

# Keyfactor Privacy Notice

RECRUITMENT APPLICANTS

**KEYFACTOR**

---

## Table of Contents

1	Purpose .....	4
2	Personal Information .....	4
2.1	“Special Categories” .....	4
2.2	How is your Personal Information Collected? .....	5
2.3	How Will Keyfactor use your Information? .....	5
2.4	Failure to Provide Personal Information .....	6
2.5	How does KeyFactor use Sensitive Information? .....	6
2.6	Does KeyFactor Collect Criminal Convictions Information? .....	6
2.7	Application Security .....	6
2.8	Your Rights .....	6



# KEYFACTOR

## 1 Purpose

### What is the purpose of this document?

Keyfactor is committed to protecting the privacy and security of your personal information. This privacy notice is prepared in accordance with the EU General Data Protection regulation (GDPR) and the 'UK GDPR', or Data Protection Act 2018.

Keyfactor is a 'Data Controller', this means that we are responsible for deciding how we hold and use personal information about you. This privacy notice is relevant to you because you are applying for work with us (whether as an employee, worker, or contractor). It makes you aware of how and why your personal data will be used, namely for the purposes of recruitment and how long it will be retained for. This document also provides you with certain information that must be provided under the GDPR and the UK Data Protection Act 2018.

## 2 Personal Information

### What information do we hold about you?

In connection with your application, we will collect, store, and use the following categories of personal information about you:

- The information you have provided to us in your curriculum vitae and covering letter.
- The information you have provided on our application form, including full name, home address, telephone number, and personal email address, date of birth, gender, employment history, educational and vocational experience, and qualifications.
- Any information you provide to us during the application process or at an interview.
- Proficiency tests results and psychometric reports, as required.

### 2.1 "Special Categories"

**We may also collect, store, and use the following types of 'special category', sensitive personal information:**

- Information about your race or ethnicity, religious beliefs, sexual orientation, and political opinions as provided to us via the Equal Opportunities Form.
- Information about your health, including any medical condition, health, and sickness records (dependent on the role that you are applying for, you may also need to complete a full medical, drugs and alcohol test and/ or psychometric evaluation).
- Information about criminal convictions and offences.

# KEYFACTOR

- Any information you provide to us via the Equal Opportunities Form as part of the application process or otherwise.

## 2.2 How is your Personal Information Collected?

We collect personal information about candidates from any or all the following sources:

- You, the candidate
- Selected local and global recruitment agencies, from which we collect your CV and other information provided to the agency.
- Where required, certain background check providers, to satisfy conditions of working within a country, i.e. Right to Work checks in the UK.
- Criminal records background check provider in respect of criminal convictions
- Your named referees, from whom we collect the following categories of data – last 7 years of employment and certification/qualification checks.

## 2.3 How Will Keyfactor use your Information?

We will use the personal information we collect about you to:

- Assess your skills, qualifications, and suitability for the role (or roles, as the case may be).
- Carry out background, medical and reference checks, where applicable.
- Communicate with you about the recruitment process.
- Keep records related to our hiring processes.
- Comply with legal or regulatory requirements.
- Deciding to shortlist, interview, employ or appoint you.
- If you are shortlisted, we will decide whether to invite you for an interview. If we decide to invite you for an interview, we will use the information provided and any additional information you provide to us at the interview to decide whether to offer you the role. If we decide to offer you the role, we may then take up references and/ or carry out a criminal record and/ or carry out any other checks. Following the successful completion of this process, we will confirm your employment or appointment in writing.

It is in our legitimate interests to collect and process your personal information for the purposes set out above to decide whether to shortlist, interview, assess or employ or appoint you for the role (or roles) that you have applied for.

We also need to process your personal information to decide whether to enter a contract with you (such a contract or employment or a contract for services).

# KEYFACTOR

## 2.4 Failure to Provide Personal Information

If you fail to provide information, when requested, which is necessary for us to consider your application (such as evidence of qualifications or work history) this may delay or obstruct the processing of your application.

## 2.5 How does Keyfactor use Sensitive Information?

Keyfactor will use special category or sensitive personal data in the following ways:

- We will use information about your disability status (if applicable) to consider whether we need to provide appropriate adjustments during the recruitment process.
- We will use information about your race or national or ethnic origin, religious, philosophical, or moral beliefs, or your sexual orientation, to ensure meaningful equal opportunity monitoring and reporting.

## 2.6 Does Keyfactor Collect Criminal Convictions Information?

We will collect information about criminal convictions if it is appropriate given the nature of the role and where we are legally able to do so. Where appropriate, we will collect information about criminal convictions as part of the recruitment process or we may be notified of such information directly by you in the course of you working for us.

## 2.7 Application Security

Recruitment applicant information is held securely. Keyfactor maintains a documented Data Retention Policy which sets out how long we keep different types of information. We follow legal requirements and best practice.

## 2.8 Your Rights

As a data subject, you have several rights. You can:

- Access and obtain a copy of your data, on request
- Require us to change inaccurate or incomplete data
- Require us to delete or stop processing your data, for example where the data is no longer necessary for the purposes of processing
- Object to the processing of your data, where we rely on our legitimate interests as the lawful basis for processing, and
- Ask us to stop processing data for a period if data is inaccurate or if there is a dispute about whether your interests override our legitimate grounds for processing personal data.

If you would like to exercise any of these rights, please contact us via [privacy@keyfactor.com](mailto:privacy@keyfactor.com).

# KEYFACTOR

Keyfactor is the leader in cloud-first PKI-as-a-Service and crypto-agility solutions. Its Crypto-Agility Platform empowers security teams to seamlessly orchestrate every key and certificate across their entire enterprise.

We help our customers apply cryptography in the right way from modern, multi-cloud enterprises to complex IoT supply chains.

With decades of cybersecurity experience, Keyfactor is trusted by more than 500 enterprises across the globe. Built on a foundation of trust and security, Keyfactor is a proud equal opportunity employer, supporter and advocate of growing a trusted, secure, diverse and inclusive workplace.

For more information, visit [www.keyfactor.com](http://www.keyfactor.com) or follow on [LinkedIn](#), [Twitter](#) and [Facebook](#).

KEYFACTOR

