

**“KORUMA KLOR ALKALİ SANAYİ VE TİCARET ANONİM ŞİRKETİ”
POLICY ON PROTECTION AND PROCESSING OF PERSONAL DATA**

09.12.2019

Index

- 1. PREAMBLE 4
- 2. PURPOSE OF THE POLICY 4
- 3. SCOPE OF THE POLICY 5
- 4. DEFINITIONS 5
- 5. PROCESSING OF PERSONAL DATA 6
 - 5.1. Principles Applicable to Processing of Personal Data 6
 - 5.1.1 Processing Personal Data in Compliance with Laws and Rules of Bona Fides 7
 - 5.1.2 Ensuring Accuracy and Up-to-dateness of Personal Data, where necessary 7
 - 5.1.3. Processing of Personal Data for Specific, Explicit and Legitimate Purposes 7
 - 5.1.4. Processing in a Way being Relevant with, Limited to and Proportionate to the Purposes for Which They are Processed 8
 - 5.1.5. Preserving Personal Data for the Period of Time Stipulated by Legislation or the Purpose for Which They are Processed 8
 - 5.2. Processing of General Quality Personal Data 8
 - 5.2.1. Existence of Explicit Consent of Data Subject 8
 - 5.2.2 It is Clearly Stipulated under the Laws 9
 - 5.2.3. Not Obtaining Explicit Consent Due to Actual Impossibility 9
 - 5.2.4. It is Directly Related to Establishment or Execution of Contract 9
 - 5.2.5. It is Mandatory for the Company to Fulfill its Legal Obligation 9
 - 5.2.6. Data is Made Available to Public by Data Subject 9
 - 5.2.7. It is mandatory for the establishment, exercise or protection of any right 10
 - 5.2.8. It is mandatory for legitimate interest of the Company 10
 - 5.3. Processing of Special Quality Personal Data 10
 - 5.4. Transfer of Personal Data 11
 - 5.4.1. Transfer of Personal Data in the Country 11
 - 5.4.2. Transfer of Personal Data Abroad 12
- 6. PROCESSING OF PERSONAL DATA AT ENTRANCES OF OR WITHIN BUILDING AND FACILITY 14
 - 6.1. Monitoring Building and Facilities through Security Cameras 14
 - 6.2. Visitors' Entrance to Building and Facilities of the Company 15
- 7. DATA IN RELATION TO INTERNET ACCESS AT BUILDING AND FACILITIES 15
- 8. PERSONAL DATA OF WEBSITE VISITORS 15
- 9. SECURITY OF PERSONAL DATA 16
- 10. ERASURE, DESTRUCTION AND ANONYMIZATION OF PERSONAL DATA 17
- 11. RIGHTS OF DATA SUBJECT AND APPLICATION TO THE COMPANY 17

11.1. Rights of Data Subject	18
11.2. Exercise of Data Subject's Rights	18
11.3. Exceptions of Data Subject's Right of Application	19
11.4. Responding to Data Subject's Application	20

1. PREAMBLE

“KORUMA KLOR ALKALİ SANAYİ VE TİCARET ANONİM ŞİRKETİ” (*Hereinafter referred to as “Company”*) places great importance on personal data protection. We show sensitivity in protection of personal data of our partners, customers, employees, candidate employees, company officials, employees of affiliates, company employees that we work together, shareholders, officers, visitors and third parties.

As stipulated in article 20 of the Turkish Constitution, everyone has a right to request the protection of its personal data. This right includes information about data subject’s personal data, access to such data, request erasure or correction of such data, and learn whether such data is used in accordance with the purpose. Personal data can only be processed under the conditions set forth in the Law or upon data subject’s explicit consent.

In accordance with the activities or requirements of the Company, protection and development of a right of “Protection of Personal Data” of our Partners, customers, employees, candidate employees, company officials, employees of affiliates, company employees that we work together, shareholders, officers, visitors and third parties, which is a Constitutional right, is adopted as a company policy. This Policy reveals the principles adopted by the Company on processing and protection of personal data.

