EUROPEAN WHISTLEBLOWING POLICY

1. GENERAL PRINCIPLES

Beko ("Beko" or "Company" refers to all companies directly or indirectly, individually or jointly controlled by Arçelik A.Ş. and its joint ventures) is committed to sustain the highest possible ethical standards and legal conduct within the Company's business operations.

This European Whistleblowing Policy (hereinafter referred to as the "**Policy**") represents the general framework regarding Whistleblower protection and regulates the way the reports are to be received, reviewed, and closed in a standard and consistent manner.

We are committed to sustain the highest ethical standards and legal conduct within the Company's business operations.

We prioritise compliance with legal requirements and internal regulations. Early detection of infringements allows us to take appropriate measures to prevent or mitigate damages to our customers, employees, business partners and the company itself.

Our aim is to encourage you to confidentially report any information obtained in a professional context regarding breaches of Beko's Global Code of Conduct, internal Policies, or applicable laws to our operations.

We encourage the identification and reporting of inappropriate, unethical, or illegal behaviour at all levels within our organisation.

We are committed to protecting the organisation against ethical breaches, fraud, and any other non-compliance issues that could harm our reputation, lead to commercial damages, or result in legal or contractual breaches or any other violations.

2. DEFINITIONS

"Company" refers to each of Beko Companies directly or indirectly controlled by Beko Europe B.V., Nieuwe Herengracht 119, 1011 SB Amsterdam, The Netherlands, within or without the jurisdiction of Whistleblowing Directive, (EU) 2019/1937.

"**Compliance Officer**" refers to the individuals performing the compliance roles in relevant countries.

"Whistleblower" is the individual reporting information related to breaches of the law that have occurred or are likely to occur, of which they became aware

while carrying out current or previous professional activities of any type, whether paid or not, within the Company.

The category of these individuals may include at minimum:

- ✓ current and former employees.
- ✓ individuals carrying out an independent activity.
- ✓ paid or unpaid volunteers, interns, and trainees.
- ✓ any individual who works for the Company's suppliers/subcontractors, regardless of the type of their employment – based on an employment contract or otherwise.
- ✓ individuals who became aware of any breaches during the recruitment process or during pre-contractual negotiations.
- ✓ shareholders and individuals being members of the Company's administrative, management or supervisory bodies.
- ✓ any individual who reports anonymously information regarding breaches of the law.

"Koç Group" means Koç Holding A.Ş. and companies which are controlled directly or indirectly, jointly, or individually by Koç Holding A.Ş. and the joint venture companies listed in its consolidated financial report.

"Legal basis" primarily refers to Directive (EU) 2019/1937 of the European Parliament and of the Council, concerning the protection of persons who report breaches of Union law. Additional local legislation applicable for certain countries can be found in the **Annex** (Annex - Differences in Local Legislation).

The Policy is supplemented by other internal regulations, The Global Code of Conduct, and related policies.

3. INTERNAL REPORTING METHODS

3.1. The responsible for managing reports of law infringements

The local Compliance team in the Company is the designated department for managing the reports, following the duties laid out in the "Global Code of Conduct Operations Policy".

3.2. Internal reporting channel

Whistleblowers can report facts that consist of an action or omission which represent a non-compliant conduct with the Global Code of Conduct, Compliance Policies, legal requirements (representing disciplinary offences, misdemeanours, crimes) or that breach the intent or purpose of the law.

Whistleblowers can choose to report actual or potential breaches to the following channels:

- Directly to their managers,
- Human Resources representatives,

- Directly to the local Compliance Team (who can be contacted via the emails listed in the **Annex**) if any, or writing to Beko Europe Management S.r.l. to the attention of Legal Department: Ethics & Compliance Office, Via Varesina, 204 - 20156 Milan, Italy,
- Through the Ethics Hotline online or by phone, as indicated below:

  ETHICS HOTLINE WEB INTAKE www.ethicsline.net
  ETHICS HOTLINE PHONE INTAKE
  (see the phone numbers provided in the link; https://secure.ethicspoint.eu/domain/media/en/gui/108227/phone.html)

