Beko

Global Data Privacy Policy

1. PURPOSE AND SCOPE

Arçelik A.Ş. and/or any of its affiliates (together or independently referred to as "Company" or "Beko") 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, the Company has adopted this Global Data Privacy Policy (the "Policy"). This Policy aims to determine the framework and coordinate the compliance activities to be carried out specifically for Beko 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 laws and the principles of integrity,
- ensuring Personal Data are accurate and, where necessary, kept up to date,
- processing Personal Data for specific, explicit, and legitimate purposes,
- ensuring that data processing is relevant and limited to what is necessary for the purposes for which they are processed,
- retaining personal data only for as long as necessary for the processing purposes or as required by Applicable Data Protection Laws.

2. DEFINED TERMS

Anonymization	:	shall mean 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	:	shall mean all relevant privacy, data protection or related laws and regulations, including but not limited to EU General Data Protection Regulation 2016/679 ("GDPR") and Turkish Personal Data Protection Law No 6698 ("KVKK").
"Beko" or "Company"	:	refers to all companies directly or indirectly, individually or jointly controlled by Arçelik A.Ş. and it's joint ventures.
Business Partners	:	shall mean suppliers, dealers, authorized service companies, all kinds of representatives, subcontractors and consultants acting on behalf of the Company.

Data Controller	:	shall refer to the natural or legal person who has the primary responsibility for managing Personal Data, including its collection, purpose, and means of processing. The data controller must ensure compliance with relevant data protection laws, oversee data processing activities, and uphold individuals' rights regarding their personal data.
Data Processor	:	shall refer 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.
Data Protection Authority	:	unless otherwise defined in Applicable Data Protection Laws, shall mean independent public authorities that supervise, through investigative and corrective powers, the application of the Applicable Data Protection Laws. Data Protection Authorities provide expert advice on data protection issues and handle complaints lodged against violations of the Applicable Data Protection Laws.
Data Subject	:	shall mean an identified or identifiable natural person whose personal data is collected, processed, or stored by the Company.
Explicit Consent	:	shall refer to a clear, specific, and informed agreement by an individual to the processing of their personal data. It shall be typically given through a deliberate action, such as signing a document or selecting an option electronically, indicating the individual's direct and unambiguous approval of the particular use of their data.
Global Data Privacy Team	:	shall refer the Company's main responsible for ensuring compliance with Applicable Data Protection Laws, identifying, and preventing data privacy related risks and managing personal data related processes reporting to Head of Global Data Privacy. Head of Global Data Privacy can be assigned by the General Counsel of Arçelik A.Ş.
Koç Group	:	shall represent all companies directly or indirectly, individually, or jointly controlled by Koç Holding A.Ş.
Koç Holding	:	shall represent Koç Holding A.Ş.
Local Privacy Responsible ("LPR")	:	shall mean contact person appointed for each country and/or region within the Company, who reports to the Global Data Privacy Team and is responsible for implementing and monitoring data privacy compliance.

Personal Data	:	shall mean any information relating to an identified or identifiable natural person.
Personal Data Breach	:	shall refer to a potential or confirmed breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data.
Personnel	:	shall mean all permanent employees, officials, subcontracted workers, full or part-time employees, relevant third-party consultants and temporary employees acting on behalf of Company and subject to this Policy.
Privacy Impact Assessment (PIA)	:	shall mean a systematic process for assessing the impact of data processing activities on the privacy of individuals. It helps identify and mitigate privacy risks associated with specific projects or initiatives.
Process or Processing	:	shall mean any operation or set of operations performed on personal data or sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction of data**.**
Records of Processing Activities	:	shall refer to significant information about data processing, including data categories, the group of data subjects, the purpose of the processing and the data recipients.
Special Categories of Personal Data or Sensitive Personal Data	:	shall refer to personal information that is more sensitive in nature, requiring higher protection due to the risk of discrimination or harm if mishandled. The types of special categories of data might be different depending on the Applicable Data Protection Laws. These categories typically include data related to racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic and biometric data, health information, and an individual's sex life or sexual orientation.
Technical and Organizational Measures	:	shall refer to measures and guidelines with regards to the privacy, security and protection requirements described under Applicable Data Protection Laws.
The Data Controllers Registry	:	shall mean the registration system in which data controllers have to register and declare information about their data processing activities (i.e., VERBIS for Turkey).

3. RESPONSIBILITIES

- The Company together with its employees shall be required to comply with this Policy. Additionally, the Company shall expect its Business Partners to adhere to this Policy as applicable to their respective roles and transactions, and to take necessary steps to ensure compliance.

- Senior management within the Company shall be 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 Privacy Team if they suspect or are aware that this Policy conflicts with any local legal or regulatory obligation or if a particular Company practice violates this Policy.

- The Company shall implement additional policies, procedures, or practices as necessary to ensure compliance with this Policy and Applicable Data Protection Laws.

