PRIVACY NOTICE
REGARDING INTERNAL REPORTING OF ETHICS & COMPLIANCE INFRINGEMENTS

1. Scope of this Privacy Notice

This Privacy Notice explains what personal data (information) we will process during the process of collecting, documenting, evaluating whistleblower reports **("Process")** carrying out follow-up actions, keeping records and handling confidential whistleblowing reports, under **European Whistleblowing Policy** (which was prepared on the basis of and complies with **Global Whistleblowing Policy** and **Koç Group Whistleblowing Policy ,** covered under Arçelik's and Koç's Global Code of Conduct (**jointly hereinafter referred to as the "Policies"**), and related Guidelines, Legal and Administrative Acts.

These Policies describes standard and custom ad hoc ethics investigation reporting within the group (acts against the interest of the company, unfair practices against employees, noncompliant actions of business partners, regulatory breaches, violations of law, policy, and other workplace misconduct) and will explain you, among other things:

- whether the report can be anonymous;
- which are the reporting mechanisms to protect whistleblowing's identity,
- what the whistleblower's report may concern,
- who can be a whistleblower,
- who and how will conduct the proceedings in connection with the whistleblower's report,
- what are the whistleblower's (and other involved people) rights.

Before reporting, please read Policies, especially European Whistleblowing Policy

This Privacy Notice applies to Arçelik A.Ş, or Beko Europe Management SRL and all companies directly or indirectly, individually or jointly controlled by Arçelik A.Ş. and it's joint ventures (hereinafter referred to as "Beko", as '**we**' or '**us**' or '**our**').
Beko Europe belongs to Arçelik A.Ş. and Koç Holding A. Ş. is the parent company of Arçelik A.Ş, responsible for managing the global Navex account (the access rights of Koç Holding and relevant Group Companies will be explained below – point 3).

This does not mean that the role of individual companies within the Group Companies is going to be always the same. The scope of access to the reports and other data is strictly limited and covered by confidentiality rules. This issue will be explained in detail below (point 3).

This Privacy Notice applies to Beko employees, as well as others who may be whistleblowers under Policies and the applicable legislation, such as, but not limited to:

- former employees;
- applicants;
- volunteers;
- interns;
- trainees;

- suppliers' or subcontractor's employees;
- shareholders and individuals being members of the Company's administrative, management or supervisory bodies.

The Privacy Notice also applies to the processing of other individual's data, e.g. those to which the whistleblower's report relates to, such as: involved person allegedly committing wrongdoing, witnesses, informants, third parties mentioned in whistleblowing report (data subjects).

We take into account the provisions of the Whistleblower Protection UE Directive (2019/1937) as well as national regulations in the EU implementing the directive and the provisions of the GDPR and other relevant legislations.

2. Who collects information about you? Roles and responsibilities during the processing of personal data

Since entities from Group Companies may have access to your data processed during the Process and under the Policies, they are joint controllers within the meaning of the GDPR. The principles of joint controllership are described below (see below – point 10).

Joint controllership means that we are responsible for deciding how we hold and use certain information about you.

Joint control does not mean that each of the companies in the structure of Group Companies will have the same scope of access and responsibility. It will be limited in accordance with the rules described in point 3 below.

In certain situations, Arçelik A.Ş. or Beko Europe Management SRL will process the data without providing access to its subsidiaries. In such a case the local company will not have access to the case in question. This applies in particular to the following cases:

- the allegation concerns top management positions;
- the person reporting the violation selects this option in the *NAVEX* reporting system (express request of reporting directly to Arçelik A.Ş. or Beko Europe Management SRL).

In any case, Koç Holding A.Ş. is responsible for managing the NAVEX platform and may therefore have access to the data (within limited access according to the *need to know* principle), but in general terms it will not actively handle cases.

3. Reporting channels and who will have access to your data?

The following persons will have access to your data:
a) NAVEX: an external, third-party provider of the platform for the purpose of receiving and processing whistleblower reports - under the data processing agreement / confidentiality agreement (see more: **https://www.navexglobal.com/compliancenext/**

Additional information on the confidentiality policies can be found at: https://www.navex.com/en-us/privacy-statement/).