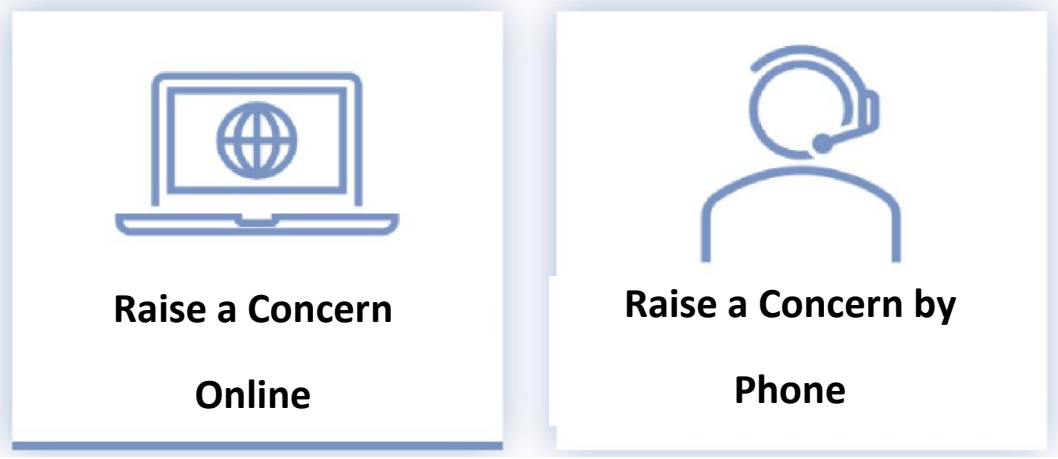
Regardless of the method chosen to report an actual or potential concern, the Whistleblower has the right to ask for a meeting in person (f2f).

3.3. Ethics Hotline reporting mechanism

The Ethics Hotline is a reporting mechanism implemented under the "Global Whistleblowing Policy", which is part of the Global Code of Conduct.

To effectively manage the reporting mechanism for unethical actions, the Company implemented an Ethics Hotline reporting mechanism, which can be used 24/7, anonymously or not, and is available for all Koç Group companies, which Company is a part of.

The licensed third-party service provider, NAVEX, offers a secure and confidential platform for raising concerns and receiving reports of potential misconduct anonymously, either online or by phone. For more details on our Ethics Hotline Mechanism's confidentiality policies, please visit: https://www.navex.com/en-us/privacy-statement/.



www.ethicsline.net

See the phone numbers from the link.

https://secure.ethicspoint.eu/domain/media/en/gui/108227/phone.html

When accessing the Ethics Hotline through the webpage "www.ethicsline.net", the Whistleblowers shall fill in:

- the country in which they are located*;
- the country where the incident took place.
- the city where the incident took place.
- the relevant Koç Group company in which the incident relates**.

> * *The country is required to be selected, to ensure compliance with the data privacy laws applicable in that country. This shall not allow to identify individual reports*.
>
> ** *The relevant Koç Group company in which the incident relates must be selected to allow the service provider to properly notify the designated Compliance Officer of Koç Group affiliated company for handling the report. For the sake of Beko Companies, Whistleblower shall select the affiliated company as "Arcelik-Beko"*.

The Whistleblower has the option to select its preferred language, in which they want the communication to take place.

We have taken appropriate measures to ensure that, at any time, at least one reporting channel is available 24/7. If, for any reason, the phone line does not work at the dialling location, the Whistleblower can report the issue through the Ethics Hotline platform (webpage).

If the Whistleblower opts to use, the toll-free numbers are available here https://secure.ethicspoint.eu/domain/media/en/gui/108227/phone.html, it is important to know that the Whistleblower's phone number cannot be seen (identified) or tracked by the third-party partner. The Whistleblower will receive a report of the conversation and will have the opportunity to verify and modify its content.

If the Whistleblower request to report a concern through an in-person meeting:

- The Compliance Officer may draft conversation notes, subject to the Whistleblower's consent.
- The Whistleblower will have the opportunity to review, correct, and express their agreement regarding the conversation note by signing it.

If the Whistleblower does not confirm the conversation note, they will be directed to report in writing by sending an email to local e-mail addresses placed in the **Annex** or by accessing the online Ethics Hotline platform at www.ethicsline.net.

