

POLICY ON THE PROTECTION AND THE
PROCESSING OF PERSONAL DATA OF KOÇ
GROUP EMPLOYEES

INFORMATION FORM

Document Name:

Policy on the Protection and the Processing of Personal Data of Koç Group Employees

Prepared By:

Koç Holding A.Ş. Personal Data Protection Committee

Approved By:

Koç Holding A.Ş. Personal Data Protection Board

Version:

2.0

Effectivity date:

23.07.2019

In cases where there is a conflict between the Turkish version which is the original language of the text and any translation of the policy, the Turkish text shall prevail.

© Koç Holding A.Ş., 2019

This document cannot be reproduced and distributed without the written permission of Koç Holding A.Ş.

Table of Contents

PART 1 - INTRODUCTION	5
1.1 Introduction	5
1.2 Purpose	5
1.3 Scope	5
1.4 Relationship of This Policy with Other Policies	5
1.5 Updatability	5
PART 2 - COLLECTION OF PERSONAL DATA DURING RECRUITMENT PROCESS	6
2.1 Steps to be Followed in Job Advertisement and Application Processes	6
2.1. 1 Specifying the Information of the Announcing Company	6
2.1. 2 Compliance of Collected Personal Data with the Recruitment Process	6
2.1.3 Processing Special Categories of Personal Data	6
2.1. 4 Steps to Follow During the Interview	7
2.2 Steps to be Followed in Pre-Employment Research or Controls	7
2.2.1 Checking the Accuracy of Personal Data Provided by Candidates and Conducting Additional Research	7
2.2.2 Time of Study	7
2.2.3 Research Method	8
2.2.4 Obtaining Permission for Research	8
2.3 Retention and Security of Candidates' Personal Data	8
PART 3 - PROCESSING EMPLOYEE DATA	9
3.1 General Approach to Processing Personal Data of Employees	9
3.1.1 Informing Employees and Personal Data Processing Conditions	9
3.1.2 Collection of Personal Data as Required According to Necessities	10
3.1.3 Keeping Personal Data Up-to-Date	10
3.2 Processing of Special Category of Employee Data	10
PART 4 - DATA ON THE EMPLOYEES' HEALTH	11
4.1 General Approach to the Processing of Employees' Health Data	11
4.2 Processing of Health Data Obtained from Examinations and Tests	12
PART 5 - PROCESSING OF EMPLOYEE DATA BY KOÇ HOLDİNG ANONİM ŞİRKETİ	13
PART 6 - SPECIAL CASES WHERE EMPLOYEE PERSONAL DATA IS PROCESSED	14
6.1 Processing Employee Personal Data in the Context of Providing Side Benefits and Additional Rights	14
6.2 Processing Employee Personal Data in the Context of Ensuring Equal Opportunity	14
6.3 Processing Employee Personal Data in the Context of Preventing Unlawful Practices	14
6.4 Processing of Employee Personal Data in Company Mergers and Acquisitions and Other Transactions Changing Company Structure	14
6.5 Processing Employee Personal Data in Disciplinary Investigations	15
6.6 Processing of Personal Data in Electronic Communications Carried Out by Employees in Connection with Business Processes	15
6.7 Security Cameras in the Workplace	16
6.8 Tracking Vehicles Provided by the Company	16
PART 7 - LEGAL RIGHTS OF EMPLOYEES WITH REGARD TO PERSONAL DATA COLLECTED ABOUT THEM	17
7.1 Legal Rights of Employees	17

7.2 Principles Regarding Employees' Exercising Their Legal Rights	17
PART 8 - TRANSFER OF EMPLOYEES' PERSONAL DATA TO THIRD PARTIES.....	17
8.1 General Rules Regarding Personal Data Transfer	17
8.2 Information and Record Keeping Regarding Personal Data Transfer	18
8.3 Publication of Personal Data	18
PART 9 - RETENTION PERIOD OF EMPLOYEES' PERSONAL DATA.....	19
PART 10 - USE OF EXTERNAL SERVICE PROVIDERS FOR THE PROCESSING OF PERSONAL DATA.....	19
PART 11 - SECURITY OF PERSONAL DATA	19
PART 12 - PROCESSING PERSONAL DATA RELATED TO THE ACTIVITIES OF THE EMPLOYEES IN THE WORKPLACE.....	20
12.1 Determining for Which Purposes and Business Activities the Personal Data of Employees Shall be Processed	20
12.2 Informing the Employees about the Personal Data Processing Activities of the Koç Group Company in relation to the Business Activities.....	20
12.3 Use of Personal Data Obtained as a Result of Personal Data Processing Regarding Business Activities of Employees for Other Purposes	20
12.4 Giving the Employees the Right to Defense Against the Information Obtained as a Result of the Processing Personal Data Regarding the Business Activities of the Employees	21
PART 13 - CATEGORIZATION OF PERSONAL DATA	21

PART 1 – INTRODUCTION

1.1 Introduction

Law No. 6698 on Personal Data Protection (the “**PDP Law**”) introduces important regulations regarding the protection and legal processing of personal data.

Protection of personal data is among the most important priorities of Koç Holding A.Ş. and Koç Group Companies (“**Group Companies**”). Group Companies have the appropriate processes in the processing of personal data will significantly increase the ability to act in accordance with the law and this will affect all related activities.

The activities carried out by each of the Group Companies regarding the protection of the personal data of the employees of the Group Companies are managed under the “Policy on Personal Data Protection and Processing of Personal Data of Employees” of related Group Company and established and implemented by the Group Companies within the framework of the principles set forth in this Policy on the Protection and the Processing of Personal Data of Koç Group Employees (“**Policy**”).

