Privacy Notice – Employee Integrity Checks

1. Introduction

This Privacy Notice is intended to describe the practices EY follows in relation to the Employee Integrity Checks ("System") with respect to the privacy of all individuals whose personal data is processed and stored in the system.

2. Who manages the System?

"EY" refers to one or more of the member firms of Ernst & Young LLP ("EY LLP"), each of which is a separate legal entity and can act as a data controller in its own right. The entity that is acting as data controller by providing this system on which your personal data will be processed and stored is Ernst & Young LLP.

The personal data you provide in the system is shared with Ernst & Young LLP (EY LLP), (see "Who can access your information" section below).

The system is hosted on servers that are located at 4th Floor, Tower 2B, India Glycols Commercial Complex, Sector 126, Noida, Uttar Pradesh 201304, India

3. Why do we need your information?

The purpose of the Employee Integrity Checks System is to collect and manage information and document as part of the background checks and verifications process, which shall include, but not limited to, verification of government issued ID proofs, permanent address, employment history, education qualifications, Police/Court record checks, reference checks, or other verifications, in order to avail employment, benefits and/or services.

The provision of your personal data to us is optional. However, if you do not provide all or part of your personal data, we may be unable to carry out the purposes for processing which are set out above.

4. What type of personal data is processed in the Service/System?

The service processes the following categories of personal data:

- Name (first name, last name)
- email address
- contact number
- Date of Birth
- Permanent residential address
- Government issued (PAN card, Driving licence, Voter id Card and Passport)
- Education Records
- Employment Records

This data is sourced from: Candidate Information Form template would be shared via email to an individual to fill their information required for conducting their Employee Integrity Check.

5. Sensitive Personal Data

Sensitive personal data reveals your racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, data concerning health or data concerning sex life or sexual orientation.

"EY LLP does not intentionally collect any sensitive personal data from you. The system's intention is not to process such information."

6. Who can access your information?

Your personal data is accessed in the system by the following persons/teams:

- Information accessible to all EIC team members (Approximately 20-25 team members) with defined access rights as per their role and responsibilities. They require this access to perform verification. EIC PII protocol document is in place to define the user specific access rights.

  o Full access role – This role involves full administrative access to the EIC system and its data, i.e. they can edit, replace and revoke, view in-process verification information and grant access to the EIC system. They are located in India and will be tasked with managing the system. Access is needed for the management of the system.

o Researcher/ verifier - Researcher/ verifier are able to access and only view the information but cannot edit verification templates. For this purpose, they have read-only access to all client information for EIC project. Researcher/ verifier will include EY counsellors (i.e. personal mentors who provide career development guidance, who may or may not be the relevant employee's direct supervisor)

o Report writer/ Quality - Report writer/ Quality will have the read-only access to the verification response. they will perform check level quality and compile all the verification reports in one report templet.

- The geographical scope of this system would be India

The access rights detailed above involves transferring personal data in various jurisdictions (including jurisdictions outside the European Union) in which EY operates (EY office locations are listed at www.ey.com/ourlocations). EY will process your personal data in the system in accordance with applicable law and professional regulations in your jurisdiction. Transfers of personal data within the EY network are governed by EY's Binding Corporate Rules (www.ey.com/bcr).

7. Data retention

The policies and/or procedures for the retention of personal data in the EIC system are:

Data retention period for EIC system is for one year after sharing the final report with the client, it may vary from client to client as per engagement signed with client.

Your personal data will be retained in compliance with applicable privacy laws and regulations.

After the end of the data retention period, your personal data will be deleted

8. Security

EY is committed to making sure your personal data is secure. To prevent unauthorized access or disclosure, EY has technical and organizational measures to safeguard and secure your personal data. All EY personnel and third parties EY engages to process your personal data are obliged to respect your data's confidentiality.

9. Controlling your personal data

EY will not transfer your personal data to third parties (other than any external parties referred to in section 6 above) unless we have your permission or are required by law to do so.

You are legally entitled to request details of EY's personal data about you.

To confirm whether your personal data is processed in the system or to access your personal data in the system, contact your usual EY representative or email your request to eic@in.ey.com or Global.data.protection@ey.com.

10. Rectification, erasure, restriction of processing or data portability

EY provides you with the ability to make sure your personal data is accurate and up to date. You can request rectification, erasure or restriction of processing of your personal data by sending an e-mail to eic@in.ey.com or global.data.protection@ey.com. We will use reasonable efforts to contact you regarding your request.

11. Complaints

If you are concerned about an alleged breach of privacy law or any other regulation by EY, you can contact EY's Global Privacy Officer, Office of the General Counsel, 6 More London Place, London, SE1 2DA, United Kingdom or via email at global.data.protection@ey.com. or ***eic@in.ey.com*** or via your usual EY representative. An EY Privacy officer will be made available to investigate your complaint and give you information about how it will be handled and resolved.

If you are not satisfied with how EY resolved your complaint, you have the right to complain to your country's data protection authority. You can also refer the matter to a court of competent jurisdiction.

12. Contact us

If you have questions or you do not feel that your concerns have been addressed in this Privacy Notice, please contact your usual EY representative, or you can reach us via global.data.protection@ey.com.

Consent: Yes ☒ No ☐ Name: Raghvender Bhati

Date: 24-08-2020 Signature: Raghvender