Privacy Notice for the use of the Website and the Processing of Candidates' Personal Data

Welcome! We are delighted that you may be interested in exploring a job opportunity with Beko. We are committed to protecting the privacy and security of your personal information during the Job Application process.

1. Scope and data controller

This Privacy Notice explains how personal information is collected and processed when you use the careers website at http://www.koccareers.com/beko to create a candidate profile, submit an application or CV, attend interviews or assessments, or otherwise engage with us in relation to a potential role.

Where this notice applies to applicants for roles in South Africa or to applicants whose personal information is processed in South Africa, references in this notice to "personal data", "controller" and "processor" are to be read as "personal information", "responsible party" and "operator" respectively, where the context requires.

For South African recruitment activity, Defy Appliances (Pty) Ltd (2007/006715/07 and address is 135 Teakwood Road, Jacobs, Durban 4052) is the responsible party for the local recruitment process to which your application relates. Relevant Beko / Arçelik group entities and service providers may also process personal information on a shared platform basis or on behalf of the relevant responsible party for recruitment administration, platform support, talent acquisition support, reporting, compliance and related services.

Where more than one group entity is involved in a recruitment process, each entity will access and use personal information only on a need-to-know basis for the recruitment purpose for which it was made available. Any internal allocation of responsibilities between entities does not limit your right to direct any privacy-related query or request to the contact details set out below.

Any application, interview or recruitment interaction does not of itself create an employment relationship or oblige us to make an offer. If an offer is made, it will remain subject to the applicable employment terms, pre-employment requirements and any lawful conditions relevant to the role.

2. Data protection principles

We will comply with Data Protection Laws, which state that the Personal Data we hold about you must be:

- used lawfully, fairly and in a transparent way
- collected only for valid purposes that the company has clearly explained to you and not used in any way that is incompatible with those purposes
- relevant to the purposes the company has told you about and limited only to those purposes
- accurate and kept up to date
- kept only as long as necessary for the purposes the company has told you about
- kept securely.

Sensitivity: Public

3. The types of Personal Data we hold about you

We will collect, store, and use the following categories of personal data ("Personal Data"):

1. Log information, cookies, web beacons and similar technologies: We may process Personal Information from you when you interact with the Website. For example, we or our service provider(s) may also use cookies, web beacons or log files. Data we collect automatically includes the type of web browser or mobile device, your operating system, your IP address, the URL of the landing page and the referring website, the time and date of your visit to the Site, and the search terms used by you to reach the website. More information regarding our use of cookies and other tracking technologies, as well as how you can manage these, can be found in the Cookie Notice available on the relevant website;
2. Your CV, including information we extract from your CV;
3. Your application for a job with us and other information you submit in relation to your application, as well as the information you have provided in your application and covering letter including: Basic identification information (such as full name, date of birth, nationality); Contact information (such as home address, telephone number, email address); Information relating to your education, qualifications, certifications relating to your employment, as well as your employment performance (such as curriculum vitae details, letters of recommendation, job description, qualifications and areas of expertise, work history, other performance measures and, where appropriate, training records, records of technical skills tests, participation in professional or academic organisations, seminar's attendance lists, learning history and certificates of completion of e-learning courses);
4. Any information you provide to us on a voluntary basis (such as a photograph or recording the online recruitment process, when you provide access to your camera and microphone on specific recruiting or assessments platforms or surveys results to gather feedback about your candidate experience);
5. Any other information (including any survey or test results) you provide during the application, recruiting, interview, or hiring stages, as part of the pre-onboarding stage.

If you applied via an online registration form (e.g. SuccessFactors tool), you will see which data is mandatory and which is optional. You will be able to access your own profile data and edit as needed, as well as to delete your own data in My profile/My candidate profile/ Delete Profile/ Delete all data.

4. Special categories of Personal Data about you

We may collect limited special personal information only where this is lawful, strictly necessary and proportionate for the role or the recruitment process. This may include information relating to health or disability to the extent necessary to consider or provide reasonable accommodation, information relating to religious observance where relevant to accommodation, criminal record information where a lawful role-specific check is required, and audio, image or video information where a particular assessment requires it and the applicable lawful basis exists. Applicants should not provide special personal information unless it is requested or unless it is necessary for accommodation or compliance purposes.

Sensitivity: Public

5. How is your Personal Data collected?

We collect personal information directly from you when you use the careers website, create a profile, submit an application, upload documents, complete forms, attend interviews or assessments, or otherwise engage with us in the recruitment process.

