JOB APPLICANT PRIVACY NOTICE FOR EUROPEAN AND ISRAELI

APPENDIX 4: EUROPEAN AND ISRAELI JOB APPLICANT PRIVACY NOTICE

INTRODUCTION

This Privacy Notice describes how Cybereason processes the personal data of (1) all current and former applicants and interview candidates located in the European Economic Area ("EEA"), Switzerland, United Kingdom ("UK") or Israel (**"**applicants" or "you" or "your"), and (2) third parties whose information you provide to us in connection with your application (e.g., next-of-kin, emergency contacts or dependents).

For the purposes of this Privacy Notice, Cybereason, Inc., Cybereason Limited, and Cybereason Labs Ltd. ("Cybereason", "we", "us" and "our") will be the data controller of your personal data. Where other Cybereason affiliates process your personal data for their own independent purposes (such as when you apply for a role with Cybereason France SAS and Cybereason Germany GmbH), these affiliates may be co-controllers of your personal data.

This Privacy Notice describes the categories of personal data we may process, how your personal data may be processed, for what purposes we process your data and how your privacy is safeguarded. This Privacy Notice does not form part of a contract of employment or service.

WHAT DATA DO WE PROCESS?

We collect various types of personal data about you for the purposes described in this Privacy Notice including:

- **personal details**, such as your title and name, gender, home contact information (e.g., postal address, telephone or mobile number, e-mail address), immigration and work eligibility information, languages spoken, and details of any disability and any reasonable adjustments required as a result;

- **recruitment and selection data**, such as your skills and experience, qualifications, references, CV and application, record of interview, interview notes and assessment, vetting and verification information (e.g., results of credit reference check, financial sanction check and a criminal record check where permitted by applicable law), right to work verification, information related to the outcome of your application, details of any offer made to you;

- **equality and diversity data**, such as, where permitted by law and provided voluntarily, data regarding gender, race, nationality, and sexuality (stored anonymously for equal

opportunities monitoring purposes); and

- any other personal data which you choose to disclose to Cybereason personnel during the application process, whether verbally or in written form (e.g., in emails).

Certain additional information will sometimes be collected where this is necessary and permitted by applicable local laws. Some of the information described above constitutes special category data (also known as sensitive data). Sensitive data includes information

relating to racial or ethnic origin, political opinions, religious or philosophical beliefs, health, trade union membership, sex life or sexual orientation, biometric or genetic information, and information relating to criminal records, offences or proceedings. Cybereason only collects sensitive personal data when permitted or required to do so by law, in circumstances described below.

HOW DOES CYBEREASON COLLECT PERSONAL DATA?

Cybereason collects and records your personal data from a variety of sources, often directly from you (e.g., when you apply for a job through our websites) or from our service providers that handle applications on our behalf. We also obtain some information from third parties, such as references from a previous employer, candidates from recruitment agencies or where we employ a third party to carry out a background check (where permitted by applicable law).

Where we ask you to provide personal data to us on a mandatory basis, we will inform you of this at the time of collection. Failure to provide any mandatory information may mean that we cannot carry out our recruitment process.

Apart from personal data relating to you, you may also provide Cybereason with personal data of third parties, such as contact information of individuals listed as references in your application. Before you provide such personal data about third parties to Cybereason, you must first inform these third parties of any such data which you intend to provide to Cybereason and of the processing to be carried out by Cybereason, as detailed in this Privacy Notice.

WHAT ARE THE PURPOSES FOR WHICH DATA ARE PROCESSED?

We collect and process your personal data because it is in our legitimate business interests to consider your suitability for a role within Cybereason. These legitimate business interests include:

- For recruitment and selection purposes, including to (i) assess your skills, qualifications and suitability for a role; (ii) carry out background and reference checks, where

applicable; (iii) make a job offer and provide a contract of employment; (iv) on-board you as personnel where you accept an offer from us; (v) contact you if you are not successful should another potentially suitable vacancy arise during one year following the completion of the recruitment process for the role you applied for (unless your object); (vi) keep records related to our hiring processes; (vii) communicate with you about the recruitment process; and (viii) handle any query, challenge or request for feedback received in relation to our recruitment decision.

- To protect private, confidential and proprietary information of Cybereason, its employees, its customers and third parties;

- To enforce our legal rights and obligations, comply with legal or regulatory requirements, (including checking your legal right to work) and for any purposes in connection with any legal claims made by, against or otherwise involving you;

- comply with lawful requests by public authorities (including without limitation to meet national security or law enforcement requirements), discovery requests, or where otherwise required or permitted by applicable laws, court orders, government regulations, or regulatory authorities (including without limitation data protection, tax and employment authorities), whether within or outside your country; and

- for other purposes permitted by applicable laws, including legitimate interests pursued by Cybereason where these are not overridden by the interests or fundamental rights and freedoms of applicants and where these have been explained to you before the relevant data is collected or the processing is carried out.

We may also need to process your personal data to decide whether to enter into a contract of employment (or other arrangement) with you, or to take steps at your request prior to entering into such a contract.

