JOB APPLICANT PRIVACY NOTICE FOR GERMANY

APPENDIX 1: EUROPEAN JOB APPLICANT PRIVACY NOTICE (GERMANY)

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 or United Kingdom ("UK") (**"**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 Germany GmbH, Theresienhöhe 28, 80339 Landsberger Straße 155, 80687 Munich, and Cybereason Inc., 1250 Prospect Street, Suite 5, La Jolla, San Diego, 92037, California, USA ("Cybereason", "we", "us" and "our") will be the data controllers of your personal data.

The contact details of the German data protection officer are as follows:

Jason Komninos
Ganghoferstraße 33, 80339 München, Germany
privacy@cybereason.com

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.

This Privacy Notice applies specifically to the processing of your personal data in the context of your application via our online application tool. For further information on data processing on our website, please refer to our general Privacy Notice.

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, email 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), background check information related to your qualification and background as an applicant where permitted by applicable law, right to work verification, information related to the outcome of your application, details of any offer made to you; 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 personal 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).

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 AND LEGAL BASES FOR WHICH PERSONAL DATA ARE PROCESSED?

We process personal data only when we have a legal basis for doing so and will process personal data for the following purposes and on the following legal bases:

We collect and 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 (i.e., for hiring / engagement decisions) for the following purposes, whereby the legal basis is Art. 6 (1) lit. b GDPR:

- For recruitment and selection purposes, including to (i) assess your skills, qualifications and suitability for a role (ii) make a job offer and provide a contract of employment (iii) on-board you as personnel where you accept an offer from us (iv) communicate with you about the recruitment process; and (v) carry out background and reference checks, where permitted by applicable law; and

- To comply with legal or regulatory requirements (including checking your legal right to work).

We may also need to process your personal data to comply with legal obligations under EEA, Swiss or UK law for the following purposes, whereby the legal basis is Art. 6 (1) lit. c GDPR:

- To comply with legal or regulatory requirements (including checking your legal right to work);

- To 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);

- To keep records related to our hiring processes; and

- To ensure meaningful equal opportunity or diversity monitoring and reporting within Cybereason as required by law.

In certain circumstances, we may also rely on your consent for the purposes of processing your job application. In this case, the legal basis is Art. 6 (1) lit. a GDPR. Where we rely on your consent, we will notify you of this at the point we collect your personal data.

We may also collect and process your personal data based on our legitimate business interests, provided that these business interests are not overridden by your rights, freedoms, or interests. In

this case, the legal basis is Art. 6 (1) lit. f GDPR. In this context, the purposes and legitimate business interests for processing your personal data are:

- 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;

- To ensure meaningful equal opportunity or diversity monitoring and reporting within Cybereason;

- To 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;

- To reach out to for up to 12 months to inform you about other job openings at Cybereason that may be of interest to you.

- To plan and implement changes within our business (e.g., in connection with a sale or transfer of all or a portion of our business or assets); 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.

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 to the extent permissible under applicable laws;

- 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 to the extent permissible under applicable laws; and

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

The legal basis in the above-mentioned cases is in particular Art. 6 para. (1) lit. c GDPR in conjunction with. Art. 9 (2) lit. b GDPR and Section 26 (3) BDSG. Additional information regarding specific processing of personal data may be provided to you or asset 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 where permissible under applicable laws.

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. This period is a maximum of six months. If we conclude an employment contract with you, your application data will be included in the personnel file to the extent necessary. If we believe that you may be interested in other job opportunities at Cybereason, we will retain your data for up to one year after completion of the application process, unless you have objected to such further processing

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: 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; and electronic signature providers.

Furthermore, we may share personal data with professional advisors (e.g., lawyers and accountants).

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.

In addition to this, we intend to, where necessary, agree on additional measures with recipients to ensure an adequate level of data protection.

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.

