



## GDPR FAIR PROCESSING NOTICE - APPLICANTS

If you apply for a job at Tenable, Inc. or its subsidiaries ("Tenable"), we will collect and process your personal data as part of the selection and recruitment process. In accordance with the requirements of the General Data Protection Regulation (GDPR). This privacy statement describes how we collect and use your data both during and after the recruitment process.

It is important that you read this notice, together with any other privacy notice we may provide on specific occasions when we are collecting or processing personal data about you, so that you are aware of how and why we are using such information.

For the purposes of the GDPR, Tenable is a "data controller". This means that we are responsible for deciding how we hold and use personal information about you. As a data controller we are required under GDPR to notify you of the information contained in this privacy notice.

### YOUR DATA

In this section we outline the purposes for which we may process your data. For each 'purpose' we also list the types of data we may process and our legal basis for the processing it.

#### **Registration & Selection**

- Acknowledging your application
- Determining your suitability for current and future vacancies
- Alerting you to future vacancies

#### Types of personal data that may be processed

- Data & time of application
- Personal data allowing identification: Title, surname, first name, date and place of birth
- Contact information: street address, telephone and email address
- Data required to verify eligibility for vacancy: nationality ( or immigration status), education, training, professional experience(prior jobs, tenure, employer name, contact details of employer, main tasks and responsibilities, linguistic and job related skills and competencies, current and prior salary, reason for leaving prior jobs)
- Data included in application forms and CV/ Resume
- Additional communication collected: cover letters, emails etc. where candidate personally expresses desire and suitability for role
- Interview: candidates will be asked questions aimed at obtaining evidence of how they meet the requirement of the vacancy. The same areas of questioning will be covered for each candidate and no questions will discriminate on grounds of race, sex, ethnic origin, religion,



disability, age or sexual orientation. Candidate responses will be recorded in writing and may additionally be recorded electronically

- Admission tests: depending on the role candidates may be requested to undertake tests targeted at identifying competencies deemed required or desirable for the vacancy. The tests are designed not to create discriminatory bias based on grounds of race, sex, ethnic origin, religion, disability, age or sexual orientation. Test results will be recorded
- Data provided by third party placement firms, recruiters, job search websites to which you have affiliated

## **Recruitment**

- Making a decision about your recruitment
- Determining the terms of an offer of employment
- Checking the validity of your qualifications and previous work history
- Checking that you are legally entitled to work in the country of employment
- Undertaking additional pre-employment checks as required by law.

### Types of personal data that may processed

- Original ID document check (passport, national ID card etc.) in accordance with local immigration 'right to work' requirements and other applicable laws
- Original qualifications document check-
- Employment verification references from former employers
- Education verification references from former educational institutions
- Criminal Record checks ( only when authorised by local law)
- Financial/Credit checks to ascertain registered debts , court judgements, bankruptcies ( only if relevant to the role to be undertaken and if authorised by local law)
- Health questionnaire /Medical – for certain vacancies we may request that you establish your fitness for the role by requesting you complete a medical questionnaire or in some instances a medical examination. Note that this will be a requirement if mandated by local law.

## **Reimbursement of travel, accommodation or other expenses**

- To facilitate the payment of approved expenses incurred during the recruitment process

### Types of personal data processed

- Travel receipts, account holder name(s), name of bank, sort code, account number.

## **Criminal Convictions**

For information about criminal convictions (and other 'excluded party lists'), in accordance with Art 10 GDPR we may only use this data where the law allows us to do so. We do not envisage that we will process information on criminal convictions, however there may be circumstances where the nature of a role requires us to request this information and if this is the case you will be provided with additional prior notification.

## **If you fail to provide personal information**

A failure to provide certain requested information may prevent us from completing our selection and recruitment formalities, however where possible we will work with candidates to ensure that an application is not prejudiced.

## **Change of purpose**

We will only use your personal information for the purposes for which we collected it, unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original purpose. If we need to use your personal information for an unrelated purpose, we will notify you and we will explain the legal basis which allows us to do so.

Please note that we may process your personal information without your knowledge or consent, in compliance with the above rules, where this is required or permitted by law.

## **Will your personal data be subjected to automated decision making?**

Automated decision-making takes place when an electronic system uses personal information to make a decision without human intervention. We are allowed to use automated decision-making in the following circumstances:

1. Where we have notified you of the decision and given you 21 days to request a reconsideration.
2. Where it is necessary to perform the contract with you and appropriate measures are in place to safeguard your rights.
3. In limited circumstances, with your explicit written consent and where appropriate measures are in place to safeguard your rights.

If we make an automated decision on the basis of any particularly sensitive personal information, we must have either your explicit written consent or it must be justified in the public interest, and we must also put in place appropriate measures to safeguard your rights.

We do not envisage that any decisions will be taken about you using automated means, however we will notify you in writing if this position changes

## **Data Sharing**

Your data will be accessed only by those individuals involved in the selection and recruitment process and wherever possible we try and minimise the number of people this involves. Within Tenable itself this will be limited to the HR team and hiring managers.

## **Third Parties**

We may have to share your data with third parties, including third-party service providers and other entities in the group.

The following activities are carried out by third-party service providers:

- Candidate sourcing
- Pre-employment qualifying assessments (if required)
- Online recruitment portal (such as Jobvite)
- Employment/Recruitment marketing
- Background screening (only with your express consent)
- Government officials/law enforcement agencies when local reporting is required
- IT services company providing system maintenance

All our third-party service providers and other entities in the group are required to take appropriate security measures to protect your personal information in line with our policies. We do not allow our third-party service providers to use your personal data for their own purposes. We only permit them to process your personal data for specified purposes, in accordance with our instructions and under the terms of a data processing agreement.

