

ARKAS PETROL ÜRÜNLERİ VE TİCARET A.Ş.
PERSONAL DATA PROTECTION AND PROCESSING POLICY (EMPLOYEES)
6.11.2019 / Version No: 1

TABLE OF CONTENTS

- I. Introduction (Purpose, Scope, Relationship with Other Policies, Update Procedure)
- II. Personal Data Collection in Recruitment Process
- III. Processing of Employees' Data
- IV. Data related to Employees' Health
- V. Purposes of Processing Employees' Data
- VI. Special Cases in which Employees' Personal Data is Processed
- VII. Legal Rights of Employees Regarding Personal Data Collected About Themselves
- VIII. Sharing Employees' Personal Data with Third Parties
- IX. Retention Period of the Personal Data of Employees
- X. Use of External Service Providers in Processing Personal Data
- XI. Personal Data Security
- XII. Processing of Personal Data Related to the Activities Performed by Employees in the Workplace
- XIII. Categorization of Personal Data

ARKAS PETROL ÜRÜNLERİ VE TİCARET A.Ş.
PERSONAL DATA PROTECTION AND PROCESSING POLICY (EMPLOYEES)
6.11.2019 / Version No: 1

I. Introduction

The Law on the Protection of Personal Data No. 6698 (Law), puts into effect significant regulations regarding the lawful processing and protection of personal data. Personal data protection is among the priorities of ARKAS PETROL ÜRÜNLERİ VE TİCARET A.Ş. (Data Controller). The activities carried out regarding the protection of the personal data of the data controller's employees are managed under this "Personal Data Protection and Processing Policy" (Policy).

1. Purpose

This policy regulates which rules the Data Controller should comply with when processing the personal data of the Data Controller's employees. Therefore, the purpose of this Policy is to ensure the processing of personal data in accordance with the Law.

2. Scope

The Data Controller is the main decision-maker of this policy. The implementation of this Policy and the regulations stated within the Policy concern the Data Controller's employees. In addition to the employees that currently are employed by the Data Controller, former employees whose personal data is still being processed and candidates who have applied to any of the Data Controller's Group Companies are also covered by this Policy. The term "employee" in this Policy shall cover the current employees, former employees and employee candidates of the Data Controller.

The departments of the Data Controller that are responsible for the processing of the personal data of employees will play the most important role in the implementation of this Policy. Responsible departments shall receive support regarding the implementation of this Policy from Personal Data Protection (KVK) Advisory Group, Senior Management of the Data Controller, Data Controller's Contact Person or other designated responsible person or persons.

3. Relationship with Other Policies

This Policy regulates the actions to be taken by our group companies regarding the processing of the personal data of the Data Controller's employees. The provisions of the "Personal Data Protection and Processing Policy" regarding the processing of personal data shall apply regarding the cases for which there is no provision in this Policy.

4. Update Procedure

This Procedure is reviewed and updated once a year regardless of the alteration requirements in its corporate or legal content. The most up-to-date version of this procedure will be published on the data controller's website.

II. Personal Data Collection in Recruitment Process

1. Steps to be Followed in Job Advertising and Application Processes

1.2. Specifying the Information of the Hiring Company

ARKAS PETROL ÜRÜNLERİ VE TİCARET A.Ş.
PERSONAL DATA PROTECTION AND PROCESSING POLICY (EMPLOYEES)
6.11.2019 / Version No: 1

The Data Controller may initiate the recruitment process for vacant positions by a job posting (on a website, via employment or consulting companies or similar methods) or find candidates through the resumes sent to them.

The Data Controller ensures that the personal data of the candidates are processed in accordance with the law and they are informed accordingly.

In case the Data Controller initiates the recruitment process through an employment or consulting company, it shall take measures to ensure that how the personal data collected by private employment platforms/offices or consulting companies will be used and shared is specified.

1.3. Compatibility of the Collected Personal Data with the Recruitment Process

The Data Controller informs the candidates of the purpose for which the personal data is collected in order to fulfil its obligation to inform the personal data owner. If the personal data that has been collected is intended to be used or shared for any purpose or vacancy other than the one the candidate has applied for, such use and sharing purposes shall be stated clearly.

The questions to be directed for the collection of personal data and the forms issued for data collection purposes that are used during the recruitment process are evaluated according to each type of open vacancy and measures are taken to prevent the collection of unnecessary personal data (for example, questions may be asked about the name, surname, address, date of birth, e-mail address, work experience and education history of the candidates). Some personal data collected from the employees is not requested until the recruitment of the candidate has been approved (e.g. bank account information).

It may be necessary to process more comprehensive personal data depending on the nature of the work the candidate applies for. However, the personal data in question should be suitable with the nature of the work. The personal data requested specifically due to the requirements of the vacancy should only be used for the relevant vacancy.

