

## **Recruitment - Personal Data Collection & Usage Notice**

Hewlett Packard Enterprise Company and its subsidiaries (“HPE” or “We”) collect and process personal information about you in connection with the recruitment process at HPE, from a job application through to a job offer. This notice provides you with detailed information on our use of your personal data for this purpose.

### **How We Use Your Personal Data**

We collect and process the following types of personal data, together with any additional information you may provide to us:

- **Personal Information** – such as name, address, telephone numbers and email address, country of residence, citizenship, gender, ethnicity in countries where the collection and processing of ethnicity data is permissible or required by law, and conflicts of interest with HPE.
- **Hiring Related Information** – such as CV, education, former employment and career history and academic qualification certificates and professional affiliations.
- **Job Related Information** – such as employment status, entitlement to work, work or residency permits and visas.

We also obtain data about you from other sources, such as recruiters including Korn Ferry International (our global recruitment services provider), identity verification providers, and publicly available information accessible via the Internet and third-party websites, including LinkedIn.

HPE may use your personal data for one or more of the following purposes:

- (i) To enable you to create a candidate profile (“**your Profile**”) in our resume database;
- (ii) To administer your job application with HPE, including the assessment, screening, and interview process and any subsequent job offer and subsequent pre-boarding and on-boarding activities;
- (iii) To assess you against established criteria and other candidates;
- (iv) To obtain references;
- (v) To conduct profiling for compliance with global trade laws (Global Profiler Questionnaire)
- (vi) To conduct background screening;
- (vii) To match your skills and qualifications against future job openings at HPE that may be of interest to you;
- (viii) To support the analysis and internal reporting of our diversity and inclusion initiatives in relation to recruitment, for example, assessing application and hiring statistics and trends; and
- (ix) For reporting purposes where required by law.

HPE’s legal basis for processing your personal data is that the processing is necessary for HPE’s legitimate interests in hiring new employees, maintaining an appropriately skilled and diverse workforce to support our business and compliance with law, in the case of global trade compliance and reporting. We will provide you with additional information about background screening and obtain your consent to conduct background screening where required by law. If you have consented

to background checks and/or where permitted by law, we also collect details of professional registrations, sanctions with professional bodies, financial checks or criminal convictions.

### **How We Share Personal Data**

We share or disclose your personal data within the HPE group of companies where necessary for the purposes outlined above. We may share your personal data outside the HPE group of companies to:

**Government authorities and/or law enforcement officials** if required by law or if required to protect HPE's legitimate interests provided we are able to do that by law.

**Service Providers.** HPE retains service providers, including Korn Ferry International (our global recruitment services provider), to assist with the recruitment process in many geographies or to provide IT related services and they may be given access to your personal data to provide these services. All HPE suppliers and partners are required to enter into contracts with HPE that include privacy and security terms to ensure the appropriate use and protection of personal data.

**Other companies and their professional advisors.** In the event we consider or decide to sell, buy, merge, reorganise or outsource all or part of the business, we may need to disclose certain information about you to these companies to facilitate or effect the transaction. We seek appropriate contractual protections from the prospective buyers or sellers in these situations and may also seek your consent where required by local law.

### **How We Transfer Personal Data Internationally**

**Transfers within HPE group of companies.** Your personal data will be transferred to our US based systems and may be transferred internationally to other members of the HPE group as necessary to manage the recruitment process. The privacy laws in some countries, notably the EU, EEA Switzerland and the UK regulate the transfer of personal data to other countries to ensure the data is protected in the recipient country.

HPE has an intra-company agreement on the transfer and processing of personal data within the HPE group of companies. This agreement also forms the basis of HPE's Binding Corporate Rules for Controller (**BCR-C**) which have been approved by the majority of the Data Protection Regulators in the European Economic Area (EEA), Switzerland and the UK. The BCR-C allow HPE to ensure that EEA, Swiss and UK personal data which is transferred and processed by HPE companies outside the EEA, Switzerland or UK, is adequately protected in accordance with applicable data protection laws. If you would like to learn more about our BCRs, please click [here](#).

**Transfers to Suppliers** - In the case of transfers of your personal data to suppliers located in countries that do not provide an adequate level of data protection under local law, HPE will take appropriate safeguards such as EU Standard Contractual Clauses or other model clauses approved by the relevant data protection authority, approved codes of conduct or certification mechanisms or other binding and enforceable commitments of the supplier. A copy of the relevant mechanism can be provided to you on request by contacting us through our [web form](#).

### **How Long We Keep Personal Data**

HPE collects the minimum amount of data required for the purposes outlined in this notice. HPE retains your personal data for as long as is reasonably necessary for the purposes outlined above. The

retention of personal data is governed and managed in accordance with HPE's Global Master Records and Information Management Policy and any supplementary data governance procedures.

