Arçelik

GLOBAL PERSONAL DATA PRIVACY POLICY

GLOBAL PERSONAL DATA PRIVACY POLICY

1. PURPOSE AND SCOPE

Arçelik and its affiliates and subsidiaries (together “Company”, “we”, “us”) is committed to protecting the privacy and the personal data of everyone we do business with, including our customers, suppliers, employees and contractors. In recognition thereof, Company has adopted this Personal Data Privacy Policy (the “Policy”). This Policy aims to determine the framework and coordinate the compliance activities to be carried out specifically for Arçelik in order to comply with the Applicable Data Protection Laws on the protection and processing of personal data.

One of the most important issues for the Company is to comply with the general principles stipulated in the Applicable Data Protection Laws in the processing of Personal Data. In this context, our Company acts in accordance with the principles listed below in the processing of Personal Data in accordance with the Applicable Data Protection Laws.

- engaging in Personal Data processing activities in compliance with the law and the rule of integrity,
- ensuring Personal Data are accurate and up-to-date when necessary,
- processing for specific, explicit and legitimate purposes,
- being related to the purpose for which they are processed, limited and measured,
- retention for as long as required for the purpose of processing or envisioned in the Applicable Data Protection Laws.

2. DEFINED TERMS

Anonymization means making Personal Data incapable of being associated with an identified or identifiable natural person under any circumstances, even by matching with other data.

Applicable Data Protection Laws, all relevant privacy, data protection or related laws and regulations in Turkey (Law on the Protection of Personal Data) in the European Economic Area (EEA), in the UK and in Switzerland that apply to the Processing of Personal Data, including but not limited to the EU General Data Protection Regulation 2016/679.

Arçelik, represents all companies directly or indirectly, individually or jointly controlled by Arçelik A.Ş. and Arçelik A.Ş.'s joint ventures included in the consolidated financial report.

Business Partners means suppliers, dealers, authorized service companies, all kinds of representatives, subcontractors and consultants acting on behalf of the Company.

Data Controller refers to the natural or legal person who determines the purposes and means of processing Personal Data and is responsible for the establishment and management of the data recording system.

Explicit Consent refers to the consent that is based on information and freely expressed regarding a specific subject.

Global Data Protection Officer: The Company official responsible for ensuring compliance with Applicable Data Protection Laws, identifying and preventing risks, preventing all kinds of violations and managing processes. Global Data Protection Officer can be assigned by the Arçelik A.Ş.'s Legal and Compliance Director.

Koç Group, represents all companies directly or indirectly, individually or jointly controlled by Koç Holding A.Ş.

Local Data Protection Officer: In case his employment is legally required by the Applicable Data Protection legislation; It is the Company officials who report to the Global Data Protection Officer and manage the processes locally in order to ensure compliance with these regulations, identify and prevent risks, and prevent all kinds of violations. Local Data Protection Officer can be assigned and dismissed by the Legal and Compliance Director.

Personal Data, any data relating to an identified or directly or indirectly identifiable natural person ("Data Subject"); identification can occur by reference to an identifier such as a name, identification number, location data, an online identifier, or to one or more factors specific to an Individual's physical, physiological, genetic, mental, economic, cultural or social identity.

Personnel means all permanent employees, officials, subcontracted workers, full or part-time employees, relevant third-party consultants and temporary employees acting on behalf of Arçelik organizations and subject to this Policy.

Process or Processing, any operation or set of operations performed upon Personal Data, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure, dissemination or otherwise making available, international transfer, alignment or combination, blocking, erasure or destruction.

Processor refers to the natural or legal person who processes personal data on behalf of the Data Controller, based on the authority given by the Data Controller.

Related Person, the natural person whose personal data is processed (customers, visitors, employees and employee candidates, etc.).

Data Security Measures refers to measures aimed at preventing, mitigating or compensating Privacy Violations, including legal, organizational or technical measures targeting the integrity, availability and confidentiality of Personal Data.

Personal Data Breach refers to the unintentional or unlawful destruction, loss, alteration, unauthorized disclosure or access to Personal Data.

Special Categories of Personal Data or Sensitive Personal Data, any Personal Data relating to an Individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic characteristics, biometrics, health, sex life, sexual orientation, or criminal convictions.