1.4. Processing Special Categories of Personal Data

Personal data of candidates relating to the race, ethnic origin, political opinion, philosophical belief, religion, religious sect or other belief, appearance, membership to associations, foundations or trade-unions, data concerning health, sexual life, criminal convictions and security measures, and the biometric and genetic data is considered special categories of personal data.

Based on the special categories of data, no hiring decisions or discriminations shall be made by the data controller or special categories of personal data shall not be processed in the recruitment processes for these purposes, except for those required by the law or the nature of the work.

If special categories of personal data is required to be processed due to the nature of the work or legal obligation, special categories of personal data only complying with this scope may be processed, being as limited as possible. In such a case, the candidate shall be informed by an application form or a separate explanatory note about the reason for requesting the special categories of personal data to be processed and its intended use.

If the special categories of personal data to be requested can be collected from the candidate at later stages, these data cannot be requested on the first stage of the recruitment process.

1.5. Steps to Follow During the Interview

ARKAS PETROL ÜRÜNLERİ VE TİCARET A.Ş.
PERSONAL DATA PROTECTION AND PROCESSING POLICY (EMPLOYEES)
6.11.2019 / Version No: 1

The Data Controller may conduct interviews with candidates either face to face or by means such as video conference or telephone calls. The Data Controller informs the employees who will perform the interviews about how the personal data collected during the interview will be recorded and stored.

If the candidate demands to use his/her legal rights regarding the personal data that the interviewer recorded during the interview, this request/demand is answered by the Company/Group Companies in no later than 30 days. The Data Controller informs the employees that will conduct the interview about this subject.

The Data Controller takes the necessary measures regarding the legal claims that may be made by the candidate.

2. Steps to be Followed in Pre-Employment Surveys or Controls

2.1. Checking the Accuracy of Personal Data Provided by Candidates and Conducting Additional Research

The accuracy of the personal data transmitted by the candidates during the recruitment process may be confirmed by the Data Controller from other sources. The check is only carried out to verify the accuracy of the personal data transmitted by the candidate.

If the accuracy of the personal data transmitted by the candidate needs to be verified and checked, the Data Controller informs the candidate about this issue (about the personal data to be checked, the control method and the resources to be used) and obtains his/her consent if explicit consent is required. Additionally, if the information obtained as a result of the check and the personal data transmitted by the candidate themselves are inconsistent, the candidate is given the opportunity to explain the situation.

In addition, in some special cases, additional information about the candidate can be actively obtained by the Data Controller. Instead of conducting research, the Data Controller gives the utmost care to obtain the requested information from the candidate as much as possible.

Lawful methods are chosen and utilized when conducting research about the candidate. If the personal data to be obtained via research cannot be collected, a more reasonable alternative is sought that serves the same purpose. (e.g., checking the accuracy of the candidate's education diploma).

The Data Controller gives importance to determining in advance for which positions additional research should be carried out, in the light of the above conditions.

The Data Controller tries to include the scope of the research and the types of resources to be used for the research as much as possible on the job application form or additional explanatory information notes. In order to obtain information from relevant sources during the research, the candidate is also informed about which personal data of the candidate will be shared.

2.2. Research Time

If additional research on candidates is deemed necessary by the Data Controller, candidates are informed in the first stages of the recruitment process that research will be conducted about them and their personal data. In the case the Data Controller is to conduct research about the candidate, the research is carried out as close to the end of the recruitment process as possible. Comprehensive research is not carried out on all candidates who have passed the preliminary screening process. However, comprehensive research may be conducted about the candidates that are selected for the vacancies or about the candidates with a high probability of being selected for the vacancy.

2.3. Research Method

ARKAS PETROL ÜRÜNLERİ VE TİCARET A.Ş.
PERSONAL DATA PROTECTION AND PROCESSING POLICY (EMPLOYEES)
6.11.2019 / Version No: 1

When the Data Controller conducts research about the candidate; people who were with the candidate during the candidate's previous work experiences and training processes and people who had one-on-one work/education relationship with the candidate are reached out to receive information. The information obtained as a result of the research is evaluated according to the reliability of the source, no employment decision is based on a source whose reliability is doubtful. The Data Controller informs the relevant employees or the persons who will undertake the research about the method of research and takes care to obtain personal data only about the related candidate and no one else other than the candidate during this research process.

2.4. Obtaining Permission for Research

If the collection of information and any documents from a third party during the research depends on the consent of the candidate, the Data Controller should obtain explicit consent from the candidate. Instead of obtaining explicit consent from the candidate to receive information from the third parties, the method of taking the information directly from the candidate is preferred as much as possible.

