



# Applicant Privacy Notice

This notice sets out what personal information we collect from you as part of our recruitment process, and what we do with it.

## Application information

Whether you apply for a role directly from the job ad, through LinkedIn or through third-party job sites, a recruiter or referral, we store your details in a system called Workable. The system will send you an email confirmation of your application.

Our People team and the relevant hiring manager will have access to your application. Sometimes other team members will also need to see your CV. If you are put forward for a role by a recruitment agency, they will also have access to your information until the point you accept any offer we make. The recruiter continues to have access to your application data if you are rejected. Should you wish to exercise your data protection rights regarding the information held with such agency, you may do so by making your request directly to them.

## Public social media, websites and blogs

As part of the candidate review, we may assess your LinkedIn profile, Github account, Bitbucket account, personal website and published blogs. This is only in relation to information relevant to the role, and to assess your capability to perform the duties described in the role.

## Tests

We require tests for some roles, for example, to demonstrate coding ability. We usually issue coding tests and view results and scores using HackerRank or Github. We may also use bespoke tests created using Google Suite for some tasks, such as those required for non-engineering roles.

## Interviews

We use standardised interview questionnaires to collate information and feedback from interviews at each stage of the process, and store this in Workable.

For interviews with the hiring team, we use Screenloop to record interviews in order to provide analytics to hiring managers, as well as to give non-present stakeholders in the hiring process the opportunity to review candidates retrospectively.

Interviews will take place via Screenloop by default, but all candidates reserve the right to opt out of Screenloop conducted interviews. If you would like to opt out of having your interview recorded, please let the relevant People/Recruitment team member you've been liaising with know in no less than 24 hours before your scheduled interview.



If you do choose not to opt out of having your interview recorded, we will store your interview video for one year after your application date. This will be automatically deleted after one year. If you would like to delete your video sooner than one year please contact [the People Team](#). We are also able to provide you with a transcript of your interview, on request.

### **Unsuccessful application**

If you are unsuccessful, we will delete any candidate application data for that role after 13 months.

If you would like us to add you to a 'talent pool' on Workable so that we can contact you about other roles for which you might be suitable please email [PeopleTeam@yoti.com](mailto:PeopleTeam@yoti.com). We will keep your information in this talent pool for 13 months.

### **Successful application**

Our People team (or a recruiter if relevant) will contact you to make an offer and ask for other details we require for your contract, references and pre-employment checks. We keep this information in our HR system, bob, and in the candidate's personnel file in our Confidential HR folder on Google Drive. In general, we keep personnel files for as long as we employ you plus a further seven years. We have legal requirements to keep some information for specific time periods, for example, where we sponsor a person's visa. We have an HR retention schedule to cover all the different types of HR personal information and the different time requirements.

### **Pre-employment checks**

We carry out certain checks on all new employees / contractors and extra checks on those in high-risk roles. Specifically, we will check the following.

#### **UK-based staff**

- ID and Right to Work checks.
- Employment references.
- Qualification checks (where we require a qualification for a role).
- Directorship checks (where we require this for a role).
- Basic Disclosure Barring Service check (where we require this for a role).
- A TransUnion check that includes bank account validation, verification and fraud check; address match; PEPs and sanctions check; CCJ and bankruptcy checks.
- The CIFAS Internal Fraud Database, which has been established to allow organisations to share data on employee fraud cases. Where the CIFAS Internal Fraud Database flags a related record in the CIFAS National Fraud Database, we will also check the related record.

As a member of CIFAS, if we identify fraud or other unlawful conduct, both when you apply for a job and during your employment, we will record the details on CIFAS. CIFAS keep this fraud record for six years. This information may be accessed from the UK and other countries and used by law enforcement agencies and other organisations to prevent fraud and may lead to refusal of employment or services. You can read the Cifas privacy notice here: <https://www.cifas.org.uk/fpn>

#### **India-based staff**



- Identity check
- Police verification check, address check, credit check and criminal court record check.
- Employment check and education / qualification check.