We encourage the reporting of legal violations through internal reporting channels as a first port of call to raise concerns. However, the Whistleblower can choose between internal or external reporting channels. External reporting channels include public authorities and institutions that, according to specific legal provisions, receive and handle reports of legal violations within their jurisdiction, both nationally and at the European level. More information can be found in the Annex.

3.4. External Reporting channels

As mentioned, Whistleblowers can also choose to report breach of law: (i) using the channels made available by competent EU institutions or bodies or reporting channels made available by applicable external authorities as defined within local jurisdiction; (ii) presenting a complaint to judicial or accounting authorities; (iii) making a public disclosure of information on the breach through the press or electronic media or otherwise by making a dissemination capable of reach a large number of people.

In particular:

- Reporting to competent EU institutions or bodies, or competent applicable authorities within local jurisdiction is possible where:
    - the entity has not an obligation to activate the internal reporting channel or this, even if mandatory, is not active or, even if activated, does not comply with the Decree's requirements.
    - the Whistleblower has already made an internal report, but it has not been followed up.
    - the Whistleblower has reasonable grounds to believe that the report would not be effectively followed up or that he/she might risk retaliation.
    - the Whistleblower has reasonable grounds to believe that the violations may constitute an imminent or obvious danger to the public interest.

- Public disclosure is possible where:
    - the Whistleblower has already made an internal or external report, but it has not been followed up within the deadlines provided by the Decree concerning the measures envisaged or taken to follow up the reports (see below).
    - the Whistleblower has reasonable grounds to believe that the violations may constitute an imminent or obvious danger to the public interest.
    - the Whistleblower has reasonable grounds to believe that the external report may involve a risk of retaliation or may not be effectively followed up because of the specific circumstances of the specific case (such as those in which evidence may be concealed or destroyed or where there is a well-founded fear that the recipient of the report may be in collusion with the author of the violations or involved in the violation itself).

○ Relevant external reporting lines in respect for the Countries provided in the **Annex**, if any.

3.5 Usage of the Ethics Hotline

The Ethics Hotline can be accessed to report cases including but not limited to:

- breaches of the law.
- breaches of the Global Code of Conduct and related Policies.
- defective management.
- abusive use of the position.
- circumstances generating significant hazards to public health or safety.
- any other activity affecting the Company's operations.

To report other facts or actions (e.g. in the field of labour relationships, working conditions, health and safety at work), the Human Resources Department shall be notified.

The Ethics Hotline is not an Emergency Service; therefore, this reporting channel should not be used to report events representing an immediate threat to life (e.g. fire, work accident) or to private property (e.g. theft). The complaints filed through the Ethics hotline may not receive an immediate response. If emergency assistance is required, the local authorities and Company representatives must be contacted.

Likewise, the channels dedicated to Whistleblowers are not intended for complaints regarding the Company's products or services.

3.6 Content of the reports

It is recommended that the reports made through the Ethics Hotline platform include the following information:

- ✓ The surname and first name(s) of the Whistleblower.
- ✓ Contact information details.
- ✓ The professional context in which the information was obtained (the Whistleblower's relationship with the Company).
- ✓ The individuals involved, if known.
- ✓ The individuals who are aware of or were witnesses to the reported case.
- ✓ A complete description of the case (details, how the Whistleblower became aware of the malpractice or potential malpractice, duration).
- ✓ The evidence supporting the report.

3.7 Anonymous reporting

For the investigation process to be conducted by the Company, it is helpful to provide a name and/or contact information to allow for follow-up in case the investigation team has additional questions. If the reporter still prefers to remain anonymous, the Whistleblower's report will still be investigated fairly and appropriately by the Company according to the provisions of the Global Code of Conduct and related policies, provided it contains substantial indications of legal breaches.

Thus, when accessing the Ethics Hotline the Whistleblower has the right to:

- request that the report made remain anonymous.
- disclose their name and contact information to the external service provider, allowing this information to be sent to the Company. This enables the Company to contact them for any necessary information to carry out the investigation.
- request that their name and contact information be provided only to the external service provider, but not to the Company. In this case, the Company can request additional information from the partner when needed, while maintaining the Whistleblower's anonymity from the Company.

3.8 Follow-up on Reports

Once a report is received by the Company, it must be checked immediately, and the Compliance Officer shall carry out a preliminary review. The acknowledgment receipt of the report will be provided to the Whistleblower within 7 calendar days.