With regard to the transfer of data to Cybereason Inc. in the USA, we would like to point out that Cybereason Inc. is certified under the EU-U.S. Data Privacy Framework and is also registered on the list maintained by the U.S. Department of Commerce (Data Privacy Framework List). This ensures an adequate level of data protection within the meaning of the

GDPR for such transfers. Insofar as data is transferred to Cybereason Inc., such a third country transfer is therefore based on Art. 45 (1) sentence 1 GDPR.

USE OF ZOOM FOR ONLINE MEETINGS

As part of our application process, we may also use the Zoom tool to conduct conference calls and/or online meetings. Zoom is a service provided by Zoom Video Communications, Inc, 55 Almaden Blvd, Suite 600, San Jose, CA 95113, USA ("Zoom"). To the extent that you access Zoom's website, Zoom is responsible for data processing. However, accessing the Internet site is only necessary to use Zoom in order to download the software for using Zoom. You can also use Zoom if you enter the respective meeting ID and, if applicable, further access data for the meeting directly in the Zoom app. If you do not want to or cannot use the Zoom app, the basic functions can also be used via a browser version, which you can also find on the Zoom website. When using Zoom, various types of data are processed. The scope of the data also depends on the data you provide before or during participation in an online meeting. The following personal data may be subject to processing: User details: first name, last name, telephone (optional), e-mail address, password (if "single sign-on" is not used), profile picture (optional).Meeting metadata: Topic, description (optional), attendee IP addresses, device/hardware information. For recordings (optional): MP4 file of all video, audio and presentation recordings, M4A file of all audio recordings, text file of the online meeting chat. For dial-in with the telephone: information on the incoming and outgoing call number, country name, start and end time. If necessary, further connection data such as the IP address of the device can be stored. Text, audio and video data: You may have the opportunity to use the chat, question or survey functions in an online meeting. To this extent, the text entries you make are processed in order to display them in the online meeting and, if necessary, to log them. In order to enable the display of video and the playback of audio, the data from the microphone of your terminal device and from any video camera of the terminal device will be processed accordingly for the duration of the meeting. You can turn off or mute the camera or microphone yourself at any time through the Zoom applications. If we want to record online meetings, we will transparently communicate this to you in advance and - if necessary - ask for consent. The fact of recording will also be displayed to you in the Zoom app. If you are registered as a user with Zoom, then reports of online meetings (meeting metadata, phone dial-in data, webinar questions and answers) can be stored

by Zoom for up to 12 months. We collect and 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 (i.e., for hiring / engagement decisions) for the following purposes, whereby the legal basis is Art. 6 (1) lit. b GDPR.

Zoom is a service provided by a provider from the US. We would like to point out that there may be additional risks due to the transfer of data to the US, for example, the enforcement of your rights to this data may be more difficult or certain US authorities may gain access to this data. We have concluded an data processing agreement with Zoom that complies with the requirements of Art. 28 GDPR. An adequate level of data protection is guaranteed by the conclusion of the so-called EU standard contractual clauses.

After transmission of the data, Zoom is solely responsible for the processing of the data. Zoom also processes the collected data for its own purposes and to the extent in accordance with its own privacy policy at https://explore.zoom.us/de/privacy/.

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 (right of access);
- that we rectify or update your personal data that is inaccurate, incomplete or outdated;
- that we cease to process certain personal data processed on the basis of legitimate interests where you object to the processing on grounds relating to your particular situation 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 effectively object to use of your personal data processed on the basis of legitimate interests;

- 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). If the processing gets restricted, such personal data shall, with the exception of storage, only be processed with your consent or for the establishment, exercise or defence of legal claims;

- withdrawal of your consent where you have given us consent to process your personal data at any time without affecting the lawfulness of the data processing that was conducted based on your consent before its withdrawal; and

- that we provide a copy of your personal data to you in a structured, commonly used and machine readable format in certain circumstances (e.g., the right to data portability).

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.

NO OBLIGATION TO PROVIDE PERSONAL DATA

You are not legally or contractually obligated to provide personal data. However, without your application data, we will not be able to consider you as part of our applicant recruitment process.

NO AUTOMATED DECISION MAKING

We do not intend to use any personal data collected from you for any automated decision making process (including profiling).

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 in 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.