1.2 Purpose

In this Policy, the rules that shall be followed by Group Companies when processing personal data of employees of Group Companies are set out. Therefore, the purpose of this Policy is to ensure that personal data are processed by our Group Companies in accordance with the law by the application of similar practices.

1.3 Scope

The primary addressee of this Policy is our Group Companies. However, the implementation of this Policy and the regulations included in the Policy concern the employees of our Group Companies. Employees who currently have an employment relationship with our Group Companies, as well as former employees whose personal data are still being processed, and candidates who have made a job application to any of our Group Companies are also covered by this Policy. The expression “employee” in this Policy shall include the current employees of the Group Companies, former employees and employee candidates to the extent it is relevant.

Units of our Group Companies that are responsible for the processing of employee personal data will play the most important role in the execution of this Policy. The responsible units will receive support from the Personal Data Protection Committee (“**PDP Committee**”) established by our Group Companies, or from the responsible person(s) assigned in this regard.

1.4 Relationship of This Policy with Other Policies

This Policy regulates the actions to be taken by our Group Companies regarding the processing of personal data of the employees of the Group Companies and draws the framework of the policy they will shape for their own employees. For cases where there are no provisions in this Policy, the provisions in the general policies regarding the processing of personal data shall be applied.

1.5 Updatability

This Policy may be updated from time to time in order to comply with changing conditions and legislation. In case of an update, our Group Companies shall be notified via www.kocweb.com or other channels.

PART 2 - COLLECTION OF PERSONAL DATA DURING RECRUITMENT PROCESS

2.1 Steps to be Followed in Job Advertisement and Application Processes

2.1. 1 Specifying the Information of the Announcing Company

Our Group Companies may initiate the recruitment process for open positions by job advertisement (website, newspaper advertisement, employment or consultancy companies or similar methods) or evaluate the resumes sent to them.

Our Group Companies shall process the personal data of candidates in accordance with the law and fulfill their obligation to inform. In this context, the title and contact information of the relevant Group Company are clearly stated in each job announcement or application form.

In the event that our Group Companies initiate the recruitment process through the employment or consultancy company, they shall take measures to ensure how the personal data collected by the employment or consultancy company will be used and transferred.

2.1. 2 Compliance of Collected Personal Data with the Recruitment Process

Our Group Companies shall inform the candidates about the purpose of collecting personal data in order to fulfill the obligation to inform the data subject. If the collected personal data is intended to be used or transferred for another position or purpose other than the position applied by the candidate, the purposes related to this processing and transferring shall be clearly stated.

During the recruitment process, the questions asked for the collection of personal data and the forms prepared to collect personal data are evaluated according to each open position type and measures are taken to prevent unnecessary personal data collection (e.g. name, surname, address, date of birth, e-mail address, job questions may be asked about her experience and training). Some personal data collected from employees should not be requested before the candidate's recruitment is approved (for example, bank account information).

Depending on the nature of the job applied by the candidate, it may be necessary to process more comprehensive personal data. However, the personal data in question shall be appropriate to the nature of the job. Personal data requested due to the nature of the job shall only be valid for the relevant position.

2.1.3 Processing Special Categories of Personal Data

Employee candidates' 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 are special categories of personal data.

Except for the purposes of fulfilling legal obligation or due to the nature of the job, our Group Companies shall not discriminate on the basis of special categories of personal data for the purpose of making a recruitment decision and not process special categories of personal data for that purpose.

If special categories of personal data are required to be processed due to the nature of the job or fulfilling legal obligation, only special categories of personal data within this scope can be processed as limited as possible. In such a case, the candidate is notified with the application form or a separate explanatory note about the ground for requesting special categories of personal data to be processed and the purpose of processing.

If the special categories of personal data that needs to be requested are of a quality that can be collected from the candidate at a later stage, these data cannot be requested at the first stage of the recruitment process.

2.1. 4 Steps to Follow During the Interview

Our Group Companies can interview candidates face to face or via the tools such as video conference and the telephone.

Our Group Companies inform their employees who will conduct the interviews on how the collected personal data during the interview will be recorded and stored.

Regarding the personal data recorded by the interviewers during the interview, in case the candidate requests to use his/her legal rights regarding his/her personal data; this request shall be concluded by the relevant Group Company within 30 days at the latest. Our Group Companies inform their employees who will conduct the interviews about this matter.

Our Group Companies shall take the necessary measures in order for the usage of requests that can be asserted by the candidate to use the legal rights.

2.2 Steps to be Followed in Pre-Employment Research or Controls

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

The accuracy of the personal data submitted by candidates during the recruitment process can be confirmed by our Group Companies from other sources. The control is made only to verify the accuracy of the personal data transmitted by the candidate.

In the event that the accuracy of the personal data submitted by the candidate is checked, our Group Companies inform the candidate about this issue (about the personal data to be checked, the control method and resources to be used) and obtain his consent if explicit consent is required. In addition, in case of inconsistency between the information obtained as a result of the control and the personal data transmitted, the candidate is given the opportunity to explain the situation.

In addition, in some special cases, our Group Companies may actively search for additional information about the candidate. Instead of conducting research, obtaining the requested information from the candidate should be sought as much as possible.