2. PURPOSE OF THE POLICY

This Policy is prepared with a view to procuring execution of activities coherently within the Company in order to comply with the Law on Personal Data Protection No. 6698 (Hereinafter referred to as “PDPL”), the resolution of Personal Data Protection Board and the secondary legislation.

Furthermore, it is aimed to inform data subjects in the most transparent way about the activities carried out by the Company in order to process personal data and provide security, measures taken and the principles of the Company.

3. SCOPE OF THE POLICY

This policy relates to technical and organizational measures for the security of personal data and transactions of any kind on 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.

4. DEFINITIONS

In this Policy;

- a. **Explicit Consent:** means freely given, specific and informed consent,
- b. **Anonymizing:** means rendering personal data impossible to link with an identified or identifiable natural person, in any manner including matching them with other data,
- c. **Data subject:** means the natural person, whose personal data is processed,
- d. **Relevant user:** means people processing personal data within the body of the organization of data controller or in accordance with the authority and instruction given by the data controller apart from person or unit being responsible for technically storage, protection and backup of data,
- e. **Demolition:** means erasure, destruction and anonymization of personal data,
- f. **Law:** means the Law on Personal Data Protection No. 6698 dated 24 March 2016
- g. **Personal data:** means all the information relating to an identified or identifiable natural

person,

- h. **Processing of personal data:** means 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,
- i. **Personal data processing inventory:** means an inventory that data controllers creates their personal data processing activities based on business process by linking with

personal data processing purposes, data category, recipient group and data subject group, and that they explain and detail the period necessary for the purposes of personal data processing, personal data stipulated to be transferred to foreign countries and the measures taken for the data security,

- j. **Policy on personal data storage and demolition:** means the policy that data controllers use as a base for determining the maximum period necessary for the purpose of processing of personal data, and for erasure, destruction and anonymization,
- k. **Board:** means the Personal Data Protection Board,
- l. **Authority:** the Personal Data Protection Authority,
- m. **Periodical demolition:** means the transactions of erasure, destruction or anonymization that might be performed ex officio at repeating intervals stated in the policy on personal data storage and demolition in case all of the conditions of personal data processing set forth in the Law are abated,
- n. **Registry:** means data controllers' registry kept by the Directorate of the Personal Data Protection Authority,
- o. **Processor:** means the natural or legal person who processes personal data on behalf of the controller upon his authorization,
- p. **Data registry system:** means the registry system which the personal data is registered into through being structured according to certain criteria,
- q. **Controller:** means the natural or legal person who determines the purpose and means of processing personal data and is responsible for establishing and managing the data registry system.

5. PROCESSING OF PERSONAL DATA

5.1. Principles Applicable to Processing of Personal Data

Our Company act in compliance with the Constitution, the Law on Personal Data Protection and legal legislation on processing personal data of data subject. In relation to processing of personal data, the principles set forth in article 4 of the Law on Personal Data Protection, that all of the activities of personal data processing fundamentally carry such principles and all of the activities of personal data processing are carried out in compliance with these principles

are the priority of our Company, and the principles, which are taken into account during data processing are listed as follows.

5.1.1. Processing Personal Data in Compliance with Laws and Rules of Bona Fides

The principle of complying with laws and rules of bona fides, which is accepted by our Company as precondition in all data processing, means the obligation to act in compliance with the principles stipulated by the laws and other legal regulations in processing of personal data. As per this principle, our Company pays regard to data subjects' interest and reasonable expectations while trying to reach its aims in data processing, and act in a way preventing the occurrence of results that data subject does not expect and does not need to expect. Within the scope of this principle, our Company aims to procure transparent data processing activity for a data subject by informing the data subject as necessary about how and for what purposes personal data will be processed.

5.1.2. Ensuring Accuracy and Up-to-dateness of Personal Data, where necessary

In case our Company reveals a consequence related to data subject based on personal data of data subject, it fulfills its obligation of due care at the point of procuring accuracy and up-to-dateness where necessary of personal data. Apart from this, in order to procure accuracy and up-to-dateness of personal data of data subject, communication channels are kept open in order for our Company to be applied, and necessary opportunities are provided.