Note that in circumstances where you have first supplied your data to a third party, such as a recruitment agency, they will also operate as a data controller for the purposes of the GDPR and as such have their own responsibilities for the security of your data.

### **Transferring information outside of the EU**

We may transfer the personal information we collect about you to countries outside the European Economic Area ('EEA' for the purposes described above.

To ensure that your personal information receives the appropriate protection when transferred outside of the EEA, we have implemented appropriate measures to ensure that your personal information is treated by those third parties in non-EEA countries in a way that is compliant with the GDPR. Specifically, in regards to personal data transferred to Tenable's US offices, we are certified under the EU-US and Swiss-US Privacy Shield Frameworks. We also have the Model Clauses in place amongst Tenable entities governing transfers from the EEA to non-EEA Tenable entities.

You can contact us if you require further information about these protective measures.

### **The period for which data is stored**

If you are successful in securing employment with Tenable the information we collect during the selection and recruitment process will form part of your personnel record and as such will be retained for the duration of your employment with Tenable or for such longer period as required by legal, accounting or reporting standards applicable to our business.

If you are unsuccessful in your application, in order that you may be considered for future vacancies we will retain your data for one (1) year commencing from the date that your application has been rejected, unless an alternative length of time frame is stated above, or where we are prohibited from

retaining your data. Please note that you have the right to object to this at the time of rejection, whereupon your data will be destroyed or returned to you.

In some circumstances we may anonymise your personal information so that it can no longer be associated with you, in which case we may continue to use such information without further notice to you.

## Data Security

When we process your personal data we will always apply the core principles of the GDPR to ensure it is:

1. Used lawfully, fairly and in a transparent way.
2. Collected only for valid purposes that we have clearly explained to you and not used in any way that is incompatible with those purposes.
3. Relevant to the purposes we have told you about and limited only to those purposes.
4. Accurate and kept up to date.
5. Kept only as long as necessary for the purposes we have told you about.
6. Kept securely.

We have put in place appropriate security measures to prevent your personal information from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. In addition, we limit access to your personal information to those employees, agents, contractors and other third parties who have a business need to know. They will only process your personal information on our instructions and they are subject to a duty of confidentiality.

We have put in place procedures to deal with any suspected data security breach and will notify you and any applicable regulator of a suspected breach where we are legally required to do so.

## YOUR RIGHTS

Under certain circumstances, by law you have the right to:

- Request access to your personal information (commonly known as a "data subject access request"). This enables you to receive a copy of the personal information we hold about you and to check that we are lawfully processing it.
- Request correction of the personal information that we hold about you. This enables you to have any incomplete or inaccurate information we hold about you corrected.
- Request erasure of your personal information. This enables you to ask us to delete or remove personal information where there is no good reason for us continuing to process it. You also have the right to ask us to delete or remove your personal information where you have exercised your right to object to processing (see below).
- Object to processing of your personal information where we are relying on a legitimate interest (or those of a third party) and there is something about your particular situation which makes you want to object to processing on this ground. You also have the right to object where we are processing your personal information for direct marketing purposes.

- Request the restriction of processing of your personal information. This enables you to ask us to suspend the processing of personal information about you, for example if you want us to establish its accuracy or the reason for processing it.
- Request the transfer of your personal information to another party.

If you want to review, verify, correct or request erasure of your personal information, object to the processing of your personal data, or request that we transfer a copy of your personal information to another party, please email [gdpr@tenable.com](mailto:gdpr@tenable.com).

As stated above the processing of your personal data is based on legal basis other than your consent, however in the very limited circumstances where you may have provided your consent to the collection and processing of your data, you have the right to withdraw your consent for that specific processing at any time. To withdraw your consent, please email [gdpr@tenable.com](mailto:gdpr@tenable.com). Once we have received notification that you have withdrawn your consent, we will no longer process your information for the purpose or purposes you originally agreed to, unless we have another legitimate basis for doing so in law.

### **No fee usually required**

You will not have to pay a fee to access your personal information (or to exercise any of the other rights). However, we may charge a reasonable fee if your request for access is clearly unfounded or excessive. Alternatively, we may refuse to comply with the request in such circumstances.

### **What we may need from you**

We may need to request specific information from you to help us confirm your identity and ensure your right to access the information (or to exercise any of your other rights). This is another appropriate security measure to ensure that personal information is not disclosed to any person who has no right to receive it.

### **Contact details**

If you have any questions about this privacy notice or how we handle your personal information, please email the following address: [gdpr@tenable.com](mailto:gdpr@tenable.com).

### **Raising a complaint**

If you are unhappy with the way in which your personal data has been processed you may in the first instance email: [gdpr@tenable.com](mailto:gdpr@tenable.com).

If you remain dissatisfied then you have the right to apply directly to the appropriate data protection authority. Please email [gdpr@tenable.com](mailto:gdpr@tenable.com) to be directed to the relevant data protection authority contacts.

## Changes to this privacy notice

We reserve the right to update this privacy notice at any time, and we will provide you with a new privacy notice when we make any substantial updates. We may also notify you in other ways from time to time about the processing of your personal information.

---

**For More Information:** Please visit [tenable.com](https://tenable.com)

**Contact Us:** Please visit [tenable.com/contact](https://tenable.com/contact)