3. Storage and Security of Candidates' Personal Data

In the recruitment process, the Data Controller shows the same care to the protection of the candidates' personal data, as they do to protect their employees' personal data. In this context; if the applications are made through a digital platform, the Data Controller uses a secure system, the applications made through the electronic platform are recorded in directories or systems that are only accessible by the persons responsible for the recruitment process, if the applications are made via mail and fax, the Data Controller ensures that they are received only by the authorized persons that are responsible for the human resources processes. The security of the obtained physical documents is ensured.

The Data Controller limits the access to candidates' personal data, allowing access only those in charge of conducting the recruitment processes. Such persons are regularly informed about the security measures to be taken and how to process personal data that belong to the candidates.

3.1. Retention Period of Personal Data Related to the Recruitment Process

The Data Controller takes all kinds of technical, administrative and legal measures to prevent the illegal processing of personal data and illegal access to personal data related to the recruitment process.

The Data Controller stores the candidates' personal data related to the recruitment process for a period that suits the purposes for which this data is processed. If the reasons that require the processing of the personal data according to the labour law and other relevant regulations become invalid, the personal data is erased, disposed of or anonymized by the Data Controller or upon the request of the candidate.

Unless there is a valid reason (such as resolution of possible disputes), the Data Controller does not retain the related personal data after the expiry of the statute of limitations of claims that may arise due to the recruitment process.

If any research has been done about the candidate during the recruitment process or any data has been obtained from third parties in any way, the information obtained from third parties is erased as soon as possible.

3.2. Personal Data to be Transferred to Employee Records of the Recruited Candidates

The Data Controller carefully determines which data will be transferred from the personal data obtained during the recruitment process to the personnel files of successful candidates that have been recruited to the vacancies.

ARKAS PETROL ÜRÜNLERİ VE TİCARET A.Ş.
PERSONAL DATA PROTECTION AND PROCESSING POLICY (EMPLOYEES)
6.11.2019 / Version No: 1

3.3. Personal Data of the Candidates whose Applications are not Accepted

If the Data Controller wishes to consider the unsuccessful applications for future vacancies, they may retain candidates' personal data in their records. If personal data will be kept for this purpose, they inform the candidates with the job application form or additional explanatory documents and indicate that the information can be erased from the records upon the candidates' requests.

III. Processing of Employees' Data

1. General Approach to the Processing of Employee Personal Data

1.1. Employee Information and Personal Data Processing Requirements

The Data Controller informs the employees as to which personal data is processed about them, the purposes and reasons for the processing, the sources from which personal data is collected, with whom the related personal data will be shared and how it will be used.

The Data Controller evaluates the personal data to be processed and processes this data based on at least one of the conditions stipulated in the Law. These conditions are;

- The explicit consent of the employee,
- Data processing being clearly stipulated in the relevant laws,
- Failure to obtain the explicit consent of the employee due to actual impossibility,
- Data processing is directly related to the establishment or performance of a contract,
- It is compulsory for the Data Controller to process data in order to fulfil its legal obligation,
- The personal data has been made public by the personal data owner,
- Data processing is mandatory for the establishment or protection of a right,
- Processing of data based on legitimate interests.

Personal data processing may be carried out in the presence of at least one of these conditions. The data processing activity may be carried out based on one or more of the conditions.

Where explicit consent is required, such explicit consent is obtained prior to the processing of personal data.

The Data Controller identifies and implements the most useful method for informing employees about the storage, usage and sharing of their personal data.

1.2. Collection of the Required Amount of Personal Data According to the Needs

The Data Controller collects personal data from employees based on clear and predictable needs and ensures that the collected data is required for fulfilling those needs.

In order to ensure compliance with the above-mentioned principle, all forms and input methods that employees submit their personal data are audited. This audit is completed as soon as possible for existing forms and input methods and for newly created forms and input methods, this audit is conducted prior to their usage.

ARKAS PETROL ÜRÜNLERİ VE TİCARET A.Ş.
PERSONAL DATA PROTECTION AND PROCESSING POLICY (EMPLOYEES)
6.11.2019 / Version No: 1

As a result of these audits, the parts on the relevant forms and input methods that provide the collection of unnecessary data are removed.

1.3. Keeping Personal Data Up to Date

The Data Controller takes the necessary measures to ensure that the personal data of the employees are up to date. In this context; personal data (address, telephone, family/close information, etc.) of the employees that are possible to change shall be determined, changeable personal data shall not be seen by everyone in electronic environment; the related data shall only be seen by the relevant employee himself/herself and other authorities that have access, if the employees do not have the opportunity to reach the personal data that are possible to change in electronic environment; necessary measures shall be taken to display these personal data in physical environment; it must be ensured that employees shall keep their changeable personal data up to date.

Apart from these methods, the Data Controller takes the necessary measures to keep the personal data of the employees up to date according to the company's specific conditions.