The investigations shall be carried out in compliance with the general principles of investigations and sanctions, as regulated in the "Global Code of Conduct Operations Policy".

If the report does not include enough information to allow for an investigation to be carried out, the Whistleblower shall be asked to complete the report, providing further information details, within 15 days.

The Whistleblower will be notified about the status of their report, and feedback should be provided within a maximum of feedback provision period 3 months from the date of confirmation of receipt. If appropriate, updates may be given subsequently, whenever developments related to subsequent actions, except when such information could jeopardise performance of the investigation.

By accessing the webpage www.ethicsline.net, the Whistleblower has the option to connect to a case tracking portal where they can view the questions asked, answers received, any comments or questions sent by the Company.

When using the phone line, the external service provider will relay all questions from the Company and any subsequent questions from the Whistleblower.

3.9 Closing the internal reports

The Company closes a report without an investigation when:

a) the report does not include the elements provided by section 3.4. of this Policy, other than the Whistleblower's identification information, and the Compliance Officer requested its completion within 15 days, and this obligation has not been fulfilled.

b) the report is filed anonymously and does not include sufficient information regarding breaches of the law, which would allow the review and settlement of the report, and the appointed person requested its completion within 15 days, and this obligation has not been fulfilled.

If an individual files several reports to the Company with the same subject-matter, the cases shall be merged into one. If a new report on the same subject is received without additional information that would justify a different subsequent action, the report will be closed by the Company.

3.10 Personal data processing

The Ethics Hotline reporting mechanism meets all the security requirements and is maintained, from a technical point of view, by an independent operator. For security reasons, before filing out the report through the webpage, the Whistleblower is asked to provide a password, which cannot be recovered or reset.

We shall process the personal data being required for settling, documenting, and archiving the report received, in compliance with the confidentiality requirements.

The reports are stored for 5 years. After the archiving period expires, we shall irrevocably delete/anonymize your data. For general information and for more details on the personal data processing and specific rights in this context, we provide, maintain and update information in the Personal Data Protection Section, available here https://www.bekocorporate.com/media/ca5abf00/global-personal-data-privacy-policy.pdf].

4. PROTECTION OF THE WHISTLEBLOWER

4.1. Right to confidentiality

We take the appropriate measures to carefully use the information received and to protect the interests of all individuals involved. The data provided is processed in compliance with the requirements on personal data processing.

The Compliance Officer may not reveal the Whistleblower's identity or the information that could lead to their direct or indirect identification, except in the following circumstances:

- The Whistleblower agrees to reveal their identity.
- Their identification is essential in order to allow the legal public authorities to carry out the investigation or to effectively investigate the case.
- The Whistleblower intentionally or voluntarily disclosed their identity in the context of a public disclosure.

If the law requires the disclosure of the Whistleblower's identity, and it is in accordance with the legal conditions and limitations, the Whistleblower will be notified in writing about the disclosure of their identity, including the reasons for it. However, this notification obligation does not apply if such disclosure would jeopardise the investigation or legal proceedings.

Information contained in the reports that represent trade secrets may only be used or disclosed for purposes directly related to resolving the report. Any other use or disclosure is strictly prohibited. The obligation to maintain confidentiality is also observed if the report reaches other individuals within the Company than the Compliance Officer, from an error. The one who gets the notification shall immediately forward the case to the Compliance Officer.

4.2. Zero tolerance for retaliation

The Company does not tolerate retaliation under any form against anyone who files a report in good faith regarding breaches or potential breaches of the Global Code of Conduct, Compliance Policies, or the law, including when the investigation conducted by the Company does not confirm or substantiate the allegations initially made.

