Cyberbit Cloud Privacy Policy

About us

The Cyberbit Cloud software-as-a-service and related documentation as well as its support services (the "**Services**"), are operated by Cyberbit Ltd. and its affiliated companies, including Cyberbit, Inc., and Cyberbit India Private Limited.

In this privacy policy when we refer to "**Cyberbit**", "**our**", "**we**" or "**us**", we mean any or all of those group companies or Cyberbit Ltd. and they are collectively referred to as the "**Cyberbit Group**".

The following U.S. entities within the Cyberbit Group also adhere to the EU-U.S. DPF Principles, UK Extension to the EU-U.S. DPF, and Swiss-U.S. DPF Principles and are covered by Cyberbit Ltd.'s DPF certification: Cyberbit, Inc.

Cyberbit is subject to the investigatory and enforcement powers of the Federal Trade Commission (FTC) with respect to compliance with the DPF Principles.

About this privacy policy

This privacy policy applies to the Services, made available through www.cyberbitrange.com (the "**Cyberbit Cloud**") and the support services available through www.cyberbit.com/support (the "**Ticketing System**").

This privacy policy applies to any registered user of the Services or administrator or manager on behalf of our customers using the Services or any other individual who has been granted access to the Services by us or is otherwise using the Services in an unpermitted manner (referred to as "**User**", "**you**" or "**your**" in this policy). For any questions or requests under this privacy policy, please send us an email at **privacy@cyberbit.com**.

Cyberbit complies with the EU-U.S. Data Privacy Framework (EU-U.S. DPF) and the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF) as set forth by the U.S. Department of Commerce. Cyberbit has certified to the U.S. Department of Commerce that it adheres to the EU-U.S. Data Privacy Framework Principles (EU-U.S. DPF Principles) with regard to the processing of personal data received from the European Union and the United Kingdom in reliance on the EU-U.S. DPF and the UK Extension to the EU-U.S. DPF. Cyberbit has certified to the U.S. Department of Commerce that it adheres to the Swiss-U.S. Data Privacy Framework Principles (Swiss-U.S. DPF Principles) with regard to the processing of personal data received from Switzerland in reliance on the Swiss-U.S. DPF. If there is any conflict between the terms in this privacy policy and the EU-U.S. DPF Principles and/or the Swiss-U.S. DPF Principles, the Principles shall govern. To learn more about the Data Privacy Framework (DPF) Program, and to view our certification, please visit https://www.dataprivacyframework.gov/

We hereby inform you, and you hereby acknowledge that you have no legal obligation to provide us with any personal data when you use the Services, and the provision of it is solely based on your free will. However without receipt of personal information it may not be possible to use the Services, so please do not use our Services if you do not wish to provide us with personal information, as detailed below.

For access to certain advanced penetration testing tools, additional terms and screening requirements apply. Users will be notified of these requirements and must agree to enhanced verification procedures before gaining access to such tools.

Please read this privacy policy carefully to understand how we handle your personal information. By accessing or browsing the Cyberbit Cloud, using any of the Services or otherwise sharing your personal information with us in connection with the Services, you confirm that you have read and understood the terms of this privacy policy.

This privacy policy is divided into the following sections:

Section 1 **What personal information do we collect about you and for which purposes?**

Section 2 **With whom do we share your personal information?**

Section 3 **How is your personal information transferred outside of the EEA and Israel?**

Section 4 **How long do we keep your personal information for?**

Section 5 **How do we keep your personal information secure?**

Section 6 **What rights do you have regarding your personal information?**

Section 7 **Does this privacy policy apply to third party links?**

Section 8 **How do we approach changes to this privacy policy?**

Section 9 **Do we respond to Do Not Track?**

Section 10 **Contact us and data controllers' details**

1. What personal information do we collect about you and for which purposes?

In this privacy policy, "**personal information**" means (i) information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular person, consumer or household; and (ii) any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly. As you use the Services, we collect personal information directly from you and/or automatically generate it as you use the Services.

"**Statistical and Analytical Purposes**" means personal information in connection with your use of the Services processed to create aggregated or anonymized data.

1.1 *Personal information that you give to us*

When you engage with certain features of our Services, we will collect personal information from you. Except as otherwise indicated below, the personal information you provide is such that we need in order to provide the Services. If you do not provide us with the requested personal information, we would not be able to do so.