Koç Holding A.Ş. manages access to the *NAVEX* platform; however, it conducts matters according to the rules set out below (according to the rules regarding authorised persons), with restricted access in accordance with the "need to know" rule.

We use a tool provided by NAVEX to receive and handle whistleblower reports for all Group Companies. Therefore, the whistleblowers will be required to mention the relevant Group company to which the incident relates. You can select relevant Group company here (if the incident relates to a Beko Group Company, Arçelik Group Company will be selected *first). The provider is obliged to maintain confidentiality and comply with the principles of personal data protection. If local regulations require additional reporting channels, you will obtain such information from the Policies and/or your Local Compliance Team.*

This tool is operated by the persons indicated in point b) below.

b) Persons authorised to receive and consider whistleblower reports (Global Compliance team members, Beko Europe Compliance Manager, Compliance Officer and other persons authorised under Whistleblowing policies) ("Authorised persons").

The composition of the team examining the submitted reports depends on whether in a given case there will be joint controllership or acting of Arçelik A.Ş. and Beko Europe Management S.R.L. as independent data controllers. In this last scenario, only authorised persons from Arçelik A.Ş. and Beko Europe Management S.R.L. Legal and Compliance Teams will handle the cases. About the role of Koç Holding A.Ş. as for NAVEX platform see point a) above).

The scope of access concerns two stages:

- access to report (at the stage of reporting a violation);
- conducting an investigation in relation to the report (follow-up).

In the first stage, the access rules are as follows:

A very limited number of employees of the Koç Holding Legal and Compliance Teams as well as Arçelik's and Beko Europe Management S.R.L. Legal and Compliance Team are authorised to have access to all inquiries around the globe. These access rights are strictly controlled and only given to Legal and Compliance team members based on a *need-to-know* basis. Authorised Local Compliance Officers have access only to the records related to their respective countries.

Compliance Officers are responsible for investigating the cases related to their own countries. In these cases, they can revise and close inquiries.

We ensure that the identity of the reporting person is not disclosed to anyone beyond the Authorised persons to receive or follow up on reports, without the explicit consent of that person or provision of the law. This also applies to any other information from which the identity of the reporting person may be directly or indirectly deduced.

The team of Authorised persons may consist of persons from the organisation in which you work as well as those selected (due to their competences) from among other companies. If local law restricts reporting / conducting investigation to company personnel only, contact your Local Compliance Team for information about internal reporting.

We ensure that the indicated authorised persons have a legal authorization from each company in the group. At

the same time, they are committed as to independence, confidentiality, data protection and secrecy.

c) public authorities in legally regulated cases

4. The types of personal data we hold about you and source

In the course of the Process, we process data obtained from the whistleblower as well as during investigation and follow-up actions (including as part of interviewing witnesses or collecting documents).

The source of data collection is the whistleblower. In the Process, data may be obtained from other sources, e.g., from witnesses, informants, authorities, third parties or persons to whom the report relates.

Categories of personal data

The whistleblowing report and the documents issued in the procedure may contain:

For the whistleblower: personal identification (Name and Surname), employment information (Business Unit Division, Company Entity, Job Title Role), contact information (professional e-mail), the country in which is located; the country where the incident took place; the city where the incident took place; the relevant Group company in which the incident relates.

For the person allegedly committing wrongdoing: personal identification (Name and Surname), employment information (Business Unit Division, Company Entity, Job Title Role), contact information (professional e-mail) any other data necessary for the demonstration of the wrongdoing.

For the witness: personal identification (Name and Surname), employment information (Business Unit Division, Company Entity, Job Title Role), contact information (professional e-mail), any other data necessary for the justification of his/her quality as a witness.

For the third party: first name and last name, function and place of employment, any other data contained in the report.

5. Purposes and our lawful bases for processing your personal data

The personal data that we process relating to you are necessary for:

- **compliance with a legal obligation** to which the controller is subject, as established by legal and administrative acts (these include for the purpose and for the period necessary to fulfil the obligations related to the receipt and handling of whistleblower report, including the period of limitation of criminal liability (the basis of the GDPR: Article 6 (1)(c) of the GDPR in connection with the relevant national regulations implementing Directive 2019/1937).