In certain circumstances, we may also rely on your consent for the purposes of processing your job application. Where we rely on your consent, we will notify you of this at the point we collect your personal data

Sensitive data may be collected and processed by Cybereason for the following purposes:

- Documentation such as work permits, details of residency and proof of citizenship will be processed to assess and review your eligibility to work for Cybereason in the jurisdiction in which you apply. We process this information where (i) we have your explicit consent

to do so, (ii) it is in the public interest to do so, such as, to determine whether an individual has committed an unlawful act or has been involved in dishonesty, malpractice or other serious misconduct, or (iii) we need to process this information to exercise rights and perform obligations in connection with your work for Cybereason;

- information about your health (including any medical condition, health and disability) to consider whether we need to provide appropriate adjustments during the recruitment process. We need to process this information to exercise rights and perform obligations in connection with your work for Cybereason;

- your racial or ethnic origin, religious or philosophical beliefs, sexual orientation, or disability status may be used for the collection of statistical data subject to local laws. We process this information where we have your explicit consent to do so, or where it is in the public interest to do so, such as to ensure meaningful equal opportunity or diversity monitoring and reporting within Cybereason; and

- Any information that is required for us to establish, exercise or defend legal claims.

Additional information regarding specific processing of personal data may be provided to you or as set out in applicable policies. Personal data relating to criminal convictions and offenses will only be processed where authorized by applicable laws. For example, a criminal record check may be carried out on recruitment.

RETENTION OF PERSONAL DATA

Cybereason retains personal data for as long as is required to satisfy the purpose for which it was collected by us or provided by you. This will usually be the period of the application process plus the length of any applicable statutory limitation period. We will keep some specific types of data (such as your CV) for up to twelve months where we have a legitimate business reason to do so, such as to contact you for future opportunities.

DISCLOSURES OF PERSONAL DATA

We share your personal data with our Cybereason affiliates and any of their personnel for the purposes described in this Privacy Notice. Cybereason also shares personal data with service providers that perform services on our behalf, such as our recruitment platform provider; background and education verification agencies; HR and recruitment service providers; employer of record service providers (e.g., XML), accounting, payment and expense reimbursement providers; travel providers; professional advisors (e.g., lawyers and accountants), and electronic signature providers.

In addition, we may disclose personal data about you (i) if we are required or permitted to do so by law or legal process (e.g., due to a court order) or in response to an order or request from a law enforcement or regulatory agency, (ii) to comply with legal and regulatory requirements, (iii) when we believe disclosure is necessary or appropriate to protect safety or prevent physical harm or financial loss, (iv) in connection with an investigation of suspected or actual fraudulent or other illegal activity, and (v) in connection with a sale or transfer of all or a portion of our business or assets (e.g., in the event of an acquisition, merger, reorganization, dissolution, or liquidation).

SECURITY OF DATA

Cybereason has technical, physical and organisational measures to maintain an appropriate level of security for your personal data. Cybereason uses a variety of technical and organisational methods to secure your personal data in accordance with applicable laws.

INTERNATIONAL TRANSFER OF PERSONAL DATA

From time to time, your personal data (including sensitive data) will be transferred to Cybereason affiliates to process for the purposes described in this Privacy Notice. These affiliates may be located elsewhere in the world (such as in the United States, Israel, Japan, the EEA, Switzerland and UK). Personal data also may be transferred to third parties (e.g., vendors as described above), who may have systems or suppliers located outside the EEA, Switzerland and UK. As a result, in some circumstances your personal data will be transferred to countries outside of the EEA, Switzerland and UK whose data protection laws may be less stringent than in the EEA, Switzerland and UK.

In such cases, Cybereason will comply with applicable legal requirements and will only transfer your personal data if:

- The country to which the personal data will be transferred has been recognized as providing an adequate level of protection for personal data, such as Japan or Israel; or

- We have put in place appropriate safeguards with respect to the transfer, such as the Standard Contractual Clauses.

You may request a copy of the safeguards that we have put in place with respect to the transfer of your personal data by contacting us as described in the Contact Us section below.

YOUR RIGHTS AS A DATA SUBJECT

Subject to applicable law, you may have the right to request:

- confirmation of whether we process personal data relating to you and, if so, to request a copy of that personal data;

- that we rectify or update your personal data that is inaccurate, incomplete or outdated;

- that we cease to process certain personal data where you object to its use and we do not have an overriding legitimate interest in carrying out the processing and it is not necessary for the establishment, exercise or defense of legal claims;

- that we erase your personal data in certain circumstances, such as where we collected personal data on the basis of your consent and you withdraw that consent, or when you object to use of your personal data;

- that we restrict the use of your personal data in certain circumstances, such as while we consider another request that you have submitted (such as a request that we update your personal data);

- withdrawal of your consent where you have given us consent to process your personal data; and

- that we provide a copy of your personal data to you in a structured, commonly used and machine readable format in certain circumstances.

If you wish to exercise any of your data protection rights, please contact us as described in the Contact Us section below. If you believe that we have processed your personal data in violation of applicable law and failed to remedy such violation to your reasonable satisfaction, you also may lodge a complaint with the data protection authority in your jurisdiction.

NOTICE OF CHANGES

Cybereason may change or update this Privacy Notice at any time. We will notify you of any material changes to this Privacy Notice to the extent required to do so by applicable law.

This Privacy Notice was last updated on August 14, 2024.

CONTACT US

If you have any questions about this Privacy Notice or if you would like to exercise your rights, please email us at: privacy@cybereason.com.