5.1.3. Processing of Personal Data for Specific, Explicit and Legitimate Purposes

Our Company shows sensitivity to compliance with the principle of being specific and explicit in legal actions and texts (explicit consent, clarification, giving response to data subject, application to data controllers' registry) where purposes of processing of personal data are explained, and pays attention to enable that data processing is clearly understandable

for data subject. Personal data is processed within the framework of purposes determined, declared, notified or stipulated under the contract.

5.1.4. Processing in a Way being Relevant with, Limited to and Proportionate to the Purposes for Which They are Processed

Our Company pays attention to that processed data in data processing is sufficient to realize the determined purpose, and prevents from processing data, which does not relate to the realization of the purpose or is not needed. Data is not processed for the fulfillment of possible requirements, which may arise in the future.

5.1.5. Preserving Personal Data for the Period of Time Stipulated by Legislation or the Purpose for Which They are Processed

The Company preserves personal data for the period of time stipulated by the legislation or needed for the purpose that they processed. In case of expiry of period stipulated by the legislation or realization of the purpose, personal data is erased, destructed or anonymized ex officio or upon data subject's request. In relation to demolition of personal data, "*Policy on Personal Data Storage and Demolition*" is prepared and published on the website of the Company.

5.2. Processing of General Quality Personal Data

As per article 20 of the Constitution and article 5 of the Law on Personal Data Protection, personal data cannot be processed without the explicit consent of data subject. In accordance with these legal regulations, our Company always pays regard to obtaining explicit consent of data subject in processing of personal data.

However, in some cases, the Law on Personal Data Protection allows personal data to be processed without explicit consent. In case of existence of one or several of such cases, personal data might be processed regardless of explicit consent. In case of processing of personal data without explicit consent of data subject, our Company acts in compliance with the principles set forth in article 5.1.

Your personal data might be processed by the Company in case of existence of one or several of the following conditions.

5.2.1. Existence of Explicit Consent of Data Subject

Obtaining explicit consent in processing of personal data is the priority of the Company. Therefore, necessary methods have been developed in order to obtain in physical and electronic mediums explicit consents of data subjects whose personal data is processed.

Before obtaining consent of data subject in relation to processing of personal data, the obligation to inform is fulfilled in accordance with article 10 of the Law, and freely given, specific and informed consent is obtained.

5.2.2. It is Clearly Stipulated under the Laws

In case it is clearly stipulated under the laws, processing of personal data complies with the law, and, in such a case, whether data subject's explicit consent is obtained or not is not assessed separately. As per article 75 of the Labor Law No. 4857 concerning Personnel File of Employee, collection of employees' data is considered within this scope.

5.2.3. Not Obtaining Explicit Consent Due to Actual Impossibility

In cases where consent could not be obtained or is not valid, it is prescribed to process data in order to protect life or physical integrity of data subjects. For example; in a case where data subject's consent is not valid since it is unconscious or is mentally handicapped, personal data might be processed during medical intervention in order to protect life or physical integrity.

5.2.4. It is Directly Related to Establishment or Execution of Contract

In case it is directly related to establishment or execution of a contract, personal data of contracting parties can be processed without explicit consent. For example; as required by the contract, account details of creditor can be obtained in order to make the payment.

5.2.5. It is Mandatory for the Company to Fulfill its Legal Obligation

In case it is mandatory for the Company to fulfill its legal obligation, personal data might be processed without explicit consent. For example; information requested by courts might be submitted to courts even explicit consent is not obtained.

5.2.6. Data is Made Available to Public by Data Subject

Data subject's personal data made available to public by itself may be processed without explicit consent. For example; a person's resume shared in a social media account can be deemed to be a data which is made available to public.

5.2.7. It is mandatory for the establishment, exercise or protection of any right

In case data processing is mandatory for the establishment, exercise or protection of a right, personal data may be processed regardless of explicit consent. The fact that the Company uses some data for a proof in a lawsuit filed by employee can be considered under this article.

