Arçelik

GLOBAL DATA PRIVACY POLICY

GLOBAL DATA PRIVACY POLICY

1. PURPOSE AND SCOPE

Arçelik and its affiliates and subsidiaries (together "**Company**", "**we**", "**us**") is committed to protecting the privacy of everyone we do business with, including our customers, suppliers, employees and contractors. In recognition thereof, Company has adopted this Data Privacy Policy (the "**Policy**").

2. DEFINED TERMS

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.

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 - employees, officers, contingent workers, employed on a full or part-time basis, or retained as third-party consultants, and temporary staff acting on behalf of any Arçelik 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 - any entity who Processes Personal Data on behalf of any Arçelik subject to this Policy.

Security Breach - a breach of security leading to the accidental or unlawful destruction, loss, alternation, unauthorized disclosure of, or access to, Personal Data.

Security Measures - measures, including legal, organizational and technical measures aimed at ensuring the ongoing integrity, availability, and confidentiality of Personal Data and at preventing, mitigating or remedying Security Breaches.

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.

3. RESPONSIBILITIES

a. Personnel is responsible for complying with this Policy when they Process Personal Data in connection with their normal work activities.

b. 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.

c. 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.

d. 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. Arçelik shall not adopt or implement such policies, procedures or practices without prior consultation and approval from the Global Data Protection Officer.

4. GENERAL POLICY

a. 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 shall be destroyed or anonymized in compliance with applicable Company policies and record retention schedules, including the Company Records 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 shall consider any request from Data Subjects in relation to their rights of access, rectification, restriction, data portability, erasure, or opposition or any clear indication that the Data Subjects want to withdraw their consent. Such requests shall be free of charge.

ii. Company shall respond to such requests within one month and make all efforts to meet the request within this timeframe in accordance with the Company Data Subject Rights Policy.

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 or excessive because of its repetitive nature.

e. Maintaining Appropriate Security and Reporting Security Breaches

i. Company shall implement Security Measures to protect Personal Data, in particular in case of transmissions of Personal Data over a network or the storage of Personal Data on portable devices or media. These 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 Security Measures.

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

iii. Personnel shall promptly report a Security Breach to the Global Data Protection Officer and Information Security and Telecommunications Departments of Arçelik and keep a record of the Security Breaches in accordance with the Company Data Breach Policy.

f. Disclosure of Personal Data

i. Company shall only disclose Personal Data to third parties, such as law enforcement authorities or courts, business partners, suppliers or customers where specifically authorized to do so by applicable laws in Turkey, the EEA, the UK or Switzerland or otherwise in accordance with Applicable Data Protection Laws.

ii. When relying on Processors, Company shall select Processors carefully and subject them to contractual controls in order to protect the confidentiality and security of the Personal Data concerned and meet the requirements of Applicable Data Protection Laws.

g. International Transfers of Personal Data

i. Company shall only transfer Personal Data to a country outside Turkey, the EEA, the UK and Switzerland in accordance with the requirements set out in Applicable Data Protection Laws.

ii. Save limited exceptions under 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 Applicable Data Protection Laws.

iii. Company may only rely on exceptions under Applicable Data Protection Laws to restrictions on international transfers following review and approval by the Global Data Protection Officer.

h. 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.

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

j. 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.

5. MORE INFORMATION

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).

Version Date: 2.12.2019