- our **legitimate interests** in connection with incident management of: Breach of Global Code of Conduct

and related Code Policies, mismanagement, abuse of the current job position, any other activity which subverts our operations. Our legitimate interest is also the basis for matters to be conducted under joint controllership.

6. Is providing data mandatory?

Pursuant to Global Whistleblowing Policy, when accessing the Ethics Hotline, the whistleblower has the right:

- not to share his/her name and contact information to remain anonymous,
- to share his/her name and contact information with the service provider of the whistleblowing tool and allow the information to be communicated to Beko. In this case, Beko can contact the informant directly to request any information needed during the investigation.
- to share his/her name and contact information only with the service Provider of the whistleblowing tool, but not with Beko. In this case, Beko can contact the service provider to request additional information when needed.

Thus, providing personal data by the whistleblower is, as a rule, not mandatory - the report can be made anonymously. **However, if the law of the Member State (of the relevant Beko Company) excludes anonymous reporting, then as part of communication with the whistleblower, we will inform you about the need to provide data. In this case, providing personal data will still be voluntary but necessary to accept and consider the whistleblower's report.**

Providing data about or of other persons is mandatory if it results from the content of the law. In this case (indicated persons) will be informed about it separately.

7. Automated decision-making

You will not be subject to decisions that will have a significant impact on you based solely on automated decision-making.

8. Keeping your personal data secure

Safeguarding the confidentiality of the identity of the reporting person during the reporting process and investigations triggered by the report is an essential ex-ante measure to prevent retaliation.

We have put in place appropriate security measures to prevent your personal data from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. In addition, we limit access to your personal data to those employees, agents, contractors and other third parties who have a business need-to-know. They will only process your personal data on our instructions, and they are subject to a duty of confidentiality.

We have also put in place procedures to deal with any suspected data security breach and will notify you and any applicable regulator/authority of a suspected data security breach whenever we are legally required to do so.

9. Transfers of information outside the EEA

When we share your personal data with our Group Companies or other companies with whom we contract (as described section 2-3 above), these companies may be located outside the European Economic Area ("EEA"), the UK or your country of residence, as applicable, in countries with different laws for protecting personal data than the laws in your country of residence. In particular, your personal data may be transferred to our Group Companies located in Turkey (Arçelik A.S. and Koç Holding A.Ş.).

If we transfer your personal data outside the EEA, the UK or your country of residence, as applicable, we will take steps to ensure that your data will receive the same level of protection as if it was being processed within the EEA, the UK or your country of residence, as applicable. For example, we may include standard contractual clauses adopted by the European Commission in our contracts with third parties or our Group Companies to ensure there are safeguards in place to protect your personal data. Please contact us using the details in '**Contact details**' for more information about the specific measures we have taken.

Please note that Arçelik A.S. and Koç Holding A.Ş. may further transfer your personal data to third parties located in countries that do not provide an adequate level of data protection. Such transfers will be carried out in accordance with applicable laws including where applicable, contractual requirements set out in standard contractual clauses.

10. Joint controllership details

Joint controllership applies to the cases indicated in point 2 above. The scope and rules of access under joint control are described in point 3 above.

"other companies" means Arçelik's A.Ş. subsidiaries stated in point 2 above and **Koç Holding A.Ş.**

Obligation under GDPR	Responsible
Art. 5 deciding on data deletion	Arçelik A.Ş. in consultation with other companies - joint controllers
Art. 5 deciding on the scope of the data obtained	Arçelik A.Ş. in consultation with other companies - joint controllers
Art. 6 Requirement of the legal basis	Arçelik A.Ş. in consultation with other companies - joint controllers
Art. 13-14 Providing information on Joint Processing of Personal Data	Arçelik A.Ş.
Art. 12 and 15-22 Rights of the data subject with regard to the Personal Data processed by Joint controllers	Arçelik A.Ş.: - creates and operates a communication channel with the data subject; - receives the request and forwards it to the appropriate Group Company for consultation on how to proceed;

	- responds to the request and implements it.
Art. 30 Records of processing activities	Each joint controller
Art. 26 (2) Making available the essence of this Joint controlling agreement	Arçelik A.Ş.
Art. 28 data processing agreement with IT	Arçelik A.Ş.
Art. 32 Security of processing	Arçelik A.Ş, (technical aspects) Each joint controller - informing employees about the principles of safe use of the platform
Art. 33-34 Notification of a personal data breach to the supervisory authority and to the data subject	Arçelik A.Ş.