4. IMPLEMENTATION OF THE POLICY

a. General Terms

The Company shall strive 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, the Company must comply with such laws and regulations.

b. Basic Principles

i. <u>Lawfulness and Purpose Limitation</u>

The 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 shall 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 the Company that is not outweighed by the interests or fundamental rights and freedoms of the Data Subjects. Where the 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 the Company shall seek such consent and honor it. The Company shall keep a record of consents that it obtains and put in place effective means for Data Subjects to withdraw their consent. The Company shall provide clear information to Data Subjects about the purpose of processing Personal Data, the legal basis for processing, and whether Personal Data is used in accordance with its intended purpose and legal compliance reasons.

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.

ii. Data Minimization

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

The 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 Accuracy, Integrity and Quality

At all times, the Company shall maintain the integrity of the Personal Data and take reasonable steps to keep Personal Data accurate, complete, up to date, and reliable for its intended use. Every reasonable step must be taken to ensure that personal data that is inaccurate, considering the purposes for which it is processed, is erased, or rectified without delay.

iv. Storage Limitation

The Company shall not retain Personal Data for longer than necessary. Personal Data must be destroyed by deletion, destruction, or anonymization in accordance with Global Data Retention and Deletion Policy which takes into account the Company's business needs, its legal obligations, and scientific, statistical or historical research considerations.

v. Confidentiality (Security)

The Company shall process Personal Data in a manner that ensures appropriate security of the data, including protection against unauthorized or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organizational measures.

The Company shall develop, implement, and maintain safeguards appropriate to its size, scope and business, our available resources, the amount of Personal Data that the Company owns or maintains on behalf of others, and identified risks (including use of encryption and Pseudonymization where applicable). The Company shall regularly review and test the effectiveness of those safeguards to ensure the security of Personal Data.

vi. Accountability

The Company shall be able to demonstrate, compliance with the other data protection principles; and have adequate resources and controls in place to ensure and to document Data Protection Legislation compliance including:

a) implementing Privacy by Design when Processing Personal Data and completing PIAs where Processing presents a high risk to rights and freedoms of Data Subjects,
b) integrating data protection into internal documents including this Policy, Related Policies and Procedures, or Privacy Notices,
c) regularly training the Company Personnel on Data Protection Legislation, this Policy, Related Policies and Procedures and data protection matters including, for example, Data Subject's rights, Consent, legal basis, PIAs and Personal Data Breaches. The Company must maintain a record of training attendance by the Company Personnel, and
d) regularly testing the privacy measures implemented and conducting periodic reviews and audits to assess compliance.

vii. Transparency

The Company shall provide clear information to Data Subjects when required by Applicable Data Protection Law. Depending on the country and the region this information shall include:

- the identity and the contact details of the Company acting as the controller of the Personal Data and/or any additional contact information required by Applicable
- the categories of Personal Data relating to Data Subjects that the 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 Personal Data, including their right to lodge a complaint with a Data Protection Authority;
- transfers of Personal Data outside the countries/regions of origin and disclosure shall encompass details about the legal safeguards governing such international transfers. The Company ensures that any data transfers align with the specific regulations outlined in the Applicable Data Protection Laws of the countries involved, thereby maintaining compliance on a global scale.
- the retention period or the criterion used to determine the retention period of the Personal Data;
- the existence of automated decision-making which produces legal or similar effects and information about the logic involved, where relevant.

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

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

All communications to Data Subjects about the Processing of their Personal Data shall be approved by the LPR and, where necessary, by the Global Data Privacy Team or Head of Global Data Privacy based on the Company's templates.

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 LPR where necessary, by the Global Data Privacy Team or Head of Global Data Privacy.

c. Rights of Data Subjects

i. The Company shall consider the Personal Data requests of the Data Subjects regarding access rights, restrictions, data portability, deletion, opposition, or withdrawal of consent based on the rights envisaged in the Applicable Data Protection Laws.

ii. Requests can be communicated to the Company in any way, including via email, fax, letter, telephone, website request or via a third-party. The individual does not need to state that it is a request to access.

iii. The Company Personnel who receive a request must forward it to the Local Privacy Responsible immediately.

iv. The Company shall 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 and at the latest within 30 days from receipt of the request.

v. The Company shall verify the identity of Data Subject in order not to allow third parties to persuade the Company into disclosing Personal Data without proper authorization. The request must come from the individual who is requesting to access their own information, or any person representing or acting on behalf of the requesting party, or a person with parental responsibility (in the case of a request made by/on behalf of a minor). The Company shall require written evidence that any person acting in such capacity has appropriate authority to make the request.

vi. The Company is not obliged to meet a request when it cannot lawfully relate Personal Data to the Individual making the request or it is manifestly unfounded because of its repetitive nature or it is contrary to our legal obligations or infringes the rights of any other person concerned.

vii. Where the Company has decided not to comply with a request, the Local Privacy Responsible and when necessary, the Global Data Privacy Team must contact the individual and explain why the request shall not be complied with.

viii. Information shall be provided in a language and format that the Data Subject can understand. In the event that the request is rejected, the response is insufficient, or the request is not answered in due time, necessary warnings shall be made within the Company and awareness shall be raised.