In order to conduct research on the candidate, all the following conditions should be met:

- The methods used should be in accordance with the law.
- There should be a risk for the relevant Group Company or its customers and/or business partners in case the personal data that needs to be investigated cannot be collected.
- There should not be a more reasonable alternative to achieve the same goal.

Our Group Companies are diligent in determining in advance the positions requiring additional research in the light of the above conditions.

Our Group Companies try to include as much as possible on the job application form or in the additional explanatory information note about the candidates to be researched, the scope of the research and the types of resources to be used for the research. 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 transferred.

2.2.2 Time of Study

If it is deemed necessary by our Group Companies to conduct additional research on the candidates, the candidates are informed about the fact that an inquiry will be made on them at the early stages of the recruitment process.

With respect to making a research on the candidate by our Group Companies, the research shall be conducted at a stage as close as possible to the conclusion of the recruitment process. Comprehensive research is not conducted for all candidates passing the pre-selection. However, extensive research can be conducted on candidates who are likely to be selected for open positions.

2.2.3 Research Method

Our Group Companies carefully select resources while doing research about the candidate. In this context, our Group Companies shall comply with the following principles:

- In order for the researched information to be requested from the relevant source, the probability of obtaining the information from that source should be high.
- Candidate's family or close circle should be consulted in exceptional cases.
- The information obtained as a result of the research should be evaluated according to the reliability of the source.
- No employment decision should be based on a source of questionable reliability.
- Information obtained from uncertain sources should not be relied upon.
- Our Group Companies should inform the relevant employee or the people who will undertake the research about the research method.
- If the result of the research is against the candidate, the candidate should be informed about the situation in question. Our Group Companies should carry out activities that will ensure that the applicant is informed about the result and that the candidate can make a statement about the situation if he/she wishes.
- The explanation of the candidate about the result should be taken into consideration.
- Personal data relating to a different person should not be obtained from the candidate during the research.
- In case of collecting and processing personal data about a person different from the candidate, the data subject should be informed about the situation and the method of processing the information. Necessary activities should be carried out for this informing.

2.2.4 Obtaining Permission for Research

If collecting information and documents from a third party during the research depends on obtaining the consent of the candidate, our Group Companies shall obtain explicit consent from the candidate. Instead of obtaining the explicit consent by a third party from the candidate, the method of obtaining the explicit consent by our Group Companies directly from the candidate should be preferred as much as possible.

2.3 Retention and Security of Candidates' Personal Data

2.3.1 Security of Candidates' Personal Data

During the recruitment process, our Group Companies pay attention to the protection of personal data of employees, as well as to candidates who apply for a job. In this context, especially the following measures are taken:

- If the applications are sent digitally, our Group Companies are required to establish a secure system. Applications submitted electronically are saved in index or systems that can only be accessed by those responsible for the recruitment process.
- If the applications are sent by mail or fax, it is ensured that these applications are conveyed to the authorized person responsible for human resources. The security of the obtained physical documents is ensured.

Our Group Companies restrict access to personal data of candidates to those who are in charge of conducting recruitment processes. These persons are regularly informed about the security measures to be taken by processing the personal data of the candidates.

2.3.2 Retention Period of Personal Data Regarding Recruitment Process

Our Group Companies shall take all kinds of technical, administrative and legal measures in order to prevent the unlawful processing of personal data regarding the recruitment process and unlawful access to these data.

Our Group Companies keep the personal data of the candidate regarding the recruitment process for a period suitable for the purposes of processing this data. In accordance with labor law and other relevant regulations, in case the reasons for processing no longer exist, personal data shall be deleted, destructed, or anonymized by our Group Companies or upon the request of the candidate.

Unless there is a valid cause (such as the resolution of possible disputes), our Group Companies do not keep the relevant personal data after the expiry of the statute of limitations for requests that may arise due to the recruitment process. As of the end of the relevant statute of limitations, the personal data of the candidate can be kept anonymously.

During the recruitment process, in cases where a research has been made about the status of the candidate or data has been obtained from third parties, the information obtained from third parties shall be deleted as soon as possible. Group Companies may keep the results of the research by stating whether the research has been conducted, the result of the research and whether the candidate has been recruited.

2.3.3 Personal Data of Recruited Candidates to be Transferred to Employee Records

Our Group Companies shall carefully determine which data will be transferred among the personal data obtained during the recruitment process to the personnel files of successful candidates who are accepted for the open position. Personal data that are not required due to the scope of the business relationship and personnel file are not transferred to the new employee's personal file.

2.3.4 Personal Data of Candidates whose Applications Are Not Accepted

If our Group Companies would like to evaluate the unsuccessful applications for future positions, they can keep the records of personal data of the candidates. If personal data will be kept for this purpose, our Group Companies are required to inform the candidates in the job application form or in additional explanatory documents on this matter and specify that the information can be deleted from the records if they request.

PART 3 - PROCESSING EMPLOYEE DATA

3.1 General Approach to Processing Personal Data of Employees

3.1.1 Informing Employees and Personal Data Processing Conditions

Our Group Companies shall inform their employees on which personal data are processed about them, for what purposes and grounds these personal data will be processed, from which sources their personal data are collected, to whom these personal data will be transferred and how they will be used.

Our Group Companies evaluate the personal data they process and process this data based on at least one of the conditions stipulated in the PDP Law. These conditions are:

- Employee's explicit consent,
- Data processing being clearly provided for in the relevant laws,
- Failure to obtaining explicit consent of the employee due to the actual impossibility,

- Data processing being directly related to the conclusion or execution of a contract,
- Data processing being mandatory for our Koç Group Company to fulfill its legal obligations,
- Personal data being made public by the data subject himself/herself,
- Data processing being mandatory for the establishment or protection of a right,
- Data processing being based on legitimate interest.