2. Processing of Special Categories of Personal Data of Employees

Some of the personal data is regulated separately as "special categories of personal data" under the Personal Data Protection Law and is subject to sensitive protection. Personal data of candidates relating to the race, ethnic origin, political opinion, philosophical belief, religion, religious sect or other belief, appearance, membership to associations, foundations or trade-unions, data concerning health, sexual life, criminal convictions and security measures, and the biometric and genetic data is considered special categories of personal data.

The Data Controller may process the health data in the following cases, provided that adequate measures to be determined by the Personal Data Protection Board are taken in cases where the explicit consent of the employee is not available:

- Special categories of personal data excluding the data related to the health and sexual life of the employee, only in cases stipulated in the law,
- Special categories of personal data related to the health and sexual life of the employee may be processed by the authorized institutions and organizations and the persons who have sworn secrecy, for planning and managing the financing and healthcare services and executing protective medicine, medical diagnosis, treatment and care services and protecting public health;
- With the explicit consent of the employee.

IV. Data related to Employees' Health

1. General Approach to the Processing of Employees' Health Data

1.1. Non-Processing of Health Data Unless Mandatory and its Separate Storage

Health data is considered special categories of personal data. The health data of the employees, especially the accident and disease reports of the employees, are stored separately from other personal data. Use of the employee's health data is avoided as much as possible when using information regarding the employee's absent days or the accidents and other incidents he/she is involved in.

ARKAS PETROL ÜRÜNLERİ VE TİCARET A.Ş.
PERSONAL DATA PROTECTION AND PROCESSING POLICY (EMPLOYEES)
6.11.2019 / Version No: 1

1.2. Processing of Health Data Related, Limited and Measured to the Specified Purpose

The Data Controller ensures that only the really necessary information is collected in the health surveys to be made to the employees and shows the utmost care not to request unnecessary information.

The Data Controller can not ask the employees to give a general explicit consent to share all their health data with the company. Companies may only request the sharing of health data which is thought to be really necessary for the stated purpose with the company.

1.3. Identification of the Persons to Process Health Data

The Data Controller's employees who will process or who authorize the processing of the health data of the employees shall be informed about the relevant legislation and the privacy policy that was created.

The health data of the employee is analyzed by the persons competent to do this job. The Data Controller takes care to inform the employees in an understandable manner about the purposes for which the health data is used and who has access to this data and for what purpose.

1.4. Sharing of Health Data and the Access to this Data

When sharing health data, the sharing processes are carried out by taking into account the legal obligations imposed for special categories of personal data.

The Data Controller shall ensure that the persons who are dealing with the health data of the employees are informed and trained about the situations presented above in regular intervals. In addition, arrangements are made for the Data Controller to receive the necessary support from the officials assigned for the protection of personal data.

As a rule, the Data Controller does not disclose employees' health data to other employees. However, if it is legally obligatory, if it is compulsory for the Data Controller to process this health data due to a work reason in the legitimate interests of the Data Controller, the personnel of the Data Controller assigned to this work shall have the access rights to the data, taking the necessary administrative and technical measures, provided that the access is only limited to fulfilling the requirements.

2. Processing of Health Data Obtained from Inspections and Tests

In general principle, authorized persons such as workplace physicians, nurses etc. who have confidentiality obligation authorized by the Data Controller (Data Controller Health Officials) are responsible for processing health data obtained from examinations and tests. The provisions of "Policy of Processing and Protecting Special Categories of Personal Data" shall be applied for the principles related to the collection and processing of this data.

2.1. Notification of the Company Policy regarding the Processing of Health Data to Employees

The Data Controller shall ensure that the policies regarding the processing of the health data of the employees are transparent.

The Data Controller determines the conditions regarding the places where the health tests will be performed, the nature of the tests, how the data obtained as a result of the test will be used and protected. He/she takes care to inform employees about these conditions.

2.2 Processing of Health Data obtained of Candidates Likely to be Hired through Inspections and Tests

ARKAS PETROL ÜRÜNLERİ VE TİCARET A.Ş.
PERSONAL DATA PROTECTION AND PROCESSING POLICY (EMPLOYEES)
6.11.2019 / Version No: 1

The Data Controller may request tests to be carried out on the concerned candidates to determine whether the candidates likely to be recruited are suitable for the job in question. The Data Controller may also perform these tests to fulfil any legal obligations or to determine the type of insurance which the prospective employee will be subject to.

The Data Controller shall determine in advance for which purposes the inspection and testing shall be carried out.

The Data Controller follows methods that can interfere less with a person's health data, taking into account their objectives.

During the recruitment process, medical examination or health tests are only performed if the person's recruitment is absolutely certain (unless there is no obstacle to doing the health-related work).

The Data Controller informs the candidate that a health examination or test can be performed in the early stages of the job application process if he/she is likely to be employed.

2.3 Collection of Health Data of Employees Through Inspection and Tests

On behalf of the Data Controller, the Data Controller's Health Officials may collect the health data of the employees through medical examinations and tests within the scope of the Occupational Health and Safety program.

