GDPR FAIR PROCESSING NOTICE

This GDPR Fair Processing Notice ("Notice") applies if you are a resident of the EUU or apply for a job at any of Pulse Secure, LLC's wholly owned European subsidiaries, i.e., Pulse Secure UK Limited, Pulse Secure GmbH, PS Secure Access AB) (collectively "Pulse Secure"). 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 Notice describes how we collect and use your data both during and after the recruitment process.

It should be noted that our legal basis for processing your data is your consent. This Notice is designed to provide you with information to ensure that your consent is informed, freely given, specific and unambiguous.

By submitting your details you will acknowledge that you have read this Notice and that your submission is an affirmative action signifying your consent and agreement to the processing of your personal data. Please do not provide your personal data If you do not consent to Pulse Secure processing it.

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 information about you, so that you are aware of how and why we are using such information.

For the purposes of the GDPR, Pulse Secure 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 the GDPR to notify you of the information contained in this 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	**Date & 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 :** covering 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 and are affiliated with.**
Lawful basis for processing personal data	- Your consent. By submitting your personal data you will be providing consent to this processing and are acknowledging that your consent is freely given, specific, informed and unambiguous (applying GDPR Art 6.1a)

Recruitment

- Making a decision about your recruitment
- Determining the terms of an offer of employment
- Checking the validity of your qualifications and previous employment 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 **Original qualifications document check** **Employment verification references from former employers** **Education verification references from former educational institutions** **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)

Lawful basis for processing personal data	- Your consent. By submitting your personal data you will be providing consent to this processing and are acknowledging that your consent is freely given, specific, informed and unambiguous (applying GDPR Art 6.1a). - To comply with a legal obligation to ensure a candidate has the lawful right to work or to complete mandatory medical checks (applying GDPR Art 6.1c- compliance with a legal obligation) - To check whether you have criminal convictions (when it is required and authorised by law and with appropriate safeguards for the rights and freedoms of data subject- applying GDPR Art 10)

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.
Lawful basis for processing personal data	- Your consent – By submitting your personal data you will be providing consent to this processing and are acknowledging that your consent is freely given, specific, informed and unambiguous (applying GDPR Art 6.1a).

Equality

- Equal opportunities monitoring

Types of personal data processed	Information about your race or ethnicity, religious beliefs, sexual orientation and political opinions **NOTE: candidates are NOT required to provide this (other than when required by law- as per point below) and therefore the supply of this data will be completely voluntary and a failure to provide will not affect your application**
Lawful basis for processing 'special categories' of personal data	- *AT THE TIME OF OUR REQUEST WE WILL SEEK SEPARATE EXPRESS CONSENT FROM YOU AND YOU ARE FREE TO OBJECT.* - To satisfy mandatory government reporting (when it is required to be collected by law) - applying GDPR Article 9 .2b and g).

Your Consent

Under the terms of the GDPR for your consent to be valid it should be given by a clear affirmative act establishing a freely given specific, informed and unambiguous indication of your agreement to the processing of data relating to you.

For online applications we have ensured that personal data can only be supplied by a candidate if they have first checked a box which confirms that they have read this Notice and also consent to the processing of their data as described in this Notice.

If data has been supplied to us via a different route then on receipt we will contact you and request that you provide your consent by signing a copy of this Notice, and advise you that in the absence of receiving this within 3 weeks of our request your data will be destroyed.

Note that the consent you provide by virtue of this Notice does not cover the processing of special categories of data (as defined by the GDPR, namely, data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and data concerning health or data concerning a natural person's sex life or sexual orientation). We will seek separate and express consent to the processing of this type of data.

You have the right to withdraw your consent at any time. To withdraw your consent, please contact Pulse Secure's Privacy Compliance Officer at: privacy@pulsesecure.net. 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.

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 Pulse Secure this will be limited to the HR team and hiring committee.

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 categories of third-parties will have access to your personal data:

- Other Pulse Secure group companies ;
- Zoom – a company that provides virtual interview facilities (when a physical meeting is not possible);
- BambooHR – a company that hosts our online recruitment portal;
- Advanced Reporting – a company that provides background screening (only with your express consent);
- Government officials/law enforcement agencies when local reporting is required;
- Zendesk – an IT services company providing system maintenance;
- Radius Global – a HR and payroll provider tasked with the provision of employment contracts.

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 in order to perform our contract with you.

There is not an adequacy decision by the European Commission in respect of these countries, which means they are not deemed to provide an adequate level of protection for your personal information.

However, to ensure that your personal information does receive an adequate level of protection we have put in place relevant appropriate measures to ensure that your personal information is treated by those third parties in a way that is consistent with and which respects the laws on data protection.

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 Pulse Secure 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 Pulse Secure or for such longer period as required by legal, accounting or reporting standards applicable to our business.

In order that you may be considered for future vacancies if you are unsuccessful we request that you consent to your data being retained for 12 months commencing from the date that your application has been rejected. 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 contact the Pulse Secure Privacy Compliance Officer at privacy@pulsesecure.net.

Where the processing of your data is based on your consent, you have the right to withdraw your consent for that specific processing at any time. To withdraw your consent, please contact the Pulse Secure Privacy Compliance Officer at privacy@pulsesecure.net. 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

We have appointed a Privacy Compliance Officer to oversee compliance with this Notice. If you have any questions about this Notice or how we handle your personal information, please contact the Privacy Compliance Officer at the following email address: privacy@pulsesecure.net.

Raising a complaint

If you are unhappy with the way in which your personal data has been processed you may in the first instance raise a complaint by contacting Pulse Secure's Privacy Compliance Officer using the contact details above.

If you remain dissatisfied then you have the right to apply directly to the British Data Protection Authority for a decision – contact details below:

Water Lane, Wycliffe House
Wilmslow - Cheshire SK9 5AF
Tel. +44 1625 545 745

e-mail: international.team@ico.org.uk
Website: https://ico.org.uk

Changes to this privacy notice

We reserve the right to update this 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.

I, _____ (your name) acknowledge that on _____ (date), I received a copy of this Fair Processing Notice for candidates and that I have read and understood it.

Signature

……

Name