If there has been no activity in relation to your Profile within one year of your most recent application, it will be deleted from our resume database unless HPE is required to keep the data for longer to comply with legal or regulatory obligations. Please note that if you have applied for a US position and if global trade compliance restriction apply, your information will be retained for a period of time in an "inactive" status as required by US or global trade law.

#### **How to Update, Amend or Delete your Profile.**

Once you have submitted your application, you are unable to make changes to it without the help of a recruiter or recruiting operations. If you would like to make amendments or delete your Profile and application(s) from our resume database, please send an email through our [web form](#) with details of the application and your contact details. We will confirm directly with you when your details are removed and contact you if we have any questions prior to removal of your personal data. This applies to candidates and applicants in all geographies.

This will withdraw your applications from all the job positions you applied to, and will remove your Profile and all associated information from the database in compliance with local records retention laws. If you have applied to a US position and if Global Trade compliance restrictions are applicable, your candidate information will be retained for a period of time in an "inactive" status as required by applicable law.

#### **Additional Information for Individuals in the EU, EEA, Switzerland, UK, Turkey and Brazil.**

Our privacy practices are aligned with the requirements of the General Data Protection Regulation (GDPR) and other applicable data protection laws. If you are located in the European Union (EU), the European Economic Area (EEA), Switzerland, UK, Turkey or Brazil, this additional information may be relevant and applicable to you.

**Data controllers.** Companies from the HPE group of companies may act as data controllers in relation to your personal data for the processing of personal data described in this privacy notice. You can find the up-to-date list of the HPE group of companies by clicking [here](#). If you would like to receive more information about which HPE entity acts as data controller for your personal data, please contact the HPE Privacy Office by sending an email through our [web form](#).

**Data Protection Officer.** HPE has appointed a Data Protection Officer (DPO) to comply with the GDPR and other relevant data protection laws. You can contact the DPO by sending an email through the web form on our website at <https://www.hpe.com/us/en/privacy/feedback-forms.html> or in writing to:

Hewlett Packard Enterprise  
Office of Legal & Administrative Affairs – ATTENTION PRIVACY OFFICE  
Bracknell/Amen Corner B1-2, UK  
Cain Rd. Amen Corner (Bldg. BRA02)  
Bracknell, RG12 1HN  
United Kingdom

## **Your Rights in Relation to Your Personal Data.**

You may have the following rights to:

- Request confirmation of the existence of processing, or access or copies of personal data HPE processes about you;
- Rectify your personal data, if inaccurate, outdated or incomplete;
- Delete or anonymize your personal data, unless an exception applies. For instance, we may need to keep your personal data to comply with legal obligations;
- Restrict the processing of your personal data, in certain circumstances. For instance, if you contest accuracy of your personal data you may request that we restrict processing of your personal data for the time enabling us to verify the accuracy of your personal data;
- Data portability, in certain circumstances. For instance, you may request us to transmit some of your personal data to another organization if the processing is based on your consent or a contract;
- Object to the processing of your personal data, in certain circumstances. For instance, you may object where we process your personal data because we have legitimate interest in doing so;
- Obtain information about the entities with which HPE has shared your personal data;
- Withdraw consent to the processing of your personal data.

These rights may be limited in some situations such as where HPE can demonstrate that HPE has a legal requirement or legitimate interest to process your personal data.

For more details on these rights and to exercise your rights please contact the HPE Privacy Office by sending an email through the [web form](#).

**Complaint with a supervisory authority.** If you consider that the processing of your personal data infringes the GDPR, you have a right to lodge a complaint with a supervisory authority in the country where you live, or work, or where you consider that data protection rules have been breached.

**Your rights under HPE Binding Corporate Rules.** You may have additional rights under our BCRs. For instance, as a third party beneficiary, where you believe your personal data has been transferred to an HPE company located outside the EU or the UK and processed by that company in breach of the BCR, you may have a right to:

- Lodge a complaint with the EU or UK HPE company which transferred your personal data outside the EU;
- Lodge a complaint with a supervisory authority located in the same country as the EU or UK HPE company which transferred your data outside the EU or the UK;
- Bring a court action against the EU or UK HPE company which transferred your personal data outside the EU.

For further information, please visit the HPE BCR web page available [here](#).

## **How To Contact Us.**

If you have any questions about this notice or the processing of your personal data, please contact HPE's Privacy Office by sending an email through our [web form](#). If you have unresolved concerns, you also have the right to complain to data protection authorities in the country where you live or where you consider that data protection rules have been breached.