The Data Controller shall determine in advance for which purposes the inspection and testing shall be carried out. The Data Controller follows the methods that can be less intrusive to the health data of the person by considering their objectives. For example, instead of looking at the results of the examination to learn the employee's health data, the Data Controller may conduct a health survey.

2.4 Failure to Use Samples Obtained from Inspection for a Specified Processing Purpose

The Data Controller shall clearly inform the employees of the purpose for which the health checks and tests are carried out.

The Data Controller shall in no way collect his/her biometric/genetic samples (fingerprints, hair, etc.) confidentially from the employee. The activities carried out on the basis of legal reasons constitute an exception.

V. Purposes of Processing the Employees' Data

The Data Controller obtains and processes personal data of employees for the following purposes:

- Supporting the determination and monitoring processes of performance evaluation criteria of the Data Controller's employees,
- Supporting the work/residence permit application processes of foreign employees of the Data Controller,
- Supporting the planning and monitoring of benefits provided to the employees of the Data Controller,
- Supporting the Data Controller in the planning and execution of the wage management and premium processes of the Data Controller's employees,

ARKAS PETROL ÜRÜNLERİ VE TİCARET A.Ş.
PERSONAL DATA PROTECTION AND PROCESSING POLICY (EMPLOYEES)
6.11.2019 / Version No: 1

- Supporting strategic human resources planning, backup processes and organizational development activities,
- Implementation of the decision to appoint, promote and dismiss senior managers and making related announcements,
- Supporting the determination of the senior managers' wage and premium packages,
- Supporting the planning and execution of the processes of measuring employee loyalty,
- Supporting the career development, training and talent management activities of the Data Controller's employees,
- Supporting recruitment processes,
- Supporting company's corporations' law and legislation processes,
- Supporting the Data Controller's compliance with the legislation it is subject to,
- Carrying out studies to protect Group reputation, sustainability and social responsibility activities,
- Organizing activities throughout the Data Controller,
- Conducting audit activities in compliance with other Data Controller's policies and relevant legislations,
- Carrying out communications activities for the employees of the Data Controller, to ensure employee satisfaction and commitment processes.

The Data Controller shall inform the employees that their personal data will be processed in accordance with the Law and the relevant legislation for the aforementioned purposes and, if necessary, obtain the relevant explicit consents.

VI. Special Cases in which Employees' Personal Data is Processed

1. Processing of Employees' Personal Data in Situations where Side Benefits and Rights are Provided

Benefits such as private health insurance, life insurance, individual accident insurance, company vehicle, individual pension, flexible benefit program or similar side benefits are referred to as side benefits and rights under this heading.

The Data Controller takes care to share the minimum required amount of personal data of the employees with the third parties from whom services are acquired in order to provide side benefits and rights to the employees. Only the personal data that is mandatory for the provision of the related side benefits and rights are shared with the mentioned third parties. Additionally, the necessary measures shall be taken for preventing the personal data collected within this scope from being used for other purposes.

The personal data to be shared with the third parties from whom the service is acquired are evaluated prior to the sharing to check whether they are special categories of personal data.

Employees are informed about the personal data sharing to be made with the third parties from whom the service is acquired. Within this scope, which personal data of the employees are shared and for what purpose they are to be used are explained to the employee in detail.

2. Processing of Employees' Personal Data for Safeguarding Equal Opportunities

ARKAS PETROL ÜRÜNLERİ VE TİCARET A.Ş.
PERSONAL DATA PROTECTION AND PROCESSING POLICY (EMPLOYEES)
6.11.2019 / Version No: 1

The Data Controller may process personal data to the extent necessary to ensure equal opportunity between employees. In this context, the Data Controller aims to ensure equal opportunities among their employees by identifying inequalities in processes such as recruitment, promotion, working conditions, internal career planning and development and by identifying equalist practice examples. In order to ensure equality between men and women in business life, personal data can be processed in this context for the implementation of the applications that are legally mandatory (such as nursery, nursery opening) or that are determined by the Data Controller.

Personal data processed to ensure the equality of opportunity is checked periodically. Personal data processed to ensure equality of opportunity is utilized by anonymizing the data as extensively as possible.

3. Processing of Employees' Personal Data for Fighting against Irregularities

The Data Controller may compare personal data sets in different units in order to prevent irregular transactions of the employees. The rules for the comparison of personal data sets to be made within the scope of the fight against irregularities are determined by the Data Controller. The Data Controller shares the personal data of their employees for the purpose of detecting irregular transactions only in the presence of one of the following conditions or similar conditions:

- It is legally mandatory to share the personal data of the relevant employee,
- There is a strong suspicion that it will not be possible to prevent or detect a crime if the personal data of the employee is not shared,
- Data sharing is necessary for the proper implementation of the Data Controller, Policies and Procedures

4. Processing of Personal Data of Employees in Mergers and Acquisitions of the Company and Other Transactions Changing the Structure of the Company

All transactions that change the structure of the company, including mergers and acquisitions, are considered under this section.