5.2.8. It is mandatory for legitimate interest of the Company

On condition that it does not damage data subject's fundamental rights and freedoms, in case data processing is mandatory for data controller's legitimate interest, personal data may be processed without explicit consent. On condition that employees' fundamental rights and freedoms are not damaged, personal data may be processed in relation to promotions, salary increases or regulation of social rights.

5.3. Processing of Special Quality Personal Data

Special importance has been attached to some personal data through the Law on Personal Data Protection by taking into account that such data has a potential of discrimination and may cause grievance for data subject in case personal data is processed unlawfully, and such data is named as "special quality personal data".

Special quality personal data is regulated under article 6 of the Law. Accordingly, Personal data relating 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 are deemed to be personal data of special quality.

The Company shows special sensitivity to processing of “special quality personal data” that the Law on Personal Data Protection attributes great importance. Employees being involved in processing of special quality personal data are provided trainings on the Law, the relevant regulations and the security of special quality personal data, sign confidentiality agreements, their authorities to such data are limited, and the authority of those, who are appointed to another duty or leave the work, is immediately removed.

Records of all transactions made in electronic mediums where special quality personal data is kept are logged safely, security updates in relation to mediums where data is kept are consistently followed, and necessary security tests are performed and test results are saved. Sufficient security measures are taken in physical environments where special quality personal data is kept, and unauthorized access to aforesaid mediums are blocked.

Data subjects’ explicit consent in processing of aforesaid data is our Company’s priority. The Company can only process special quality personal data under the following exceptional circumstances set forth in the Law on Personal Data Protection in case data subject’s explicit consent is not provided;

- Personal data, excluding those relating to health and sexual life, may be processed without seeking explicit consent of the data subject, in the cases provided for by laws.
- Personal data relating to health and sexual life may only be processed, without seeking explicit consent of the data subject, 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.

5.4. Transfer of Personal Data

5.4.1. Transfer of Personal Data in the Country

Obtaining explicit consent during the transfer of personal data is our Company's priority. Therefore, necessary methods have been developed in order to obtain explicit consent of data subjects, whose personal data are share with third parties, physically and electronically.

In accordance with the purposes of processing personal data, our Company may share data subject's personal data with third parties in compliance with the law and the rules of good faith.

5.4.1.1. Transfer of General Quality Personal Data in the Country

Our Company may transfer data subject's personal data to third parties in compliance with the principles adopted in processing of personal data. A sensitivity is displayed to obtain data subject's approval while transferring personal data to third parties, and in case one or several of the following conditions exist, personal data may be transferred without obtaining explicit approval;

- It is clearly stipulated under 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 of contracting parties is necessary provided that it is directly related to the establishment or fulfilment of that contract.
- It is mandatory for the controller to be able to perform its legal obligations.
- Data is made available to the public by the data subject.
- 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.

5.4.1.2. Transfer of Special Quality Personal Data in the Country

Our Company may transfer data subjects' personal data to third parties in compliance with the principles adopted in processing of personal data.

It is sensitive to obtain data subject's approval while transferring special quality personal data to third parties, and special quality personal data is transferred in the country by taking

sufficient technical and organizational measures. However, in case of the following conditions, special quality personal data may be transferred regardless of data subject's explicit consent by taking sufficient technical and organizational measures;

- Personal data relating to the race, ethnic origin, political opinion, philosophical belief, religion, sect or other belief, clothing, membership to associations, foundations or trade-unions, convictions and security measures, and the biometric and genetic data, as stipulated under the law,
- Personal data relating to health and sexual life 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.

5.4.2. Transfer of Personal Data Abroad

While transferring personal data abroad, it is importance to obtain data subject's explicit consent. Therefore, necessary methods have been improved in order to obtain data subjects' explicit consent physically and electronically.

Our Company may transfer data subjects' personal data abroad in compliance with the law and the rules of good faith and depending on the purposes of processing of personal data.