The Data Controllers Registry (VERBIS) is a registration system in which data controllers have to register and declare information about their data processing activities.

3. RESPONSIBILITIES

- Company employees and managers are obliged to comply with this Policy. The Company expects its Business Partners to comply with this Policy to the extent applicable to the relevant party and transaction and takes the necessary steps for this.

- Senior management within Company is responsible for enforcing compliance with this Policy, including the maintenance of an appropriate governance structure and the allocation of resources necessary to ensure compliance and enforcement.

- Personnel shall promptly notify the Global Data Protection Officer if they suspect or are aware that this Policy conflicts with any local legal or regulatory obligation or that a particular Company practice violates this Policy.

- Company may implement additional policies, procedures or practices as may be necessary to ensure compliance with this Policy or meet local Applicable Data Protection Laws.

4. IMPLEMENTATION OF THE POLICY

a. General Terms

Company strives to Process Personal Data in a manner consistent with this Policy and with Applicable Data Protection Laws. Where Applicable Data Protection Laws impose a higher level of protection than this Policy, Company must comply with such laws or regulations.

b. Basic Principles

i. Lawfulness and Purpose Limitation

Company shall only Process Personal Data lawfully, fairly and for specified, explicit and legitimate business purposes and with an appropriate justification (legal basis) under Applicable Data Protection Laws. This justification can be consent of the Data Subjects, the performance of an agreement or taking steps prior to entering into an agreement, a legal obligation, or a legitimate interest of Company that is not outweighed by the interests or fundamental rights and freedoms of the Data Subjects. Where Company is required by applicable law or by internal policies to request and obtain the consent of the Data Subjects prior to the Processing of certain Personal Data then Company shall seek such consent and honor it. Company shall keep a record of consents that it obtains and put in place effective means for Data Subjects to withdraw their consent.

ii. Data Minimization

Company shall limit its Processing of Personal Data to the minimum amount of information necessary to pursue the established purpose or purposes. Where possible, Company shall rely on information that does not identify Data Subjects.

Company shall minimize the extent of its Processing, access to and retention of Personal Data to what is necessary for the established purpose or purposes. Access shall be limited to a need-to-know basis. Save exceptions, Personal Data shall not be made accessible to an indefinite number of individuals.

iii. Maintaining Integrity and Quality

Company shall at all times maintain the integrity of the Personal Data IT Processes and take reasonable steps to keep Personal Data accurate, complete, up-to-date and reliable for its intended use.

iv. Retaining and Deleting Personal Data

Company shall not retain Personal Data for longer than necessary. Personal Data must be destroyed by deletion, destruction, or anonymization in accordance with applicable Company Policies and record retention schedules, including the Company's Global Personal Data Protection and Record Retention Policy.. These Company policies and record retention schedules take into account Company's business needs, its legal obligations, and scientific, statistical or historical research considerations.

c.Transparency

i. Company shall provide clear information to Data Subjects about, at a minimum:

- the identity and the contact details of Company acting as the controller.of the Personal Data and of its Global Data Protection Officer, if such exists, or of its Data Protection Officers at local level;
- the categories of Personal Data relating to Data Subjects that Company Processes;
- the purposes for which the Personal Data is Processed, and the Company's justifications for such Processing;
- disclosures of the Personal Data to third-party recipients;
- the rights of Data Subjects in respect of their the Personal Data, including their right to lodge a complaint with a supervisory authority;
- transfers of Personal Data outside Turkey, the EEA, the UK and Switzerland and the legal safeguards applying to such transferred Personal Data;
- the retention period or the criterion used to determine the retention period of the Personal Data;
- whether the provision of the Personal Data is mandatory and the possible consequences if the Individual fails to provide the Personal Data; and
- the existence of automated decision-making which produces legal or similar effects and information about the logic involved, where relevant.

ii. Data Subjects shall be provided with any additional information required by local Applicable Data Protection Laws.

iii. Save limited exceptions, the information set out above shall be provided to the Data Subjects at the time their Personal Data is obtained.

iv. All communications to Data Subjects about the Processing of their Personal Data shall be approved by the local Data Protection Officer and, where necessary, by the Global Data Protection Officer based on Company's templates.

v. Applicable Data Protection Laws may provide for derogations to the transparency requirement in exceptional cases, for example, where providing such information imposes a disproportionate burden. Such derogations shall not be relied upon without prior consultation of the Global Data Protection Officer.