When the Data Controller needs to share the personal data of the employees in order to change the structure of the company; first of all, it ensures that these personal data are shared by being made as anonymized as possible.

For employees' personal data that cannot be anonymized prior to being shared, the other party undertakes to use this personal data limited to the processes related to the change in the company structure, to protect the personal data in accordance with the data security provisions of the Law and to process them in accordance with the relevant provisions of the Law, not to transfer the personal data to third parties and to erase or dispose of the personal data after the completion of the related transactions.

5. Processing of Personal Data of Employees in Disciplinary Investigations

The Data Controller is obliged to comply exactly with the obligations regarding the protection of the personal data of the employees during disciplinary investigations. In this context, the following actions are taken in particular:

- Aligning the policies and procedures related to disciplinary investigations with the obligations related to the protection of personal data,

ARKAS PETROL ÜRÜNLERİ VE TİCARET A.Ş.
PERSONAL DATA PROTECTION AND PROCESSING POLICY (EMPLOYEES)
6.11.2019 / Version No: 1

- Informing the persons authorized to conduct disciplinary investigations that personal data falling within the scope of disciplinary investigations can also be accessed within the scope of employees' right to access their personal data,
- Taking measures to ensure that personal data is not obtained by illegal methods during disciplinary investigations,
- Ensuring that the personal data to be used during disciplinary investigations is accurate and up to date,
- Ensuring the safe storage of personal data and records related to disciplinary investigation,
- Ensuring that unfounded claims against employees are erased from their files if there is no legal reason not to dispose them.

The Data Controller prevents arbitrary access to the personal data of the employees solely because of the existence of disciplinary investigation. In this context, the personal data of the employees cannot be accessed solely due to the disciplinary investigation if it is not suitable with the purposes of obtaining the personal data or if access to the personal data is considered to be a disproportionate process according to the seriousness of the investigation.

6. Processing of Personal Data Related to the Electronic Communications Processes Performed by Employees for Business Activities

The principles related to the processing of personal data related to the electronic communications transactions carried out by the for their business activities are specified in the " Information Systems General Standards and Security Policy" of the Data Controller.

7. Workplace Security Camera Application

The Data Controller can place security cameras at various points in order to ensure the safety of the workplaces. Care is taken to ensure that the image areas of these security cameras cover only areas with special risk, entrance-exit and similar areas, not the entire workplace. The data controller takes care to inform the employees about the areas that are filmed with security cameras, monitored with security cameras and the purposes of monitoring.

8. Tracking the Vehicles Provided by the Company

In cases where vehicles are allocated to the employees by the Data controller; the allocated vehicles can be monitored for determining the distance travelled, fuel use measurement, location data and similar purposes. Employees are informed in advance of this tracking and monitoring.

VII. Legal Rights of Employees Regarding Personal Data Collected About Themselves

1. Legal Rights of Employees

Employees have the following rights to:

- Find out whether personal data are processed,
- Request information about the personal data that is reported to be processed,
- Find out the reasons for processing personal data and whether the data are processed in line with the stated purposes.

ARKAS PETROL ÜRÜNLERİ VE TİCARET A.Ş.
PERSONAL DATA PROTECTION AND PROCESSING POLICY (EMPLOYEES)
6.11.2019 / Version No: 1

- Request correction of personal data in case of incomplete or incorrect processing and, if applicable, to request notification of the third parties to whom personal data has been transferred, regarding the corrections that has been made.
 - Be aware of the third parties to whom personal data are transferred in Turkey or abroad
 - Request the erasure or destruction of your personal data within the framework of the conditions stipulated in the relevant legislation and notification of the transactions made on the personal data made in accordance with the relevant legislation to third parties to whom their personal data are transferred.
 - Request the removal of the damage if the personal data is damaged due to the processing of their personal data in violation of the Law.
 - Object to a result against the contact as a result of exclusive analysis of the processed data through automated systems
2. Principles Regarding Employees' Use of their Legal Rights

The Data Controller shall take any administrative, legal and technical measures that will enable employees to exercise their statutory rights, make the necessary applications, and respond to their application within 30 days at the latest, and shall design and inform employees of the relevant processes.

In Data Controller's responses to employees who have used their statutory rights, utmost care will be given to not to disclose any personal data of third parties.

VIII. Sharing Employees' Personal Data with Third Parties

1. General Rules on Personal Data Sharing

The Data Controller determines the internal procedures for the sharing of employees' personal data. Data sharing requests shall be covered by competent employees in this regard.