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

In cases where an explicit consent is required, obtaining of the explicit consent process is completed before the personal data is processed.

Our Group Companies shall determine and apply the most beneficial method according to their specific conditions with regard to the informing employees about the retention, use and transfer of their personal data.

3.1.2 Collection of Personal Data as Required According to Necessities

Our Group Companies shall collect personal data from employees upon a clear and predictable necessity. Our Group Companies shall ensure that the collected data is suitable for meeting the mentioned needs.

In order to ensure compliance with the above-mentioned principle, all forms and login methods in which employees enter personal data are audited. This audit is completed as soon as possible for existing forms and, for the new form and login methods to be created, the audit is completed before starting to use these form and methods. As a result of the audit to be carried out, parts that cause unnecessary data collection are removed from the relevant form and login method. In addition, personal data obtained through these parts are immediately deleted, destructed, or anonymized.

3.1.3 Keeping Personal Data Up to Date

Our Group Companies shall take the necessary measures to keep the personal data of employees up-to-date. In this context, particular attention is paid to the following:

- Employees' personal data that may change (address, telephone, family/close information, etc.) shall be determined.
- Measures shall be taken in electronic environment for easy viewing of personal data that may change.
- Personal data that may change shall be seen only by the relevant employee and other authorized people having access in the electronic environment, and not by everyone.
- If employees do not have the opportunity to view personal data that may change in the electronic environment, necessary measures shall be taken in order to display these personal data in a physical environment.
- It is ensured that employees keep up-to-date the personal data that may change. In this scope, active follow-up is carried out by human resources personnel regarding awareness studies.

Apart from the method enumerated above, our Group Companies shall take the necessary measures to keep the processed personal data of employees up-to-date, according to their own specific conditions.

3.2 Processing of Special Category of Employee Data

Some of the personal data are regulated separately as "special categories of personal data" within the scope of the PDP Law and are subject to special kind of protection.

Special categories of personal data are race, ethnicity, the data on political opinion, philosophical belief, religion, sect or other beliefs, attire, association, foundation or union membership, health, sexual life, criminal conviction, biometric and genetic data.

Our Group Companies may process health data in below cases where the employee does not give his/her explicit consent, provided that adequate measures specified by the Personal Data Protection Board are taken:

- (i) Special categories of personal data except for those concerning the employee's health and sexual life, only in cases stipulated by law,
- (ii) Special categories of personal data concerning the health and sexual life of the employee, by the persons subject to secrecy obligation or authorized public institutions and organizations, 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.

PART 4 - DATA ON THE EMPLOYEES' HEALTH

4.1 General Approach to the Processing of Employees' Health Data

4.1.1 Not Processing Health Data Unless Mandatory and Separate Retention

Health data are among the special categories of personal data. Employees' health data, especially the employee's accident and illness reports, are retained separately from other personal data. The use of employee health data is avoided as much as possible while using information about the absence days or about the accident and other incidents involved.

4.1.2 Related to the Specified Purpose, Limited and Proportional Processing of Health Data

Our Group Companies make sure that only the highly necessary information is collected within health surveys to be made to employees and present due diligence for not requesting unnecessary information.

Our Group Companies cannot ask employees to give a general explicit consent to transfer all health data to the company. Companies can only request transferring of the health data that is deemed really necessary for the specified purpose to the company.

4.1.3 Identifying the Persons to Process Health Data

It is ensured that Group Company employees who will process or authorized to process health data are informed about the relevant regulation and the established privacy policy.

Health data of the employee are analyzed by persons who are competent to conduct such work.

Our Group Companies wary of clearly informing the employees for what purposes the health data are used and who accessed these data for which purpose.

4.1.4 Transfer of and Access to Health Data

In terms of transferring the health data, the transferring procedures are carried out by taking into account the legal obligations provided for special categories of personal data and in accordance with these obligations.

Group Companies ensure that persons taking care of the employee health data are regularly informed and trained about the above cases. In addition, Group Companies make arrangements for these persons to receive the necessary support from the PDP Committee of the relevant company or from the officials assigned for the protection of personal data.

Our Group Companies, in principle, do not make the health data of the employees accessible to other employees. However, if the work and the processing of such data are necessary due to the legitimate interests of the relevant Group Company, the necessary administrative and technical measures are taken to process this personal data and the right to access them is provided, on the condition that the personnel in charge of this work are limited to fulfill the requirements of the work.

The health data which are needed to be known in order to fulfill managing roles may be disclosed to the managers. Managers of our Group Companies are informed about the sensitivity of health data and the processing conditions of these data in the PDP Law before the health data are shared with them.

4.2 Processing of Health Data Obtained from Examinations and Tests

4.2.1 Notification of the Company Policy Regarding the Processing of Employee Health Data

Our Group Companies operates diligently to ensure that policies regarding the processing of employee health data are transparent.

Our Group Companies designate the conditions regarding the places where the health tests will be performed, the quality of the tests, and how the data obtained from the test will be used and protected. It presents due diligence to inform the employees about these conditions.

4.2.2 Processing of Health Data of Potential Candidates via Examinations and Tests

Our Group Companies may request the candidates who are likely to be recruited to conduct tests to evaluate whether they are eligible for the job in question. It can also perform these tests to meet any legal obligations or to determine the type of insurance that the potential employee will be subject to.