Specifically, we collect personal information directly from you or your organization when you:

(a) Register and access to the Cyberbit Cloud. When you are designated as a User by your organization ("**Customer**") and receive log in credentials to access the Cyberbit Cloud and use the Services, we will need you to provide us with personal information (i.e., full name, email address and role), and the organization account ("**Account**") to which you are associated.

We use this personal information to enable you to register and access the Cyberbit Cloud and keep track of your use of the Services; administer the Account; provide technical support; provide you with customer support services; recognize you when you return to the Cyberbit Cloud; provide you with your training history and with customized content; improve and optimize (i) the specific Customer's use of the Cyberbit Cloud; (ii) specific Customer's and User's experience in connection with the Cyberbit Cloud; and (iii) enhance the deployment of the Cyberbit Cloud by the specific Customer. EU legal basis – When we process personal information for these purposes, we process personal data on behalf of the Customer to provide the Services. Therefore, the Customer, as data controller, is responsible for determining the legal basis.

We also use this personal information to ensure that the Cyberbit Cloud is functioning correctly; monitor, investigate any bug with, improve the Cyberbit Cloud and Services and your User experience. EU legal basis - We process personal information for these purposes based on our legitimate interests to improve and secure our Services and user's experience.

(b) Answer our on-boarding questionnaire. When you are designated as a User by your organization, we may ask you to provide professional details about yourself (i.e., your current role, years of experience, professional qualifications, topics of interest.)

Please note that we do not need these details in order to provide the Services and that the provision of these details is at your sole discretion.

We use personal information in order to allow us to offer you units that are relevant to your professional experience and preferences; and improve and optimize (i) the specific Customer's use of the Cyberbit Cloud; (ii) specific Customer's and User's experience in connection with the Cyberbit Cloud; and (iii) enhance the deployment of the Cyberbit Cloud by the specific Customer. EU legal basis – When we process personal information for these purposes, we process personal data on behalf of the Customer to provide the Services. Therefore, the Customer, as data controller, is responsible for determining the legal basis.

We also use personal information for Statistical and Analytical Purposes and to improve the Cyberbit Cloud and/or Services and your User experience. EU legal basis - We process personal information for these purposes based on our legitimate interests to improve and secure our Services and user's experience.

(c) Provide us your (ISC)2 member ID. When you are designated as a User by your organization, we may ask you to provide your member ID in the International Information System Security Certification Consortium ("(ISC)2") so that we will be able to submit information about your training history to (ISC)2 in order for you to obtain and maintain Continuing Professional Education (CPE) credits ("CPE Credits"); and improve and optimize (i) the specific Customer's use of the Cyberbit Cloud; (ii) specific Customer's and User's experience in connection with the Cyberbit Cloud; and (iii) enhance the deployment of the Cyberbit Cloud by the specific Customer. Please note that we do not need your member ID in (ISC)2 in order to provide the Services and that the provision of your member ID is at your sole discretion. EU legal basis - When we process personal information for these purposes, we process personal information on behalf of the Customer to provide the Services. Therefore, the Customer, as data controller, is responsible for determining the legal basis.

(d) We also use personal information to improve the Services and your User experience. EU legal basis - We process personal information for these purposes based on our legitimate interests to improve and secure our Services and user's experience.

(e) When you request to subscribe for exercises used for teaching penetration testing (including utilization of Cobalt Strike), we may collect additional personal information for security screening and compliance purposes, including: professional background, employment history, company information and verification, sanctions and other government watch list screening results, address verification data, LinkedIn profile information, home and business address and professional certifications. This information is collected to comply with our legal and contractual obligations regarding responsible use of advanced penetration testing tools and to prevent misuse. Please note that access to these tools requires enhanced verification and that providing this information is mandatory for access to such tools. We use this personal information to conduct compliance screening for Users requesting to subscribe for exercises used for teaching penetration testing ; verify professional credentials and employment status; check against government watch lists and sanctions databases; validate company information and addresses; assess suitability for access to advanced penetration testing tools; and comply with our legal and contractual obligations regarding responsible tool access. EU legal basis - We process

personal information for these purposes based on our legitimate interests in preventing misuse of advanced penetration testing tools, protecting cybersecurity, fulfilling our contractual obligations to third-party tool providers, and compliance with legal obligations.

(f) Contact us. If you send us a question or inquiry, schedule a demo, or ask for other support, you will need you to provide us with personal information (i.e., name, email address, telephone number, company, country and any content you decide to add).