We may also collect personal information from recruitment agencies, referees you nominate, assessment or background screening providers acting on our behalf, publicly available professional sources relevant to your application, and internal group systems where you have previously interacted with us through a prior application or candidate profile.

When you use the careers website, certain technical information may be collected through cookies and similar technologies. Further details are set out in the Cookie Notice for the relevant careers portal.

We do not collect personal information for recruitment purposes from general market research sources.

If you provide us with another person's personal information, such as referee details, you should ensure that you are authorised to do so and that the person is aware that we may contact them in connection with your application.

6. Purposes and Legal Basis for Processing Personal Data

We use personal information for the following recruitment-related purposes:

(a) to operate the careers website and recruitment platform, maintain security, support site functionality and improve the user experience;

(b) to create and manage your candidate profile, receive and assess your application, communicate with you, arrange interviews or assessments, verify information where necessary and lawful, and decide whether to progress your application;

(c) where you choose that option, to keep your profile visible for other current or future vacancies for the period stated in this notice; and

(d) to carry out related recruitment, hiring, compliance and business protection activities, including immigration or permit support where relevant, lawful background verification, fraud prevention, record keeping, legal and regulatory compliance, and the establishment, exercise or defence of legal rights.

For South African applicants, the provision of personal information marked as mandatory, or otherwise reasonably required for the recruitment process, is voluntary in the sense that you may choose not to provide it, but if you do not provide it we may be unable to consider or progress your application, verify your suitability, comply with applicable legal requirements or make an offer.

Where the applicable law requires the basis for processing to be identified, the processing described above is carried out because it is reasonably necessary to consider and manage your application, to take steps at your request in relation to a possible employment relationship, to comply with legal obligations, to protect your or our legitimate interests where applicable, and, where required, with your consent .

Sensitivity: Public

The above purposes will be implemented, among others, within the framework of the following principles:

Surveys

As part of the recruitment process, we may use Qualtrics or a similar survey tool to gather feedback about the recruitment experience.

Participation is voluntary. Survey responses must not be used to make recruitment decisions. Where personal information is processed through the survey tool, it will be used only to understand and improve the recruitment experience, and access will be limited to authorised personnel.

Assessment of English Proficiency

Where English language proficiency is a requirement for a role, we may use ITEP or an equivalent assessment provider to assess the language skills relevant to the position. The information processed for that purpose may include registration details, contact information, assessment responses, assessment results, and technical information generated by the platform.

If microphone, camera, image or voice access is required for exam integrity or assessment purposes, that functionality must be clearly disclosed at the point of collection and must be limited to what is necessary and lawful for the assessment.

Assessment results and related records may be accessed on a need-to-know basis by authorised recruitment personnel involved in the relevant application.

Assessment of competencies, cognitive abilities and motivations

We may use Korn Ferry or an equivalent assessment provider to support the structured assessment of competencies, traits, drivers, cognitive ability or other role-related criteria. Assessment outputs are used as one input in the recruitment process and are reviewed together with interviews, qualifications, experience and other relevant information. They are not used in isolation to determine whether a candidate will proceed in the process.

The provider acts on our instructions in relation to platform hosting and support, and authorised recruitment personnel may access the results on a need-to-know basis for the relevant recruitment process.

7. Automated decision-making

We may use technology-enabled assessment tools to support the recruitment process. No candidate is appointed, rejected or otherwise subjected to a decision based solely on automated processing. All material recruitment decisions are taken with human involvement.

8. Who will have access to your data?

Depending on the Job Application Process you choose, we will access your Personal Data on a need-to-know basis. If you applied through an online registration form (e.g., the SuccessFactors tool), the following persons will actively participate in the recruitment process (e.g. by viewing your data):

Sensitivity: Public

1. If you select the option “Make my profile visible to only recruiters managing jobs I apply to”, the local HR team of the company you are applying for and manager/s responsible for the position you are applying for will have access to your data.

2. If you select the option " Make my profile visible to all group companies in my country of residence", the local HR teams of all group companies in your country and the managers responsible for the open positions in those entities, will have access to your data.

3. If you select the option "Make my profile visible to all group companies worldwide", the local HR teams of all group companies worldwide and the managers responsible for the open positions in those entities, will have access to your data.