Our Group Companies determine in advance the purposes for which examinations and tests will be carried out.

Our Group Companies follow methods that would interfere in persons' health data to a lesser extent, while taking into account their objectives.

During the recruitment process, a medical examination or health test is only done if the person is indeed likely to be hired.

Our Group Companies inform the candidate in the early stages of the job application process that a health examination or test can be done if the possibility of being recruited is high.

4.2.3 Collecting Health Data of Employees via Examinations and Tests

Our Group Companies can collect employee health data through medical examinations and tests within the scope of the occupational health and safety program. Participation in examinations and tests other than mandatory inspections and tests according to legal regulations are left to the employee's own choice.

Our Group Companies predetermine the purposes for which examinations and tests will be carried out.

Our Group Companies follow methods that would interfere in persons' health data to a lesser extent, while taking into account their objectives. For example, instead of looking at the examination results, a health survey may be conducted in order to learn the employee's health data.

4.2.4 Not Using Samples Obtained from Examination Beyond the Purpose of Processing Specified

Our Group Companies clearly inform the employees about the purpose of health checks and tests.

Our Group Companies cannot, under any circumstances, secretly collect biometric/genetic samples (fingerprints, hair strands, etc.) belonging to the employee. Activities performed based on legal grounds are reserved.

PART 5 - PROCESSING OF EMPLOYEE DATA BY KOÇ HOLDİNG ANONİM ŞİRKETİ

Koç Holding Anonim Şirketi obtains and processes employee personal data for the following purposes from the relevant Group Companies:

- Determining and providing support regarding the monitoring processes on the performance evaluation criteria of the employees of the Group Companies,
- Providing support regarding the working/residence permit application processes of the foreign employees of the Group Companies,
- Providing support regarding the planning and follow-up processes of the side benefits and additional rights provided to the employees of the Group Companies,
- Providing support regarding Group Companies in planning and execution of wage management and bonus processes,
- Providing support regarding the collective union agreements of the Group Companies,
- Providing support regarding the planning of the strategic human resources of the Group Companies, backup processes and organizational development activities,
- Implementing the assignment, promotion and leaving decisions of the senior executives of the Group Companies and making relevant announcements,
- Providing support regarding the senior managers of the Group Companies in determining the wage and bonus packages,
- Providing support regarding the planning and execution of employee engagement measurement processes of Group Companies,
- Providing support regarding the planning and execution of career development, training and talent management activities of the employees of the Group Companies,
- Providing support regarding the recruitment processes of Group Companies,
- Providing support regarding the Group Companies' corporate and partnership law transactions,
- Providing support for the Group Companies' compliance with the regulations to which they are subject,
- Carrying out works aimed at protecting the reputation of the group, sustainability and social responsibility studies,
- Organizing events across the Group Companies,
- Conducting auditing activities for carrying out the activities of the Group Companies in accordance with the Koç Group Companies policies and the relevant regulations,
- Conducting the communication activities for the employees of the Group Companies, employee satisfaction and loyalty processes.

Our Group Companies will inform the employees as stipulated in the scope of PDP Law and the relevant legislation regarding the transfer of employee personal data to Koç Holding A.Ş. for the aforementioned purposes and, if necessary, obtain their explicit consent.

PART 6 - SPECIAL CASES WHERE EMPLOYEE PERSONAL DATA IS PROCESSED

6.1 Processing Employee Personal Data in the Context of Providing Side Benefits and Additional Rights

Under this section, private health insurance, life insurance, personal accident insurance, company vehicle, private pension, flexible side benefits program or similar benefits are referred to as side benefits.

Group Companies pay the utmost attention to ensuring that minimum amount of the data is transferred, when transferring employee personal data to third parties providing side benefits to employees. Only personal data that is necessary to provide side benefits is transferred to said third parties. In addition, necessary measures are implemented to prevent personal data from being processed for any purpose other than the purpose of collection.

Prior to transfers to said third-party service providers, evaluations are made as to whether it contains special categories of personal data.

It is ensured that employees are informed on the transfer of personal data to said third-party service providers. In this regard, employees are informed on the categories of personal data that will be transferred and the purposes for which they will be used.

6.2 Processing Employee Personal Data in the Context of Ensuring Equal Opportunity

Group Companies may process personal data to the extent necessary in order to ensure equal opportunity among employees.

Personal data that is processed for the purpose of ensuring equal opportunity is monitored periodically. Personal data that is processed for the purpose of ensuring equal opportunity is anonymized to maximum extent possible.

6.3 Processing Employee Personal Data in the Context of Preventing Unlawful Practices

Group Companies can compare personal data sets in different units in order to prevent unlawful practices by employees.

Group Companies determine the rules that apply to the comparison processes of personal data sets for preventing unlawful practices.

Employee personal data will only be transferred to third parties in order to determine unlawful practices, where the following conditions or conditions similar to them are met:

- Transfer of employee personal data is a legal obligation,
- There is strong suspicion that it will not be possible to prevent or detect a crime if the employee personal data is not transferred,
- There is a specific provision in the employment contract of the relevant employee regarding the transfer of personal data within this scope.

6.4 Processing of Employee Personal Data in Company Mergers and Acquisitions and Other Transactions Changing Company Structure

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

6.4.1 Transferring Employee Personal Data for Changes in the Company Structure

When our Group Companies are required to transfer employee personal data for changes in the company structure; it is ensured that personal data is anonymized to the maximum extent possible.