We use personal information to fulfil your request for additional information or support from us. EU legal basis - When we process personal information for these purposes, we process personal information on behalf of the Customer to provide the Services. Therefore, the Customer, as data controller, is responsible for determining the legal basis.

We may also use this personal information to send you communications on Cyberbit products or offers we feel may be of interest to you (including via the Cyberbit Cloud, by email or post), such as service announcements and administrative messages and call you in relation thereto. EU legal basis - We process personal information for these purposes based on our legitimate interests in updating customers on new offers related to the Services. You can unsubscribe from these communications by contacting us at privacy@cyberbit.com or to unsubscribe link exists in the emails sent.

(g) Use Cyberbit's support services. When you are designated as a User by your organization and receive log in credentials to access the Ticketing System, we will need you to provide us with personal information (i.e., full name, email address, phone number, title, company) and the Account to which you are associated.

We use personal information to enable you to access the support services, use the Ticketing System to open and track support requests and access our knowledge base. EU legal basis - When we process personal information for these purposes, we process personal information on behalf of the Customer to provide the Services. Therefore, the Customer, as data controller, is responsible for determining the legal basis.

We may also use all the personal information described above from (a) to (g) to establish, exercise or defend Cyberbit's legal rights. EU legal basis - We process personal information for these purposes based on our legitimate interest in defending our rights and interests.

We may also use all the personal information described above from (a) to (g) to comply with legal and regulatory obligations. EU legal basis - We process personal information for these purposes based on legal and regulatory obligations to which Cyberbit is subject.

1.2 ***Personal information we collect automatically***

If you are a User, we will collect automatically the following personal information about you:

(a) Training history record - i.e. which units you performed/executed and when, performance evaluation, such as scores/grades for each unit and in a lab/ Live Fire Exercise, training duration (completion time), amount of taken hints, etc. We may also collect visual records of units - i.e. recordings of a User's browser while the User is in a unit (if such a feature is enabled by the managers or administrators of the Account). These visual records will be available only to the managers or administrators of the Account (not to other Users from your organization).

We use this personal information to enable you and the managers/administrators of the Account to keep track of your past performance; and send emails to administrators or managers detailing and analyzing the training history of users in the Account, provide the support services that you or your organization has requested and improve and optimize (i) the specific Customer's use of the Cyberbit Cloud; (ii) specific Customer's and User's experience in connection with the Cyberbit Cloud; and (iii) enhance the deployment of the Cyberbit Cloud by the specific Customer. EU legal basis – When we

process personal information for these purposes, we process personal information on behalf of the Customer to provide the Services. Therefore, the Customer, as data controller, is responsible for determining the legal basis.

We also use this personal information for Statistical and Analytical Purposes and to improve the Services and your User experience. EU legal basis - We process personal information for these purposes based on our legitimate interests to improve and secure our Services and user's experience.

(b) Per Account information: Account name, all units performed under the Account, dates, evaluation and performances of each User associated to the Account, use authorizations granted by the administrators/managers of the Account to the Users, different tags decided by the administrators/managers of the Account to Users, etc.

We use this personal information to enable you and the managers/administrators of the Account to keep track of your Account's past performance and improve and optimize (i) the specific Customer's use of the Cyberbit Cloud; (ii) specific Customer's and User's experience in connection with the Cyberbit Cloud; and (iii) enhance the deployment of the Cyberbit Cloud by the specific Customer. EU legal basis – When we process personal information for these purposes, we process personal information on behalf of the Customer to provide the Services. Therefore, the Customer, as data controller, is responsible for determining the legal basis.

We also use this personal information for Statistical and Analytical Purposes and to improve the Services and your User experience. EU legal basis - We process personal information for these purposes based on our legitimate interests to improve and secure our Services and user's experience.

We may also use all the personal information described above in (a) and (b) to establish, exercise or defend Cyberbit's legal rights. EU legal basis - We process personal information for these purposes based on our legitimate interest in defending our rights and interests.

We may also use all the personal information described above in (a) and (b) to comply with legal and regulatory obligations. EU legal basis - We process personal information for these purposes based on legal and regulatory obligations to which Cyberbit is subject.