Measures are taken to confirm the authenticity and accuracy of data-sharing requests from outside the company (such as judicial authorities, administrative authorities, insurance company requests). Data sharing requests from outside the company shall be carried out in writing.

In case the personal data of the employees are sent abroad upon incoming request, all kinds of administrative, legal and technical measures shall be taken for transferring the personal data abroad.

If the sharing of employees' personal data constitutes a legal obligation, only personal data subject to this legal obligation may be shared.

Subject to the statutory requirements for international data transfer and the transfer of special categories of personal data, personal data from employees may only be transferred to third parties if one of the following conditions exist:

- The explicit consent of the data owner,
- If there is an explicit regulation in the laws regarding the transfer of personal data,
- If it is mandatory for the protection of the life or body integrity of the personal data owner or another person and the personal data owner is in a position where he/she can not express his/her consent due to the actual impossibility or if legal validity is not given for his/her consent;

ARKAS PETROL ÜRÜNLERİ VE TİCARET A.Ş.
PERSONAL DATA PROTECTION AND PROCESSING POLICY (EMPLOYEES)
6.11.2019 / Version No: 1

- If the transfer of personal data pertaining to one of the parties in a contract is necessary, provided that it is directly related to the establishment or performance of that contract,
- If personal data transfer is mandatory in order to fulfil a legal obligation,
- If the personal data is made public by the personal data owner,
- If personal data transfer is mandatory for the establishment, use or protection of a right,
- If it is mandatory to transfer personal data for the legitimate interests of the relevant group companies, provided that it does not harm the fundamental rights and freedoms of the personal data owner.

2. Record Keeping and Informing about Personal Data Sharing

In case the personal data of the employees are shared with third parties, prior to its sharing, it is required that check that the data sharing is based on one of the conditions stipulated in the Law.

Employees, if they have not been informed priorly, are informed about this sharing at the latest at the time of sharing. However, if giving this information to the employee creates a violation of the Law or constitutes a prior warning of an investigation that is being done by the competent authorities, the relevant employee shall not be informed of the matter.

Requests for the external sharing of the personal data of the employees which are not routinely done and the shared information within this scope can be recorded by the Data Controller. In this context, at least the person who gives consent to sharing, the person who requests sharing, the reason for sharing, the date and time of sharing and the types of data shared are recorded. These records are regularly inspected and reviewed.

3. Publishing of the Personal Data

The Data Controller may publish the personal data of the employees only by taking the following conditions into account:

- There is a legal right or obligation to publish personal data or the employee has given explicit consent for the release,
- Personal data is not explicitly unfit for release. The Data Controller acts with a balancing approach to the benefits to be obtained as a result of the publishing of personal data and the expectations that employees' privacy will be protected.

In the event that the names of some employees and other personal data are published in media such as annual reports, releases or websites, these situations are considered sensitive and whether explicit consent is required is determined. If it is decided that explicit consent is required, explicit consent of the relevant employees is obtained before the release of personal data. Personal data types to be shared during obtaining explicit consent shall be notified to the employee individually.

IX. Retention period of the personal data of employees

The Data Controller stores the personal data of the employees in accordance with the time period required for the purpose for which they are processed and according to the minimum retention periods stipulated in the legal legislation which the relevant activity is subject to.

ARKAS PETROL ÜRÜNLERİ VE TİCARET A.Ş.
PERSONAL DATA PROTECTION AND PROCESSING POLICY (EMPLOYEES)
6.11.2019 / Version No: 1

In this context, our Company primarily determines whether a specific time period is foreseen for the storage of personal data in the relevant legislation, and if a time period is determined, it acts in accordance with this period. If a legal time period is not available, personal data is kept for as long as is necessary for the purpose for which they are processed. Personal data are disposed of at the end of the specified storage periods in accordance with the periodic disposal periods or according to the application of the data owner by the designated disposal methods (erasure and/or disposal and/or anonymization).

X. Use of External Service Providers in Processing Personal Data

The Data Controller may use external service providers to process the personal data of employees. However, the Data Controller must take the following measures regarding external service providers:

- Checking that the external service provider has taken the technical and administrative security measures required by the relevant legislation and sector practices,
- Periodically inspecting that the external service provider has taken the technical and administrative security measures required by the relevant legislation and sector practices,
- Forming a contract with the external service provider that states the specific regulations for taking the necessary technical and administrative security measures,
- Taking the necessary legal, administrative and technical measures if personal data is sent to external service providers abroad.

XI. Personal Data Security

The Data Controller shall take all reasonable measures necessary to ensure the security of the employee's data. The measures taken are designed to prevent unauthorized access risks, accidental data losses, deliberate erasure of the data or damage to the data.