We act in compliance with article 9 of the Law on Personal Data Protection while transferring personal data abroad.

5.4.2.1. Transfer of General Quality Personal Data Abroad

Our Company may transfer data subject's personal data to third parties in compliance with the principles adopted in processing of personal data. While transferring personal data to third parties abroad, we show sensitivity to obtain data subject's approval.

In case of absence of data subject's explicit consent, on condition that sufficient protection is provided in the foreign country where the data is to be transferred, or data controllers guarantee a sufficient protection in writing and the Personal Data Protection Board gives

permission, and in case of existence of one the following conditions, personal data may be transferred abroad;

- It is clearly stipulated under 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 of contracting parties is necessary provided that it is directly related to the establishment or fulfilment of that contract.
- It is mandatory for the controller to be able to perform its legal obligations.
- Data is made available to the public by the data subject.
- 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.

5.4.2.2. Transfer of Special Quality Personal Data Abroad

Our Company may transfer data subject's personal data abroad in compliance with the principles adopted in processing of personal data.

On condition that sufficient protection is provided in the foreign country where the data is to be transferred, or data controllers guarantee a sufficient protection in writing and the Personal Data Protection Board gives permission, and in case of existence of one the following conditions, personal data may be transferred abroad without any need for data subject's explicit consent;

- Personal data relating to the race, ethnic origin, political opinion, philosophical belief, religion, sect or other belief, clothing, membership to associations, foundations or

trade-unions, convictions and security measures, and the biometric and genetic data, as stipulated under the law,

- Personal data relating to health and sexual life 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.

6. PROCESSING OF PERSONAL DATA AT ENTRANCES OF OR WITHIN BUILDING AND FACILITY

In order to provide security of building and facility and in accordance with its legitimate interests, the Company carries out monitoring activities 7 days and 24 hours through security cameras at building and facilities of the company and personal data processing operations for pursuing visitors' entrance and exit. Processed personal data pursuant to such operations, are processed exclusively for the security of building and facility and to the extent required by the legitimate interests.

6.1. Monitoring Building and Facilities through Security Cameras

The Company performs monitoring operations through cameras in accordance with the Law on Private Security Services and the relevant legal legislation. Personal data recorded through security cameras are processed only for the purpose of security, we abide by the principles and conditions of processing of personal data set forth in the Law on Personal Data Protection.

We show necessary sensitivity in order not to violate fundamental rights and freedoms and right of privacy, and balance between the purpose of providing security of the Company and protecting its legitimate interest, and protecting data subjects' rights.

In this direction, we do planning, which will suffice to provide security, while locating security cameras and determining number and recording time. In places where there might be a right of privacy, monitoring activities are not performed through security cameras.

Notice saying that monitoring activities are being carried out 24/7 through security cameras and footages are recorded is hanged at visible places in building and facilities, and data subjects are informed about data processing.

The Company takes necessary technical and organizational measures in order to provide security of personal data recorded through security cameras. The recorded footages can only be accessed by the limited number of company employees.

6.2. Visitors' Entrance to Building and Facilities of the Company

The Company processes data in order to follow visitors' entrance and exist at the entrances of building and facilities of the company with the intent of providing security. Within this scope, personal data such as visitors' names and surnames, license plate details etc. may be stored for a definite period of time in order to provide security of building and facilities, and may be used only for this purpose.

As per article 10 of the Law on Personal Data Protection, the Company fulfills its obligation to inform enlightens data subjects on this matter, in the capacity of data controller. Notice saying that visitors' personal data is processed for security purposes is hanged at visible places in building and facilities, and it is aimed to enlighten data subjects about data processing.

7. DATA IN RELATION TO INTERNET ACCESS AT BUILDING AND FACILITIES

At building and facilities of the company, personnel and visitors are provided with an opportunity to access to internet. Name and surname, telephone number, TR identification number of personnel and visitors that want to use internet access, and used websites and hour details are stored as a legal obligation as per the Law on Regulation of Publications on the Internet and Combating Crimes Committed by Means of Such Publication No. 5651 and the Regulation on Public Use Providers issued depending on the Law.