As for employee personal data that cannot be transferred in an anonymized manner, it is ensured that the recipient party undertakes to only use personal data in transactions for changing the company structure, to process and ensure the security of personal data in accordance with the PDP Law, not to transfer personal data to third parties and that personal data will be deleted or destructed once the transaction is finalized.

6.4.2 Providing Notification

Employees will be informed on the purposes of transferring personal data, provided that this information does not have any negative impact on the interests of the relevant Group Company (for instance, in cases where the employee uses becomes aware of a merger transaction and uses this information to affect the prices of company's stocks).

Employees are also informed about the categories of personal data that will be transferred to their new employers as a result of a change in the company structure.

6.5 Processing Employee Personal Data in Disciplinary Investigations

Group Companies must comply with their personal data protection obligations during disciplinary investigations. In this context, the following actions shall primarily be taken:

- Aligning the policies and procedures on disciplinary investigations with personal data protection obligations,
- Informing individuals authorized to conduct disciplinary investigations that personal data processed as part of disciplinary investigations may also be accessed within the scope of employees' right to access personal data,
- Taking measures to ensure that personal data is not obtained through unlawful means during disciplinary investigations,
- Ensuring that personal data used during disciplinary investigations is accurate and up to date,
- Secure retention of personal data and records used during disciplinary investigation,
- Ensuring that ungrounded allegations about employees are deleted from the respective employee files provided there is no lawful ground necessitating further retention.

Group Companies prevent any arbitrary access to employee personal data that relies on the existence of an ongoing disciplinary investigation. In this context, employee personal data shall not be accessed solely based on the disciplinary investigation if such data is not suitable with or proportionate to the purpose of processing. In terms of their access authorizations, persons responsible for carrying out the investigation shall be informed by the PDP Committee, prior to commencement of each investigation.

6.6 Processing of Personal Data in Electronic Communications Carried Out by Employees in Connection with Business Processes

6.6.1 Determining the Policy on Use of Electronic Communication Tools

If electronic communications tools and devices assigned to employees such as telephone, fax, e-mail, laptop, internet access are to be monitored by our Group Companies, a policy on the use of such electronic communication tools and devices shall be prepared and presented to employees. This policy shall also include sanctions to be imposed upon employees in the event of failure to comply with specified rules.

If existing policies provide for rules regarding the use of electronic communication tools, an evaluation shall be made as to whether these comply with the personal data protection legislation and other applicable legislation; policies shall be revised in order to ensure compliance with the personal data protection legislation.

Group Companies individually determine their internal policies as to the use of electronic communication tools for personal purposes.

If the use of electronic communication devices for personal purposes is permitted, the limits of such personal use shall be determined, and employee shall be notified.

It is essential that employees are informed and aware that the content of communication that is established as part of business processes may always be monitored.

6.6.2 Processing Personal Data for Corporate Electronic Mail Communications

Group Companies may process employee personal data as part of their use of corporate e-mail accounts. It is essential that employees are informed on the scope and purpose of such processing activities. Additionally, employees shall be informed on the legal nature and scope of processing activities in this context.

6.6.3 Processing Personal Data for Internet Use

Group Companies may impose restrictions on internet use in the workplace and audit compliance with these restrictions.

Koç Group Companies shall adequately inform employees on the processing of personal data as part of their internet use.

If processing of personal data in the context of internet use is necessary to comply with a legal obligation or if such processing based on the conditions of processing personal data under the PDP Law, employee's explicit consent shall not be required. However, if personal data is processed for purposes other than those based on processing conditions specified under the PDP Law, then employee's explicit consent shall be obtained.

6.6.4 Retention Period for Personal Data Processed in Electronic Communications

In respect of personal data processed in electronic communications as part of business processes, Group Companies shall establish policies and procedures that determine the types of personal data to be retained and the periods for retention. If the absence of a statutory obligation, personal data processed for the purposes specified under this Policy shall be retained during the term of employment and after termination of employment, for the period of statute of limitation in consideration of legal disputes that may potentially arise. The retention periods for personal data shall be reviewed in accordance with the respective regulations. Said retention periods may be extended in case of exceptional circumstances. If extended, employees shall be notified on the extended retention period, the ground for extending the period and the types of personal data.

6.7 Security Cameras in the Workplace

Group Companies may place security cameras at various points in order to ensure the security of the workplace. These security cameras shall not be placed in a manner viewing the entire workplace; but rather only implemented in areas that are exposed to security risks such as entrance-exits.

Group Companies shall show a reasonable effort to inform the employees regarding the areas that are being surveilled and monitored by security cameras and the purposes of monitoring.

6.8 Tracking Vehicles Provided by the Company

In cases where vehicles are allocated to employees by our Group Companies; allocated vehicles can be tracked for purposes such as determining the distance travelled, measuring fuel usage, obtaining location data. Employees shall be informed, prior to any such tracking.

PART 7 - LEGAL RIGHTS OF EMPLOYEES WITH REGARD TO PERSONAL DATA COLLECTED ABOUT THEM

7.1 Legal Rights of Employees

Our employees are entitled to the following rights:

- 1) To learn whether his/her personal data are being processed,
- 2) To request information if his/her personal data have been processed,
- 3) To learn the purpose of the processing of his/her personal data and whether they have been used accordingly,
- 4) To learn which third parties domestic or abroad his/her personal data has been transferred to,
- 5) To request rectification in case his/her personal data has been processed incompletely or inaccurately and to demand the operations in this regard be reported to third parties his/her personal data has been transferred to,
- 6) To demand the erasure or destruction of his/her personal data in the event that the reasons for the processing no longer exist even though it was processed in accordance with the PDP Law and other relevant provisions and to demand the operations in this regard be reported to third parties his/her personal data has been transferred to,
- 7) To object to negative consequences to him/her that are concluded, as a result of analysis of the processed personal data through solely automatic systems,
- 8) To demand compensation for the damages that he/she has suffered as a result of an unlawful processing of his/her personal data.