There shall always be zero tolerance for the actions or deeds aiming to disadvantage them by means of any actions/omissions related to the reported deed, threats of reprisals or attempted retaliation, especially those regarding:

a) any suspension of the individual employment contract.
b) dismissal.
c) amendment of the employment contract.
d) wage reduction or change of the working hours.
e) demotion or preventing promotion and professional development, including by means of negative evaluations of the individual professional performance or by means of negative recommendations for the professional activity carried out.
f) application of any other disciplinary measures.
g) coercion, intimidation, harassment.
h) discrimination, creating any another disadvantage or subjecting to unfair treatment.
i) refusal to convert a fixed-term employment contract into an indefinite-term employment contract, if the employee had legitimate expectations that they would be offered a permanent position.
j) the refusal to renew a fixed-term employment contract or the early termination of such a contract.
k) causing damages, including to the reputation of the relevant individual, especially on social media platforms, or financial losses, including as loss of business opportunities and loss of income.
l) the inclusion on a denylist or in a restricted database, on the basis of a formal or informal sectoral or industry-level agreement, which may imply that the relevant individual shall not find a job in the future the relevant sector or in the relevant industry.
m) the unilateral extrajudicial termination of an agreement for goods or services, and the requirements for this purpose are not met.

n) the cancellation of a granted licence or a permit.
o) the request for a psychiatric or medical evaluation.

4.3. Requirements set out by the law for benefiting from protection for internal reporting

To benefit from the protection measures, the Whistleblower must meet all the following requirements:

- to be one of the individuals filing reports according to the "Whistleblower definition" of this Policy.
- to have obtained information regarding law infringements within a professional context.
- to report in good faith: to have had reasonable reasons to believe that the information related to the reported breaches was true at the time of filing the report.
- to have filed an internal report, an external report or made a public disclosure.

If, for any reason, the reporter does not wish to use the Company's internal reporting channels as laid out in section 3.3, they can rely on their local external reporting channels where applicable.

The Whistleblower who publicly discloses information regarding the breach of the law (to the media, professional organisations, trade unions or employer organisations, non-governmental organisations, parliamentary committees or by making available in any way to the public the information related to breaches of the law) benefits from protection if one of the following requirements is met:

a) they first filed the report internally and externally, but deem that appropriate measures were not ordered within a period not exceeding 3 months or, in justified cases, 6 months from the receipt of the report.

b) they have good reasons to consider that:
   - the breach may represent an imminent or clear hazard to the public interest or the risk of irreparable damage; or
   - in the case of external reporting, there is a risk of reprisals or a small probability that the breach shall be effectively remedied considering the specific circumstances of the report.

4.4. Other categories of individuals who benefits from protection in internal or external reporting

- Whistleblowers who file reports with the competent institutions, bodies, offices, or agencies of the European Union.
- Facilitators – natural persons who assist the Whistleblower during the reporting process in a professional context and whose assistance must be confidential.

- Third parties who have connections with the Whistleblower and who could suffer reprisals in a professional context, such as their co-workers or relatives.
- Legal entities owned by the Whistleblower or for whom the Whistleblower works or with whom they have other types of connections in a professional context.
- The Whistleblower who has anonymously reported or publicly disclosed information related to breaches, but who is later identified and suffers reprisals.

5. AUTHORITY AND RESPONSIBILITIES

This Policy is drafted by the Legal and Compliance Department and will be periodically reviewed.

Any violation of this Policy will result in disciplinary action, up to and including termination of employment.

Version 1.1 date: 05/05/2025
Version 1.0 date: 21/11/2024

ANNEX – Differences in Local Legislation

Country	Local Legal basis Direct Local e mail addresses	External Reporting Line in addition to internal lines
Romania	LEGE nr. 361 din 16 decembrie 2022 privind protecția avertizorilor în interes public Law number 361/2022 regarding the protection of the whistleblowers Direct Local e-mail address compliance.ro@beko.com	The National Agency of Integrity (NAI), and other authorities and institutions to which NAI sends the claims for competent resolution are the designated authorities to receive external reporting.
Poland	Polish Whistleblower Protection Act. Direct Local e-mail address compliance.poland@beko.com	External reporting can be made to the Ombudsman (Rzecznik Praw Obywatelskich), responsible for handling whistleblowing complaints starting December 25, 2024.
Germany	German Whisteblower Act (Hinweisgeberschutzgesetz-HinSchG)	Several external reporting offices: Federal Office of Justice (at the federal level), state-level offices, a specialized office at the Federal Financial Supervisory Authority, and the Federal Cartel Office for EU competition law violations.
Austria	Austrian Whistleblower Act (HinweisgeberInnenschutzgesetz - HSchG)	The Federal Bureau of Anti-Corruption (Bundesamt für Korruptionsprävention und Korruptionsbekämpfung - BAK) will receive reports as an external body for the private and public sector.
Netherlands	Dutch Whistleblower Act (Wet bescherming klokkenluiders)	Dutch Whistleblowers Authority has been selected to be the authority with responsibility for oversight over the functioning of the external reporting.

