out by the PDPL, personal data may be transferred without obtaining data subjects' explicit consents:

- In case of express permission by the laws;
- In case of necessity in order to protect the life or physical integrity of an individual or another person where the individual's consent is not deemed legally valid or the individual is incapable of giving explicit consent because of de facto impossibility;
- In case it is necessary to process personal data pertaining to the parties of a contract, provided that this is directly related to the conclusion or performance of such contract;
- In case of necessity in order for the data controller to fulfill its legal obligations;
- In case the data subject has made his/her data public;
- In case data processing is mandatory for the establishment, exercise or protection of a right;
- • In case processing of data by the data controller is mandatory for its legitimate interests, provided that the fundamental rights and freedoms of the data subject are not harmed.

Provided that adequate measures are taken; in case of permission by the laws with regard to the special categories of personal data other than health and sexual life, on the other hand, when it comes to the special categories of personal data related to health and sexual life, your personal data may -without obtaining explicit consent- be transferred for the purposes such as:

- Protecting the public health,
- Conducting preventive medicine,
- Medical diagnosis,
- Treatment and nursing services,
- Planning and management of healthcare services and their financing.

In the transfer of special categories of personal data, the conditions specified as to the terms of processing these data are also observed.

5.6. Transfer of personal data to the persons abroad

With respect to the transfer of personal data abroad, the explicit consents of the data subjects are sought by the Firm within the scope of the PDPL. However, in the existence of the conditions allowing processing of personal data, including special categories of personal data, without explicit consent of the data subject, such personal data may be transferred to foreign countries by our Corporation without seeking the data subject's explicit consent, provided that adequate protection is provided in those countries to which personal data will be transferred. If the country to which personal data will be transferred is not designated by the Board as one of the countries providing adequate protection, our Corporation and the data controller/data processor in the relevant country shall make a written commitment for the adequate protection.

The Firm does not transfer personal data to foreign countries in any way and does not keep personal data on the servers held in foreign countries.

5.7. Rights of personal data subjects

The data subject rights arising from the Personal Data Protection Law are listed by article 11 of the same Law. These rights are as follows:

Article 11- (1) Each data subject has the right to apply for the data controller about him/her and thus, has the right to:

- learn whether or not his/her personal data are processed;
- request for relevant information, if his/her personal data have been processed;
- know the third parties in the Country or abroad, to whom his/her personal data are transferred;
- request for rectification in case his/her personal data have been processed incompletely or inaccurately;
- request for erasure or destruction of his/her personal data within the framework of the conditions prescribed by article 7 of the Law;
- request that the operations carried out under the subparagraphs (d) and (e) of article 11/1 be notified to the third parties to whom his/her personal data are transferred;
- object to occurrence of any results that are to his/her detriment through analysis of his/her processed data exclusively by automated systems;
- request for compensation of the damages in case he/she incurs damages due to the unlawfully processing of his/her personal data.

- The requests for the exercise of the rights listed above may be submitted by filling up the "Personal Data Subject Application Form". As required by the Law, details of the data controller and the data controller's contact person are as follows:

Data controller : FALLİNG ACTION DANIŞMANLIK VE REKLAMCILIK SANAYİ VE TİCARET A.Ş.

Data controller's contact person : IT Personnel

5.8. Obligation to inform

Under article 10 of the PDPL, it is necessary to inform data subjects before their personal data are obtained or at the latest while their personal data are obtained. The information necessary to be provided to the data subjects within the framework of the obligation to inform is as follows:

- The identity of the data controller and of its representative, if any,
- For what purpose the personal data will be processed,
- To whom and for what purpose the processed personal data may be transferred,
- The method and legal cause of the personal data collection,
- The other rights listed by article 11 of the PDPL.

On the other hand, within the framework of article 28/1 of the PDPL, the obligation to inform does not apply in the following cases:

- In case personal data are processed by natural persons within the context of the activities merely related to those natural persons or related to their family members staying at the same house, provided that the data are not transferred to third parties and that the data security-related obligations are observed;
- In case personal data are processed for the purposes of official statistics and for the purposes such as research, planning and statistics through anonymization;
- In case personal data are processed for the purposes of art, history, literature or science or within the context of the freedom of expression, provided that the data do not violate the national defense, the national security, the public safety, the public order, the economic security, the privacy of private life or personal rights or that they do not constitute an offense;
- In case personal data are processed within the context of preventive, protective and intelligence-related activities carried out by public institutions and organizations to which the laws make the assignment and grant the authorization for ensuring the national defense, the national security, the public safety, the public order or the economic security;
- In case personal data are processed by judicial or execution authorities in relation to investigation, prosecution, judicial or execution proceedings.

5.9. Conditions for the erasure, destruction and anonymization of personal data

The personal data obtained by the Firm will be erased, destroyed or anonymized by the Firm in line with the requests of the personal data subjects, due to legal necessities and if the use of personal data is not mandatory for the protection of public order.