7.2 Principles Regarding Employees' Exercising Their Legal Rights

Our Group Companies shall take all kinds of administrative, legal and technical measures to ensure that employees are able to exercise their legal rights, make the necessary applications and obtain responses to their applications within 30 days at the latest, and shall design the relevant processes to inform the employees on the issue.

Group Companies shall ensure that the personal data of third parties are not unlawfully disclosed in the responses to be given to employees exercising their legal rights.

PART 8 - TRANSFER OF EMPLOYEES' PERSONAL DATA TO THIRD PARTIES

8.1 General Rules Regarding Personal Data Transfer

Our Group Companies determine the internal procedures regarding the transfer of personal data of employees. It is ensured that requests regarding the transfer of personal data are answered by competent employees.

Necessary measures shall be taken to verify the genuineness and reliability of data transfer requests made from outside the company (such as requests from judicial authorities, administrative authorities, insurance companies). As a general rule, data transfer requests received from third parties has to be received in writing.

In case the personal data of the employees are sent abroad upon request, all administrative, legal and technical measures shall be taken regarding the transfer of personal data abroad.

If the transfer of personal data of employees constitutes a legal obligation, personal data can only be transferred in accordance with the scope of this legal obligation.

Without prejudice to the legal requirements regarding international data transfer and transfer of special categories of personal data; personal data of employees can only be transferred to third parties if one of the following conditions is met:

- Data subject has given explicit consent,
- It is expressly provided for by the laws,
- It is necessary for the protection of life or physical integrity of the person himself/herself or of any other person, who is unable to explain his/her consent due to the physical disability or whose consent is not deemed legally valid,
- Processing of personal data of the parties of a contract is necessary, provided that it is directly related to the establishment or performance of the contract,
- It is necessary for compliance with a legal obligation to which the data controller is subject,
- Personal data have been made public by the data subject himself/herself,
- Transfer of the personal data is necessary for the establishment, exercise or protection of any right.
- Processing of data is necessary for the legitimate interests pursued by the data controller, provided that this processing shall not violate the fundamental rights and freedoms of the data subject.

8.2 Information and Record Keeping Regarding Personal Data Transfer

In case the personal data of the employees are transferred to third parties, it is required to ensure that the data transfer is based on one of the legal bases for data processing stipulated in the PDP Law.

If they have not been informed before, the employees are informed about this transfer at the latest at the moment of the transfer. However, if the prior notice would constitute a breach of law or it would provide a prior warning about an investigation that is run by the competent authorities, the prior information shall not be given to the employee.

External transfer requests of employees' personal data that are not carried out on regular basis and the transfer made within this scope can be recorded by our Group Companies. In this context, at minimum, the person approving the transfer, the person requesting the transfer, the reason for the transfer, the date and time of the transfer and the types of data transferred shall be recorded. These records are checked and reviewed on regular basis.

8.3 Publication of Personal Data

Our Group Companies can only publish personal data of employees by paying attention to the following conditions:

- If there is a legal right or obligation to publish personal data or if the employee has given explicit consent for publication,
- Personal data are not clearly unsuitable.

Our Group Companies pursue to strike a balance between the benefits as a result of the publication of personal data and the expectations of employees that their privacy shall be protected.

In the event that the names or personal data of employees are published in mediums such as annual reports, publications or websites, these publications are closely evaluated to determine whether there is a requirement for explicit consent or not. If it is deemed necessary to obtain explicit consent, the explicit consent of the relevant employees is obtained before the publication of personal data. When obtaining explicit consent, the types of personal data to be published shall be notified to each employee explicitly.

PART 9 - RETENTION PERIOD OF EMPLOYEES' PERSONAL DATA

Our Group Companies keep the personal data of employees in accordance with the time required for the purpose for which they are processed and, if any, for the minimum retention periods stipulated in the regulations to which the relevant activity is subjected to. In this context, our company shall determine at first whether a specific period is stipulated for the retention of personal data in the relevant legislation, and such period is specified, it shall act in accordance with this retention requirement. If there is no legal period specified, personal data shall be retained for the time required for the purpose for which they are processed. Personal data shall be destructed at the end of the specified retention periods in accordance with the regular destruction periods or the data subject application and by the decided destruction methods (deletion and/or destruction and/or anonymization).

PART 10 - USE OF EXTERNAL SERVICE PROVIDERS FOR THE PROCESSING OF PERSONAL DATA

Our Group Companies may use external service providers for the processing of personal data of employees. However, our Group Companies are obliged to take the following measures regarding external service providers:

- Ensuring that the external service provider has taken the technical and administrative security measures required by the relevant legislation and industry practices,
- Auditing periodically that the external service provider sustains the technical and administrative security measures required by the relevant regulation and sector practices,
- Signing a contract with the external service provider, including the conditions for taking necessary technical and administrative security measures,
- Taking necessary legal, administrative, and technical measures in case personal data are sent to foreign service providers abroad.

PART 11 - SECURITY OF PERSONAL DATA

Our Group Companies take all reasonable precautions to ensure the security of employee data. The measures taken are designed to prevent unauthorized access risks, accidental data loss, deliberate deletion of data or damage to data.