Such records might be shared with legally authorized institutions and organizations in order to fulfill legal obligations upon the requests of authorized institutions and organizations.

8. PERSONAL DATA OF WEBSITE VISITORS

At some of the website belonging to the Company, visitors' data might be saved through technical means (cookies etc.) or through sharing by visitor during its membership.

At these websites, "Clarification Text on Processing and Protection of Personal Data" in relation to how and for what purposes personal data is collected under article 10 of the Law on Personal Data Protection Law is published and visitors have been informed on this matter.

9. SECURITY OF PERSONAL DATA

The Company takes the necessary technical and organizational measures of any kind for providing the appropriate security level in order to prevent unlawful processing of personal data and unlawful access to personal data, and to preserve personal data.

Within this scope, first of all, our Company performed a study in relation to the determination of what the processed personal data is, and then determined the risks which may arise concerning the protection of such data by taking into account that whether the processed personal data is a special-quality data, and the necessary technical and organizational measures for minimizing or eliminating the risks have been put into practice.

In order to provide the security of personal data, the personnel and managers are being provided trainings in an attempt to prevent personal data from being explained and shared unlawfully and to create awareness in relation to the Law on Personal Data Protection.

Furthermore, the employees getting involved in personal data processing are requested to sign confidentiality agreements as a part of their employment process, and the necessary discipline process is carried out in case it is determined that the employees have acted in contrary to the security policies and procedures.

Personal data included in the data processing by the company have been limited for access on personnel basis, and the limited number of personnel has been granted authority to access personal data, which relates to the business process that they carry out. Data processing carried out by the personnel is recorded. All across the company, as to the personal data processing, we take care to abide by the principle of "Everything is forbidden unless permitted".

In order to prevent unlawful processing of personal data and unlawful access to personal data, technical systems have been established with a view to follow-up and audit of processes in

relation to processing of personal data. Regular internal audits have been carried out in order to prevent unlawful processing of personal data and unlawful access to personal data.

With the intention of preventing unlawful access to personal data and preserving such data in secure medium, technical methods having appropriate security levels are being used, and the aforesaid methods are being updated in compliance with the developing technology.

In case of any attack inside or outside to the data registry system of the company, in order to recognize this situation early and to provide early intervention, which software and services works at information networks and whether there is any leakage or any action, which should not happen, are being checked regularly, transaction activities of all users are kept on a regular basis.

10. ERASURE, DESTRUCTION AND ANONYMIZATION OF PERSONAL DATA

Despite being processed in compliance with the legal legislation, the Company erase, destruct or anonymize personal data ex officio or upon demand by the data subject, upon disappearance of reasons which require the processing or the period stipulated under the legislation expires.

Personal data preserved in physical mediums is erased, destructed or anonymized ex officio or upon data subject's request in case the purpose of processing personal data is realized or the period stipulated in the legislation expires.

Personal data recorded in digital data registry systems is erased, destructed or anonymized ex officio or upon data subject's request in case the purpose of processing personal data is realized or the period stipulated in the legislation expires.

The Law on Personal Data Protection is not applicable to personal data that is anonymized under the Law. Anonymization of personal data means rendering personal data impossible to link with an identified or identifiable natural person, in any manner including matching them with other data.

Personal data might be anonymized ex officio or upon data subject's request in case of disappearance of reasons which require the processing or the period stipulated under the legislation expires. Anonymized personal data might be used for purposes such as research,

statistics and planning, might be stored for an indefinite period of time and be transferred in the country and abroad.

In relation to demolition of personal data, “*Policy on Storage and Demolition of Personal Data*” has been prepared and published on the website of the Company.

11. RIGHTS OF DATA SUBJECT AND APPLICATION TO THE COMPANY

Our Company informs data subjects, whom personal data is processed, about their rights and how they can exercise such rights under article 10 of the Law on Personal Data Protection.