### **Staff in other locations**

- A TransUnion check that includes an ID check, bank account validation, verification and fraud check; address match; PEPs and sanctions check; CCJ and bankruptcy checks.
- Right to work check.
- Employment references.

Please contact [PeopleTeam@Yoti.com](mailto:PeopleTeam@Yoti.com) for information or questions on fraud prevention databases we use.

## **Your rights and choices**

### **Access rights**

You are entitled to see the personal information we hold about you. You will already have a copy of your application. To request access to any other information we may hold about you, please contact [privacy@yoti.com](mailto:privacy@yoti.com).

### **Correction rights**

You are entitled to correct personal information we hold about you that is inaccurate. If you think that any of the information we hold about you is not accurate, please contact [privacy@yoti.com](mailto:privacy@yoti.com) setting out the inaccuracy, the correct information, and any relevant evidence.

### **Deletion rights**

In certain circumstances you are entitled to ask us to delete the personal information we hold about you. Please contact [privacy@yoti.com](mailto:privacy@yoti.com) with any deletion request.

### **Objection rights**

In certain circumstances you are entitled to object to Yoti processing your personal information. If you want to contact us about your objection rights, please email: [privacy@yoti.com](mailto:privacy@yoti.com)

### **Restriction rights**

In certain circumstances you are entitled to ask us to restrict our processing of your personal information. You can ask us to do this if you dispute the accuracy of your personal information; if our processing is unlawful but you prefer restriction to deletion; if we no longer need the information but you need it for legal reasons; or if you have objected to our processing and we are still dealing with this objection.

### **Portability rights**

In certain circumstances you are entitled to receive the personal information you have provided us in a structured, commonly used and machine-readable format.

## **Complain to the ICO**



You can also complain to the Information Commissioner's Office (ICO) who is responsible for making sure that organisations comply with the law on handling personal information. (<https://ico.org.uk/global/contact-us/>).

**Lawful bases**

EU data protection law requires an organisation to have a lawful basis for its personal data collection and use, and there are several lawful bases available. We are a global company and so in some cases our choice of EU lawful basis reflects the need to comply with different laws in different countries.

Performance of a contract	When you apply for a job with us we need certain information from you to assess your suitability for the role and to decide whether to offer you the job.
Legitimate Interests	Some personal data collection and use is in our legitimate business interests.  Background checks: to check your identity, the facts you have given us about your employment history and qualifications, and fraud prevention checks.
Fraud prevention	Fraud reporting: CIFAS require us to report identity fraud we discover.  For background checks involving sensitive data, such as records of criminal activity.
Consent	Talent pool: to keep information on candidates who were not successful in a specific role so that we can contact you later on if we think you are a good fit for another role. Note you are only added to the talent pool by your specific request - you can withdraw consent for this at any time by contacting PeopleTeam@yoti.com

**Contact us**

E-mail: [privacy@yoti.com](mailto:privacy@yoti.com); [PeopleTeam@yoti.com](mailto:PeopleTeam@yoti.com)  
 Website: <https://www.yoti.com/contact/#contact-us-choose>  
 FAQs: <https://yoti.zendesk.com/hc/en-us>

Address: Yoti Ltd, 6th Floor, Bankside House, 107 Leadenhall Street, London, EC3A 4AF



## Revision history

Version	Reason for change	Date
1.0	First version	January 2018
1.1	Updated for GDPR to expand on rights information and to add section on lawful bases.	May 2018
1.2	Updated to clarify pre-employment checks; add relevant Cifas-required information; and to update retention periods.	28 February 2019
1.3	Updated to reference different background checks for different locations. Update CallCredit to TransUnion.	26 February 2020
1.4	Updated checks.	26 May 2020
1.5	Annual review.	26 May 2021
1.6	Annual review.	31 May 2022
1.7	Annual review. Minor amend to post-application email confirmation and change to talent pool procedure, retention and lawful basis.	18 July 2023