d. Rights of Data Subjects

i. Company should consider the Personal Data requests of the Related persons regarding access rights, restrictions, data portability, deletion, opposition or withdrawal of consent based on the rights envisaged in the Applicable Data Protection Laws. .Such requests shall be free of charge.

ii. Company must respond to these requests as soon as possible and ensure that the request is met, Unless a shorter period of time is stipulated by the Applicable Data Protection Laws at the latest within one month.

iii. Company is not obliged to meet a request when it cannot lawfully relate Personal Data to the Individual making the request or when a request is manifestly unfounded because of its repetitive nature.

iv. While the relevant application is being finalized, information should be given in a language and format that the person can understand. In the event that the application of the person concerned is rejected, the response is insufficient, or the application is not answered in due time, necessary warnings should be made within the Company and awareness should be raised about the right to complain to the relevant authority.

v. During the acquisition of Personal Data, the persons concerned should be informed in accordance with the Applicable Data Protection Laws. In this context, Personal Data collection channels should be determined by the Company in order to fulfill its obligation of disclosure; Regarding these collection activities, the related persons should be informed about the clarification texts that have the scope and conditions sought in the Applicable Data Protection Laws and appropriate processes should be designed accordingly.

vi. Personal Data collection channels should be kept up-to-date by Arçelik in a list and shared with the company's department or officer responsible for compliance and Koç Holding Legal and Compliance Consultancy at 6-monthly periods (June-December) twice a year.

e. Processing Personal Data

i. As a rule, Personal Data should be processed in accordance with at least one of the conditions specified in the Applicable Data Protection Laws. It should be determined whether the Personal Data processing activities carried out by the Company business units are carried out based on at least one of these conditions, and Personal Data processing activities that do not meet this requirement should not be included in the processes.

ii. Personal Data must be processed for legitimate and lawful reasons. Arçelik should process Personal Data in connection with its activities and process it whenever it is legally necessary.

iii. Personal Data should only be retained for the period stipulated in the Applicable Data Protection Laws or required by the Personal Data processing purpose. In this context, first of all, it should be determined whether a certain period is foreseen for the storage of Personal Data in the Applicable Data Protection Laws, if any period is determined, this period should be acted upon, and if the period is not determined, Personal Data should be kept for the period necessary for the realization of the purpose of processing. Personal Data should be deleted, destroyed or anonymized in the event that the period expires or the reasons for its processing disappear. Personal Data should not be stored for future use.

iv. As a rule, Special Categories of Personal Data should be processed in accordance with the conditions determined in the Applicable Data Protection Laws. It should be ensured that the Special Categories of Personal Data processing activities carried out by the business units of the Company are acted in accordance with these conditions, the administrative and technical measures to be taken regarding the processing of Special Categories of Personal Data and the existence of the following conditions should be ensured:

(i) Special Categories of Personal Data other than health and sexual life may be processed without the Explicit Consent of the person concerned, provided that it is expressly stipulated in the law, in other words, there is a clear provision in the relevant law regarding the processing of Personal Data. Otherwise, the Explicit Consent of the person concerned should be obtained.

(ii) Special Categories of Personal Data regarding health and sexual life can be processed for the purpose of protection of public health, preventive medicine, medical diagnosis, treatment and care services, planning and management of health services and financing, without seeking the Explicit Consent of persons under the obligation of keeping confidentiality or authorized institutions and organizations. Otherwise, the Explicit Consent of the person concerned should be obtained.

Processing activities on Special Categories of Personal Data should be carried out, taking into account the regulations stipulated in the Applicable Data Protection Laws regarding the processing of sensitive Personal Data and their transfer to third parties at home and abroad; In addition to the above-mentioned issues, Personal Data processing activities should be carried out by fulfilling the special requirements of the Applicable Data Protection Laws in these cases.

f. Maintaining Appropriate Security and Reporting Personal Data Breaches

i. Company should apply Data Security Measures to ensure the security of data, especially in all transactions concerning the transfer of Personal Data.These Data Security Measures shall take into account the risks represented by the Processing, the nature of the Personal Data concerned, the state of the art and cost of the implementation of the Data Security Measures.

ii. The Data Security Measures shall be set out in written security policies and procedures.