In addition to that, the following teams may have access to your data:

a) Relevant Talent Acquisition HR team of Arçelik A.Ş. (regardless of the active role in the selection of the candidate in accordance with points 2-3) may have access (in all cases stated above – point 1-3) to support the recruitment process, including supervising compliance with legal requirements and internal organizational and reporting rules;
b) Relevant HR teams and hiring managers of Arçelik A.Ş., when their intervention is required in the recruitment process;
c) Employees (e.g. IT) of Koç Holding A.Ş. and Arçelik A.Ş.: IT support and IT team managing account of the recruitment tool / platform (potential access to all recruitment process);
d) Relevant Legal and Compliance teams of Koç Holding A.Ş., Arçelik A.Ş. and Beko Europe: in exceptional cases, e.g., the need to verify the recruitment in terms of compliance with the law.

9. Why might we share your Personal Data with third parties?

We may share personal information on a need-to-know basis with the relevant recruiting entity, group HR teams, hiring managers, referees you identify, IT and platform support providers, assessment providers, recruitment agencies, background screening providers where lawful, professional advisers, and public authorities where disclosure is required or permitted by law.

Where personal information is shared with service providers or other operators, they may process it only for the purposes for which it was provided and subject to appropriate confidentiality, security and data handling obligations.

10. Joint controllership details

Where more than one group entity participates in a recruitment process, the relevant entities allocate their privacy responsibilities internally. This internal allocation does not affect your right to direct any request or query to the contact details in this notice, and the relevant entity will coordinate the response with the other participating entity or service provider as required.

Sensitivity: Public

11. Cross-border processing

Your personal information may be stored in or accessed from countries outside South Africa where group entities or service providers supporting the recruitment platform, recruitment administration or related services are located.

Where personal information is transferred outside South Africa, this will be done only where an adequate level of protection or another lawful basis exists, and appropriate safeguards will be implemented where required.

If you would like more information about cross-border processing or the safeguards used, please contact us using the details set out below.

12. Keeping your Personal Data secure

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 of a suspected data security breach whenever we are legally required to do so.

13. How long we keep your personal information

We retain applicant personal information only for as long as reasonably necessary for the recruitment process, any agreed talent pooling or future opportunities period, compliance with legal obligations, internal governance, record keeping and the establishment, exercise or defence of legal rights.

Unsuccessful applicant data should not be retained beyond 6 months unless there is a lawful reason for doing so and the applicant has been told about that retention. Successful applicant data will form part of the relevant employee record and will thereafter be retained in accordance with the applicable employee privacy notice and record retention requirements.

14. Your rights in connection with your Personal Data

If you have any questions about how we use your Personal Data or this privacy notice in general, please contact us using this form.

For South African applicants, you may request details of the personal information held about you, request correction or deletion where appropriate, object to certain processing, withdraw consent where processing is based on consent, and lodge a complaint with the Information Regulator. If your application involves another group entity, the relevant entity will coordinate any response with that entity as required.

Complaints may be directed to the Information Regulator, South Africa.

Sensitivity: Public

Information Officer: Marsha Govender
Marsha.govender@defy.co.za
031 460 9711
PO Box 12004, Jacobs, Durban 4026

Links to third-party sites may appear on the career's website. Those sites operate under their own privacy and cookie practices, and you should review their notices before providing personal information to them.

When you use the careers website, cookies and similar technologies may be used as described in the Cookie Notice for the relevant portal. You can manage your preferences through the cookie settings tool and, to a limited extent, through your browser settings

15. Third-party websites and content

Links to third-party sites may appear on the career's website. Those sites operate under their own privacy and cookie practices, and you should review their notices before providing personal information to them.

When you use the careers website, cookies and similar technologies may be used as described in the Cookie Notice for the relevant portal. You can manage your preferences through the cookie settings tool and, to a limited extent, through your browser settings.

16. 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.

Should you wish to file a complaint, you may also reach out to the appropriate data protection authority as outlined in the 'Supervisory Authorities' section below.

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 company within the Group, write to us and we will send you the contact details of that company.

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@beko.com

17. 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.

Sensitivity: Public

Generally speaking, the main contact point for questions on data protection is the Supervisory Authority in the country where company/organization in question is based. However, if that company/organization 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.

Contact details of ICO (Information Commissioner's Office): available clicking here.

Contact details of Federal Data Protection and Information Commissioner (Switzerland Supervisory Authority), available clicking here.

18. Changes to this Privacy Notice

We keep this Privacy Notice under regular review. We may update this Privacy Notice from time to time to reflect changes to our privacy practices. Any changes to our privacy notice will be posted in the tool. We encourage you to periodically review our Privacy Notice for the latest information on our privacy practices.

This Privacy Notice was last updated on **21.07.2026.**

Sensitivity: Public