The Data Controller appoints responsible employees within the company for the personal data processing activities to be carried out regarding the business activities of the employees. In this context, the number of employees who will be responsible for the personal data processing activity and will have the authority to access the personal data obtained as a result of this processing is kept as limited as possible. In this context, the Data Controller removes or limits the access rights of these employees if there are employees who do not need access to this data in the current situation. Physical security measures are taken to ensure that only authorized persons have access to the personal data of the employees. In this context, access authorized persons are also prevented from having unnecessarily extensive authority.

In accordance with the Law No. 5651 on the Regulation of Broadcasts on the Internet on Information Systems and the Fight Against Crimes Through These Broadcasts, measures such as an audit trail are taken to determine who has access to the personal data of the employees. Access records to be created in this context are checked on a regular basis and investigation mechanisms for unauthorized access are established.

It is essential that other employees who have access to the personal data of the employees undergo the necessary security checks. In addition, it is ensured that these persons sign a confidentiality agreement/commitment that provides the necessary protection or that provisions are included in the employment contracts in this context and that they are continuously trained about their responsibilities.

ARKAS PETROL ÜRÜNLERİ VE TİCARET A.Ş.
PERSONAL DATA PROTECTION AND PROCESSING POLICY (EMPLOYEES)
6.11.2019 / Version No: 1

If the personal data of the employees are taken out of the workplace by various means such as laptops, necessary security measures are taken and relevant employees are informed about these measures.

XII. Processing of Personal Data Related to the Activities Performed by Employees in the Workplace

This section details the issues related to which personal data of the employees can be processed (communication, vehicle use, etc.) and the principles to be followed by the Data Controller in this regard.

1. Determining in which Business Activities and for what Purposes the Personal Data of Employees will be processed

The Data Controller determines the specific business activities of the employees and the purposes for which they process their personal data (such as e-mail control, use of vehicle tracking devices, camera monitoring) and determines the personal data processing methods that will be appropriate for the intended result of the processing of the personal data.

The Data Controller ensures that the personal data processing purposes or methods of the employees to be carried out in the context of their business activities comply with the rules on the protection of personal data as a result of the evaluation they will carry out within their company.

The Data Controller informs the employees in charge of personal data processing activities to be carried out particularly regarding the business activities of the employees about the protection of personal data and other legislations related to the subject, the matters to be considered within the scope of the relevant legislation and the obligations of the Data Controller arising from the legislation. Additional confidentiality and security obligations are added to the contracts made with employees who have access to personal data obtained as a result of these activities or it is ensured that privacy policies/commitments are signed by these persons.

2. Informing the Employees regarding the Data Controller's Personal Data Processing about the Employee's Business Activities

The Data Controller informs the employees about the personal data processing activities (such as e-mail control, use of vehicle tracking devices, camera monitoring), the purposes and procedures of the processing of this personal data within the scope of the activities carried out in relation to the work.

If the Data Controller processes the personal data of the employee for the purposes of determining whether the employee is behaving in accordance with the work and workplace rules during working hours and whether the employee fulfils his/her duties properly and whether there are actions that will disturb the peace and order in the workplace environment and so on, he/she should inform the relevant employees clearly and in detail.

Warnings are placed in accordance with the nature of the working environment before the Data Controller in order to inform the employees about which personal data processing activities are carried out by their employer in relation to their own business activities and to raise awareness.

3. Usage of the Personal Data Obtained as a result of Processing of Personal Data regarding Employees' Business Activities for Other Purposes

The personal data of the employees processed in relation to their business activities may also be processed for other legitimate purposes in accordance with the requirements set out in Article 5 of the Law and the

ARKAS PETROL ÜRÜNLERİ VE TİCARET A.Ş.
PERSONAL DATA PROTECTION AND PROCESSING POLICY (EMPLOYEES)
6.11.2019 / Version No: 1

principles of the processing of personal data set out in Article 4. Employees are also informed by the Data Controller in appropriate methods about what these purposes are.

4. Granting the Employees the Right of Defence regarding the Information Obtained by the Processing of Personal Data regarding Employees' Business Activities

Employees are given the right to see, disclose and defend the data obtained before a complaint procedure or disciplinary process is initiated against an employee based on the data obtained as a result of the processing of employees' personal data related to their business activities.

XIII. Categorization of Personal Data

Within the scope of this Policy, in addition to the categorization of the personal data specified in the "Personal Data Protection and Processing Policy" <https://arkasbunker.com/> the personal data of the employees are processed in the following categories:

- *Employee Information:* Personal data (including vehicle information, training information, marital status information, reference information) processed within the scope of the activities carried out to ensure commercial and legal security of the company and employees during the employment of the employees.
- *Candidate Information:* All kinds of personal data (including military status information, training information, reference information) processed for obtaining information that will be the basis for evaluating employee candidates for the suitable vacancies in the recruitment processes.
- *Performance and Career Development Information:* Personal data processed for the purpose of measuring the performance of the Data Controller's employees and planning and conducting career developments within the scope of our Company's human resources policy and auditing such activities.