(c) Each time you visit the Cyberbit Cloud or use our Services we may automatically collect the following internet or other electronic network activity information:

(i) Technical information, including the Internet protocol (IP) address used to connect your computer to the internet, domain name and country which requests information;

(ii) The time of approval of our terms of use of the Services by each User associated to the Account,

(iii) Information about your visit and usage, including which features of the Services you used and at what frequency you used them, grades, name of executed exercises, amount of taken hints, time and length of visits to certain pages and page interaction information (such as scrolling, clicks, and mouse-overs), application debug logs, and other communication data and information provided when requesting further service or downloads; and

(iv) Location information, which may be determined through your IP address.

To collect this information, we use cookies. Cookies are small pieces of text sent by your browser to your device. Cookies can be persistent (cookies that remain on your

device for a set period of time or until you delete them) or session (cookies that are deleted as soon as you close your browser). When you use the Services, we and our third-party providers may place a number of cookies on your device.

There are two broad categories of cookies: (i) first party cookies, served directly by us to your computer or mobile device, and (ii) third party cookies, which are served by a third party.

We use **strictly necessary cookies** as described below to authenticate Users and access the Cyberbit Cloud, prevent fraudulent use of the Cyberbit Cloud, allow the Services and its features to function properly and provide technical services. Please note that these cookies are strictly necessary for the Services to function and cannot be switched off in the systems. These cookies include:

FIRST PARTY

Host	Cookie Name	Description	Expiry Duration
login.www.cyberbitrange.com	_csrf	This cookie is used to prevent Cross-Site Request Forgery (CSRF) attacks, ensuring that each request made to the server is from the user's browser and is intentional.	9 days
login.www.cyberbitrange.com	did	This cookie name is used for device identification for attack protection and as a fallback cookie for anomaly detection on browsers that don’t support the sameSite=None attribute.	1 year.
login.www.cyberbitrange.com	_cfuvid	The _cfuvid cookie is used by Cloudflare to distinguish individual users who share the same IP address for the purpose of enforcing rate limiting rules.	Session
login.www.cyberbitrange.com	auth0_compat	This cookie name is used for single sign-on on browsers that don’t support the sameSite=None attribute and for maintaining authentication state across different pages.	2 days.
login.www.cyberbitrange.com	did_compat	This cookie name is used for attack protection fallback and anomaly detection on browsers that	1 year.

		don't support the sameSite=None attribute. It also serves as a fallback cookie for did in the event a legacy browser does not support sameSite being set to None and changes the way the server renders when the visitor returns, setting a seen cookie.	
login.www.cyberbitrange.com	auth0		2 days.

Particular third-party cookies which the Cyberbit Cloud and/or the Ticketing System currently uses include:

(a) Auth0 - We use Auto0 (https://auth0.com/) for authentication of Users. Autho0 uses various cookies on the Cyberbit Cloud in order to authenticate Users. We are not responsible for the privacy practices of Auto0 and their use of cookies. A list of Auth0 cookies stored in the browser can be found in the documentation here: https://auth0.com/docs/sessions-and-cookies/samesite-cookie-attribute-changes#browser-cookie-changes and the Auto0 privacy policy can be found here https://auth0.com/privacy.

(b) Mixpanel- We use Mixpanel (https://mixpanel.com/home) for analytics purposes for improving the Cyberbit Cloud and the user experience. Mixpanel uses various cookies in order to collect information on the User of the Cyberbit Cloud. We are not responsible for the privacy practices of Mixpanel and their use of cookies. The Mixpanel Privacy Policy can be found here: https://mixpanel.com/legal/privacy-policy/. You can also opt out of Mixpanel at any time by following the instructions available at: https://help.mixpanel.com/hc/en-us/articles/360001113426-Opt-Out-of-Tracking.

(c) Zoho – We use Zoho (https://www.zoho.com/) for providing support services to our Users. Zoho uses various cookies in the Ticketing System in order to create the User's account and to provide the platform for providing the support services. We are not responsible for the privacy practices of Zoho and their use of cookies A list of cookies used by Zoho can be found here: https://www.zoho.com/privacy/cookie-policy.html and the Zoho Privacy Policy can be found here: https://www.zoho.com/privacy.html and the Zoho Privacy Policy for California residents can be found here: https://www.zoho.com/us-ca/privacy.html.

(d) HubSpot – We use HubSpot as our customer relationship management (CRM) platform to manage our marketing, and customer communications. HubSpot may collect information, including contact information, to provide CRM services. We have disabled HubSpot's Intent Sharing and Smart Enrichment features to limit data sharing across HubSpot's network. HubSpot's use of information is governed by their Privacy Policy, available at https://legal.hubspot.com/privacy-policy.