Our Group Companies appoint responsible employees within the company for personal data processing activities to be carried out in the business activities of employees. The number of employees who shall be responsible for personal data processing activities and be authorized to access personal data obtained as a result of this process is designated as limited as possible. Group Companies remove or limit the access rights of employees that have unnecessary access to the personal data of other employees. Necessary physical security measures shall be taken to ensure that only those authorized to access can access the personal data of the employees. In this context, the access rights of the employees are kept to a minimum that is necessary to perform their duties.

Measures such as audit trails shall be taken to determine who has access to personal data of employees on information systems. Access records to be created within this scope shall be regularly controlled and investigation mechanisms are established for unauthorized access.

It is essential that other employees having access to personal data of employees shall undergo necessary security checks. In addition, it shall be ensured that these employees sign separate confidentiality agreements/commitments that provide the necessary protection to the data they process or provisions that has similar purpose are included into their employment contracts. Furthermore, employees that have access rights shall be continuously trained about their responsibilities.

In case personal data belonging to employees are taken out from the workplace by various means such as laptop computers, necessary security measures shall be taken, and the relevant employees shall be informed about these measures.

PART 12 - PROCESSING PERSONAL DATA RELATED TO THE ACTIVITIES OF THE EMPLOYEES IN THE WORKPLACE

Under this section, the matters regarding which personal data can be processed (communication, vehicle use, etc.) and the principles to be followed by our Group Companies in this regard are detailed, in particular for the processes conducted by employees during the execution of the activities of our Group Company.

12.1 Determining for Which Purposes and Business Activities the Personal Data of Employees Shall be Processed

Our Group Companies shall determine the specific business activities and purposes based on for processing employees' personal data (such as e-mail control, use of vehicle tracking devices, camera monitoring) and the personal data processing methods that shall be suitable for the desired result reached by the purpose of processing personal data.

Our Group Companies ensure that the personal data processing purposes or methods to be carried out in the business activities of the employees are in compliance with the rules of protection of personal data, as a result of the assessment they shall perform within their own organization.

Our Group Companies inform their employees who are in charge of personal data processing activities to be carried out in the business activities of the employees on the protection of personal data and other relevant regulations and the matters to take into consideration within the scope of the related regulations and the liabilities of the relevant Group Company arising from the regulations. Additional confidentiality and security obligations shall be included to contracts signed with employees who have access to personal data obtained as a result of these activities or privacy policies/commitments that shall be signed by these persons.

12.2 Informing the Employees about the Personal Data Processing Activities of the Koç Group Company in relation to the Business Activities

Our Group Companies inform their employees about the personal data processing activity methods (such as e-mail control, use of vehicle tracking devices, camera monitoring) within the scope of their business-related activities, and the purposes and procedures for processing these personal data.

Our Group Companies must clearly and in detail inform the relevant employees in the case of processing employee personal data for the purposes of determination of whether the business and workplace rules are followed, and the duties are properly fulfilled by the employees during working hours and tracking whether the behaviors impeding the peace and order in the workplace environment and for similar purposes.

In order to inform the employees about the personal data processing activities carried out by their employers regarding their business activities and to raise awareness, warnings shall be placed within the premises of Group Companies in accordance with the nature of the working environment.

12.3 Use of Personal Data Obtained as a Result of Personal Data Processing Regarding Business Activities of Employees for Other Purposes

The processed personal data of the employees related to the business activities can be processed for other legal purposes, in accordance with the conditions specified in Article 5 of the PDP Law and the principles of processing personal data stipulated in Article 4. Employees shall be informed by our Group Companies with appropriate procedures about what these purposes are.

12.4 Giving the Employees the Right to Defense Against the Information Obtained as a Result of the Processing Personal Data Regarding the Business Activities of the Employees

Before initiating a complaint or disciplinary process against an employee over the obtained data as a result of the processing of personal data related to the business activities of the employees, employees shall be given the right to see the obtained data to make explanations and provide their arguments about these data.

PART 13 - CATEGORIZATION OF PERSONAL DATA

Within the scope of this Policy, below categories of personal data are being processed in addition to the personal data categories specified in Koç Holding Anonim Şirketi Personal Data Protection and Processing Policy at www.koc.com.tr/legal-informations.

PERSONAL DATA CATEGORIZATION	PERSONAL DATA	PERSONAL DATA CATEGORIZATION OF KOÇ GROUP EMPLOYEES
Employee Information		Personal data (including vehicle information, education information, marital status information, reference information) processed within the scope of activities carried out to ensure the commercial and legal security of the Company and employees during their employment.
Employee Information	Candidate	All kinds of personal data (including military status information, educational information, reference information) to obtain information that are basis for the evaluation of employee candidates for the appropriate position in the recruitment process.
Performance and Career Development Information		Personal data processed for the purpose of measuring the performance of the employees of Koç Group Companies, planning and conducting their career development within the scope of the human resources policy of our Company and auditing the said activities.
Fringe Benefits and Interests Information		Personal data (including insurance information) processed within the scope of activities carried out for the purposes of employee satisfaction and loyalty, planning the fringe benefits and benefits offered to the employees, determining objective criteria for entitlement and ensuring their progress payments.
Personnel Information		All kinds of personal data processed within the scope of the establishment, improvement, execution and supervision of the Group's human resources policies and to obtain information that will be the basis of the personal rights of real persons who have a working relationship with Koç Group Companies.