11.1. Rights of Data Subject

Data subject has the following rights under article 11 of the Law on Personal Data Protection;

- to learn whether its personal data is processed or not,
- to request information if its personal data is processed,
- to learn the purpose of its data processing and whether this data is used for intended purposes,
- to know the third parties to whom its personal data is transferred at home or abroad,
- to request the rectification of the incomplete or inaccurate data, if any, and to notify the rectification to third parties whom personal data is transferred,
- to request the erasure or destruction of its personal data under the conditions laid down in Article 7 except for legal boundaries, and to notify erasure or destruction to third parties whom personal data is transferred,
- to object to the processing, exclusively by automatic means, of its personal data, which leads to an unfavorable consequence for the data subject,
- to request compensation for the damage arising from the unlawful processing of its personal data.

11.2. Exercise of Data Subject’s Rights

Data subject should submit its requests under article 11 of the Law on Personal Data Protection in writing and with its original signature or through a registered electronic mail

address, secure electronic address, mobile signature or by using the electronic mail address which has been notified by data subject to our Company beforehand and registered in our system. As for written applications, the application address is “*Deniz Mahallesi Petrol Ofisi Caddesi No:43 Derince/Kocaeli*”.

The mandatory information to be included in your application in minimum are as follows;

- Name, surname and signature, if application is in writing,
- TR identification number for Turkish citizens; nationality, passport number or identification number if any for foreigners,
- Residential or workplace address for notification,
- E-mail address, telephone and fax numbers if any for notification,
- Subject of request

Furthermore, relevant information and documents should be attached to the application. Application Form has been prepared in order for applicants to use during their application process, and is published on the website of the Company.

In case a person makes a request on behalf of data subject, a special power of attorney relating to the matter granted by data subject to the applicant should be issued.

11.3. Exceptions of Data Subject’s Right of Application

As per article 28 of the Law on Personal Data Protection, some circumstances are excluded from the Law on Personal Data Protection. Under such circumstances, data subjects cannot exercise their rights under article 11 of the Law on Personal Data Protection. These circumstances are as follows;

- Personal data is processed for the purpose of official statistics and for research, planning and statistical purposes after having been anonymized.
- Personal data is processed with artistic, historical, literary or scientific purposes, or within the scope of freedom of expression provided that national defense, national security, public security, public order, economic security, right to privacy or personal rights are not violated or they are processed so as not to constitute a crime.

- Personal data is processed within the scope of preventive, protective and intelligence activities carried out by public institutions and organizations duly authorized and assigned to maintain national defense, national security, public security, public order or economic security.
- Personal data is processed by judicial authorities or execution authorities with regard to investigation, prosecution, criminal proceedings or execution proceedings.

Furthermore, as per article 28/2 of the Law on Personal Data Protection, under the following conditions, apart from the right to demand the indemnification of a loss, it is not possible to exercise other rights set forth under article 11 of the Law on Personal Data Protection;

Data processing:

- is required for the prevention of a crime or crime investigation.
- is carried out on the data which is made public by the data subject himself.
- is required for inspection or regulatory duties and disciplinary investigation and prosecution to be carried out by the public institutions and organizations and by professional associations having the status of public institution, assigned and authorized for such actions, in accordance with the power conferred on them by the law,
- is required for protection of State's economic and financial interests with regard to budgetary, tax-related and financial issues.

11.4. Responding to Data Subject's Application

The Company takes all necessary technical and organizational measures in order to conclude data subject's applications under article 11 of the Law on Personal Data Protection efficiently and in compliance with the laws and the rules of good faith.

The Company shall finalize applications within thirty days at the latest and with no charge according to the quality of request. In case a response exceeds ten pages, 1 Turkish Lira may be charged as a transaction fee for each page exceeding ten pages. In case a response is given through a CD or flash disk, the cost of data recording medium may be demanded.

The company may request additional information, if necessary, in order to determine whether an applicant is the data subject and to assess the requests, and may address questions to the data subject concerning the application in order to clarify the matters stated in the application.