ix. During the collection of Personal Data, the data subjects concerned shall be informed in accordance with the Applicable Data Protection Laws. In this context, Personal Data collection channels, tools and landing pages shall be identified by the Company in order to fulfill its obligations. Regarding these collection activities, the Data Subjects shall be informed through the privacy notices that have the scope and requirements established in the Applicable Data Protection Laws and appropriate processes shall be designed accordingly.

x. Personal Data collection channels shall be kept up to date by the Company in a list and shared with the Global Data Privacy Team and Koç Holding Legal and Compliance Team biannually in June and December.

d. Processing Personal Data

i. As a rule, Personal Data shall be processed in accordance with at least one of the legal basis of data processing specified in the Applicable Data Protection Laws. It shall be Applicable Data Protection Laws and the Global Data Retention and Deletion Policy, if any whether the Personal Data processing activities carried out by the Company business units are carried out based on at least one of these legal basis and Personal Data processing activities that do not meet this requirement shall not be included in the processes.

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

ii. As a corporate policy, Special Categories of Personal Data shall be processed in accordance with the requirements and legal basis of processing personal data determined in the Applicable Data Protection Laws. It shall be ensured that the Special Categories of Personal Data processing activities carried out by the business units of the Company are processed in accordance with these requirements and legal basis. The technical and the organizational measures to be implemented regarding the processing of Special Categories of Personal Data and the implementation of the measures determined in the Applicable Data Protection Laws shall be ensured.

Processing activities involving Special Categories of Personal Data shall comply with the regulations outlined in the Applicable Data Protection Laws, particularly concerning the processing of sensitive Personal Data and its transfer to third parties, both locally and internationally. Additionally, these processing activities must fulfill the specific requirements set forth by the Applicable Data Protection Laws for such cases.

e. Maintaining Appropriate Security and Reporting Personal Data Breaches

i. The Company shall apply all appropriate Technical and Organizational Measures to ensure the security of data, especially in all transactions concerning the domestic or international transfer of Personal Data internally within the organization or to third parties. These Technical and Organizational Measures shall take into account the risks originated by the Processing, the nature of the Personal Data processed, the state of the art and cost of the implementation of the Technical and Organizational Measures.

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

iii. Personnel shall immediately report a suspected Personal Data Breach to the relevant LPR and follow the steps described in the Company's Procedure for Global Data Breach Management.

iv. Recognizing the importance of data security in all aspects of the Company, appropriate and necessary Technical and Organizational Measures must be implemented to prevent unlawful processing or access to Personal Data and to ensure that the data is maintained in compliance with the Applicable Data Protection Laws. In this context, the necessary audits shall be carried out by the Company and/or third party. Employees shall be given training on the Applicable Data Protection Laws as part of the measures implemented by the Company.

f. Disclosure of Personal Data

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

ii. To protect the privacy and security of Personal Data, the Company shall carefully select its Data Processors, subject them to contractually mandated controls and ensure that Data Processors comply with the Applicable Data Protection Laws.

g. International Transfers of Personal Data

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

ii. Except for limited exceptions under the Applicable Data Protection Laws, the Company shall implement appropriate safeguards, such as transfer agreements, to address restrictions on international transfers of Personal Data as stipulated by these laws.

iii. Exceptions under the Applicable Data Protection Laws regarding restrictions on international transfers shall only be processed after review and approval by the relevant LPRs and in any case with the approval of the Global Data Privacy Team.

h. Training

Employees Processing Personal Data as part of their role or function shall be regularly trained for compliance with this Policy. Training shall be adapted to the role and/or function of the Personnel concerned. The LPRs shall inform the Global Data Privacy Team regarding the trainings held within this scope; and the Global Data Privacy Team shall forward information to Koç Holding Legal and Compliance Team.

i. Monitoring and Records

i. The Global Data Privacy Team and the LPRs 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 shall be reported to the Data Subject as soon as possible and to the relevant Data Protection Authority in accordance with the Applicable Data Protection Laws. This Process shall be conducted in accordance with the Company's Procedure for Global Data Breach Management.

In addition, in such cases, Koç Holding Legal and Compliance Team shall be informed accordingly.

iii. The Company shall maintain a Record of Processing Activities, if required by the Applicable data Protection Laws, these records must be made available to the relevant Data Protection Authority upon request.

iv. Our Companies located in Turkey, which are obliged to register with VERBIS according to the criteria determined in the Turkish Legislation, shall 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 of the date of the change. The updates made in VERBIS by our Companies residing in Turkey shall be reported to Koç Holding Legal and Compliance Team by the Global Data Privacy Team at 6- monthly periods (June-December) twice a year.

j. Compliance and Waivers

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

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

iii. Violation of this Policy shall 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 business relationship between the said parties and Koç Group may be terminated.

5. MORE INFORMATION

Legal and Compliance Directorate shall be the unit responsible for the implementation of this Policy.

The 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 Privacy Team Office (contactable via e-mail at globalprivacy@beko.com). As an alternative method, you can make all your notifications about ethical violations via the link "www.ethicsline.net".

Version Date: 01.06.2024