iii. Personnel must immediately report the Personal Data Breach to Arçelik A.Ş.'s Global Data Protection Officer and Information Security and Telecommunication Departments and keep a record of the Security violations in accordance with the Company's Data Breach Protocol..

iv. With the awareness of the importance of ensuring data security in all aspects within the Company, appropriate and necessary technical and administrative measures should be taken to prevent the unlawful processing or access of the processed Personal Data and to ensure that the data is kept in accordance with the law. In this context, the necessary audits should be carried out by the Company and/or should be done by a third party. Employees should be given training on the Applicable Data Protection Laws within the scope of the measures by the Company. Arçelik should inform the Company's Local Data Protection Officer or Global Data Protection Officer and Koç Holding Legal and Compliance Consultancy should be informed about the trainings held within this scope.

g. Disclosure of Personal Data

i. Company shall only disclose Personal Data only when required by law and as long as it is not contrary to the Applicable Data Protection Laws.

ii. For the sake of privacy and security of Personal Data, the Company should carefully select the Data Processors working with, subject them to contractually committed controls and ensure that Data Processors comply with the Applicable Data Protection Laws.

h. International Transfers of Personal Data

i. Company shall only transfer Personal Data only in accordance with the terms in the Applicable Data Protection Laws.

ii. Save limited exceptions under the Applicable Data Protection Laws, Company shall put in place appropriate safeguards, such as transfer agreements to overcome restrictions on international transfers of Personal Data under the Applicable Data Protection Laws.

iii. Exceptions under the Applicable Data Protection Laws regarding restrictions on International Transfers may only be processed after review and approval by the Company's Global Data Protection Officer.

i. Training

Employees Processing Personal Data as part of their role or function shall be regularly trained on compliance with this Policy. Training should be adapted to the role or function of the Personnel concerned. Arçelik should inform the Company's Local Data Protection Officer or Global Data Protection Officer and Koç Holding Legal and Compliance Consultancy regarding the trainings held within this scope.

j. Monitoring and Records

i. The Global Data Protection Officer and the local Data Protection Officers shall conduct periodic reviews and audits to ensure compliance with this Policy.

ii. In the event that the processed Personal Data is obtained by others illegally, this should be reported to the related person as soon as possible and to the relevant authorities in accordance with the Applicable Data Protection Laws. In this context, the necessary infrastructure should be established by the Company, which will include the Local Data Protection Officer and the Global Data Protection Officer. In addition, in such cases, Koç Holding Legal and Compliance Consultancy should be informed immediately.

iii. Company shall maintain a record of Processing operations. The record must be made available to supervisory authorities upon request.

iv. Arçelik companies located in Turkey, which are obliged to register with VERBIS according to the criteria determined in the Turkish Legislation, must register with VERBIS as a Data Controller. In case of a change in the registered information, the information must be updated in VERBIS within seven days from the date of the change. The updates made in VERBIS by Arçelik companies residing in Turkey should be reported to Koç Holding Legal and Compliance Consultancy by the Global Data Protection Officer at 6-monthly periods (June-December) twice a year.

k. Compliance and Waivers

i. Requirements imposed by this Policy may be waived only on a case-by-case basis in exceptional circumstances and subject to conditions, following approval from the Global Data Protection Officer.

ii. Any member of Personnel not compliant with this Policy may be subject to disciplinary measures, including termination of employment.

iii. Violation of this Policy may result in serious consequences for the Company's relevant managers and employees, including legal, administrative and criminal sanctions depending on the Applicable Data Protection Laws in the region of operation, and most importantly, the reputation of the Company and Koç Group. In case of violation of this Policy by third parties, the legal relationship between the said parties and Koç Group may be terminated immediately.

5. MORE INFORMATION

Arçelik Legal and Compliance Directorate is the unit responsible for the implementation of this Policy.

Company shall circulate this Policy to the Personnel and may translate the Policy into local languages for information purposes. In case of discrepancies between local language and the English version, the English version of the Policy shall prevail.

Questions or concerns regarding this Policy or privacy matters more generally must be directed to the Global Data Protection Officers Office (contactable via phone on +90 212 314 34 34 or e-mail at compliance@arcelik.com). As an alternative method, you can make all your notifications about ethical violations via the link “www.ethicsline.net”.

Version Date: 15.06.2022