Belgium	Belgium Whistleblower Act- private sector (NL: Wet betreffende de bescherming van melders van inbreuken op het Unie- of nationale recht vastgesteld binnen een juridische entiteit in de private sector/ FR: Loi sur la protection des personnes qui signalent des violations au droit de l'Union ou au droit national constatées au sein d'une entité juridique du secteur privé)	The GBA (Gegevensbeschermingsautoriteit) is the designated authority to receive notifications under the Act of 28 November 2022, which protects whistleblowers reporting breaches of Union or national law in the private sector.
Sweden	Swedish Whistleblowing Act (Sw. Lag (2021:890) om skydd för personer som rapporterar om missförhållanden)	The Swedish Work Environment Authority has been selected to be the authority with responsibility for oversight over the functioning of the external reporting.
Denmark	Danish Whistleblower Act (Lov om beskyttelse af whistleblowers)	The Danish Data Protection Agency (Datatilsynet) has been designated as the external reporting channel.
Finland	Finnish Whistleblower Act (Laki 1171/2022 Euroopan unionin ja kansallisen oikeuden rikkomisesta ilmoittavien henkilöiden suojelusta (Ilmoittajansuojelulaki)	The Office of the Chancellor of Justice acts as a centralised external reporting channel for whistleblower protection.
Italy	Legislative Decree n. 24/2023 Direct Local e-mail address compliance.italy@beko.com	The National Anti-Corruption Authority (ANAC) is designated as the competent external authority for whistleblowing reports
Luxembourg	Luxembourg Whistleblower Act (Loi du 16 mai 2023)	External reporting channels are listed in Article 18 of the Act. These include authorities designated for handling breaches in various sectors

France	French Decree No. 2022-1284, which implements French Law No. 2022-401, on whistleblower protections ("Waserman Law") Law No. 2016-1691 on Transparency, Fighting Corruption, and Modernizing Economic Life ("Sapin II") Direct Local e-mail address compliance.fr@beko.com	External reports can be made to the competent authority as listed in Decree 2022-1284, to the Rights Defender, the judicial authority, or to EU institutions responsible for handling breaches. French anticorruption agency (AFA): https://www.agence-francaise-anticorruption.gouv.fr/
Serbia	Law on protection of Whistleblowers (Zakon o zaštiti uzbunjivača) Direct Local e-mail address compliance.balkans@beko.com ** The employer is obligated, upon the whistleblower's request, to provide the whistleblower with information about the progress and actions taken.	Government body, local authority, or public power holder responsible under the law can be external authority.
United Kingdom	Public Interest Disclosure Act 1998 (PIDA)	-
Spain	Law 2/2023 on the protection of persons who report regulatory offences and the fight against corruption of 21 February 2023 *(Ley 2/2023, de 20 de febrero, reguladora de la protección de las personas que informen sobre infracciones normativas y de lucha contra la corrupción*). Pursuant to article 8 of the Law, Company governing body holds the authority to appoint the Person Responsible for the	Autoridad Independiente de Protección del Informante, A.A.I - Oficina Antifraude de Cataluña

	Internal Information System (*Responsable del Sistema interno de información*). Direct local e-mail address: compliance.iberia@beko.com	
Portugal	Law 93/2021 - Establishing the general regime for the protection of whistleblowers reporting violations (*Lei n.º 93/2021. Estabelece o regime geral de proteção de denunciantes de infrações*) Direct local e-mail address: compliance.iberia@beko.com	Pursuant to Art. 12 of Lei 93/2021, External reports are submitted to the authorities that, according to their duties and competencies, should or may have knowledge of the subject matter of the report, including: a) The Public Prosecutor's Office; b) Criminal police authorities; c) The Bank of Portugal; d) Independent administrative authorities; e) Public institutes; f) Inspectorates-general and equivalent entities, and other central services of the direct State administration with administrative autonomy; g) Local authorities; and h) Public associations.