Notwithstanding the arrangements referred above, the data subject may exercise his or her rights under this Regulation towards each of the controllers.

11. How long we keep your personal data

We will only retain your personal data in compliance with the confidentiality requirements for as long as necessary to fulfil the purposes we collected it for. We also will do it in a way that is proportionate in order to comply with the requirements imposed by EU Whistleblowing Directive, or other requirements imposed by EU or national law.

Personal data which are manifestly not relevant for the handling of a specific report will not be collected or, if accidentally collected, will be deleted without undue delay.

12. Your rights in connection with your personal data

Under certain circumstances, by law you have the right to:

- **Be informed** on the purposes and methods of the processing of your Personal Data
- **Request access** to your personal data (commonly known as a "**subject access request**"). This enables you to receive a copy of the personal data we hold about you and to check that we are lawfully processing it.
- **Request correction** of the personal data that we hold about you. This enables you to have any incomplete or inaccurate information we hold about you corrected.
- **Request erasure** of your personal data. This enables you to ask us to delete or remove personal data where there is no good reason for us continuing to process it. You also have the right to ask us to delete or remove your personal data where you have exercised your right to object to processing (see below).
- **Object to processing** of your personal data where we are relying on a legitimate interest (or those of a third party) and there is something about your particular situation which makes you want to object to processing on this ground.

- **Request the restriction of processing** of your personal data. This enables you to ask us to suspend the processing of personal data about you, for example if you want us to establish its accuracy or the reason for processing it.
- Receive in a structured, commonly used and machine-readable format Personal Data concerning you and provided by you, as well as to transmit those Personal Data to another party (commonly known as a "**right to portability**").
- **Obtain information about third parties** with whom your data has been shared.

We may need to request specific information from you to confirm your identity and ensure your right to access your Personal Data (or to exercise any of your other rights). This is another appropriate security measure to ensure that Personal Data is not disclosed to any person who has no right to receive it. Without prejudice to any administrative or legal remedy, you also have the right to **lodge a complaint to the competent supervisory Authority**, if you believe that processing of your data breaches the Data Protection Laws.

Where available, these rights (as well as any other right provided for by applicable Data Protection Laws) may be exercised by using the form provided in the "***How to contact us***" section below.

13. How to contact us

If you have any questions about how we use your personal data or this privacy notice in general, please contact us using this form. You can also use this form to contact and ask for information about the DPO (Data Protection Officer) or LPR (Local Privacy Responsible) in charge of data protection compliance within your organisation.

This is a common contact point for all joint controllers. If you want to contact a specific entity write to us and we will send you the contact details of that entity.

The controller's representative (within the meaning of Article 27 of the GDPR) in the EEA is Beko S.A. with its registered office in Warsaw, at 366 Puławska St., (02-819) Warsaw, entered in the Register of Entrepreneurs of the National Court Register kept by the District Court for the Capital City of Warsaw in Warsaw, XIII Economic Department of the National Court Register, under KRS No. 0000078147, with its tax number (NIP): 525 207 35 73

You can contact the data controller (address stated above) directly or the representative at the e-mail address representativegdpr@arcelik.com

14. Supervisory Authorities

Supervisory Authorities are independent public authorities that supervise, through investigative and corrective powers, the application of the data protection law. They provide expert advice on data protection issues and handle complaints lodged against violations of the applicable data protection legislation.

Generally speaking, the main contact point for questions on data protection is the Supervisory Authority in the country where the company/organisation in question is based. However, if that company/organisation processes data in different countries or is part of a group of companies established in different countries, that main contact point may be a Supervisory Authority in another country.

For EEA (European Economic Area) countries find your National Supervisory Authority clicking here.

For UK, the statutory authority is: Information Commissioner's Office (contact details available clicking here).

For Switzerland, the statutory authority is: Federal Data Protection and Information Commissioner (contact details available clicking here).

15. Changes to this Privacy notice

We may change and update this privacy notice from time to time. Any changes to our privacy notice will be posted on this web page. We will notify you of any material changes or additions to this privacy notice.

This Privacy notice was last updated on **May 10 2025**