2. **With whom do we share your personal information?**

2.1 We share your personal information as described below:

(a) With our trusted service providers and sub-contractors including customer success providers, technical, IT, hosting, logistical or administrative services providers, our communication vendors, payment processors and insurers, and government databases and verification services for the purpose of conducting security screenings, including

but not limited to the U.S. Consolidated Screening List and domain registration databases.. For example, we will share information with AWS (https://aws.amazon.com/) which hosts the Cyberbit Cloud (including the personal information processed as part of your use of it) in its servers in the United States, with User pilot (https://userpilot.com) which provide us services that help Users get more value from the Cyberbit Cloud and allows us to get Users' feedback, and with Incredible (https://www.accredible.com) which provides digital credential management services for creating, issuing, managing, and verifying digital certificates and badges.

(b) To the extent required or authorized by law, if we think it is necessary to comply with the law or if we need to do so to protect or defend our legal rights, or the rights of others (including to investigate and protect our users from fraudulent or unlawful use of the Cyberbit Cloud or Services), we will share your personal information with third parties requiring information for legal reasons or third party investigators, authorities, regulators or law enforcement bodies.

(c) Your personal information will be shared with any member of the Cyberbit Group where we consider that it is in our legitimate interests to do so for internal administrative purposes (for example, ensuring consistent and coherent delivery of services to our customers, corporate strategy, compliance, auditing and monitoring, research and development and quality assurance).

(d) Companies that assist us in our marketing, advertising and promotional activities; and

(e) Analytics providers that assist us in the improvement and optimization of the Cyberbit Cloud and process personal information in the context of provision of analytical services to us.

(f) User's personal information, as detailed in Sections 1.1.a, 1.1c, 1.1d, 1.2a,b,c, above, and the result of security screenings, will be shared with the respective Account which User is associated with, including without limitation, with the administrators and representatives of the Account. We may share such personal information by sending emails to you and to administrators or managers of the Account using SendGrid (https://sendgrid.com),

(g) Third-party tool providers (including Fortran, LLC), and relevant government authorities for the purpose of conducting security screenings and/or reporting on User screening and compliance for advanced penetration testing tools.

2.2 We will also disclose your personal information to third parties:

(a) where it is in our legitimate interests to do so to run, grow and develop our business:

(i) if we sell or buy any business or assets, we will disclose your personal information to the prospective seller or buyer of such business or assets;

(ii) if Cyberbit or substantially all of its assets are acquired by a third party, in which case personal information held by Cyberbit will be one of the transferred assets;

(b) to establish, protect, or exercise our legal rights, as required to enforce our terms of service or other contracts; to defend against legal claims or demands; to detect, investigate, prevent, or take action against illegal activities, fraud, or situations involving potential threats to the rights;

(c) to protect the rights, property or safety of the Cyberbit Group, our employees, customers, suppliers or other persons; and

(d) if we are under a duty to disclose or share your personal information in order to comply with any legal obligation, any lawful request from government or law enforcement

officials and as may be required to meet national security or law enforcement requirements or prevent illegal activity.

2.3 In the preceding twelve (12) months, we have disclosed the following categories of personal information for a business purpose: (i) we have disclosed your personal information detailed in 1.1.c above to Zoho, and the information detailed in 1.1.a and 1.1.b above to third parties that help us administer the Services, such as our support vendor, technical, IT, hosting, logistical or administrative services providers, government screening databases, professional verification services, and to Incredible to provide digital credential management services; (ii) we have disclosed your personal identifiers and internet or other electronic network activity information to our IT support and data analytics providers to detect security incidents, protect against malicious, deceptive, fraudulent, or illegal activity, and to identify and repair Cyberbit Cloud and Services errors; and (iii) we have disclosed your internet or other electronic network activity information to our IT support and data analytics providers to maintain the quality of the Cyberbit Cloud and to improve and enhance the Cyberbit Cloud and Services.

2.4 In the preceding twelve (12) months, we have shared your internet or other electronic network activity information collected via cookies and other tracking technologies with our data analytics provider, support services provider and authentication provider. Such sharing may be deemed a sale under the California Consumer Privacy Act. To opt-out of this sharing, see the instructions in **Section 1.2 above.**

2.5 DPF Onward Transfer Liability - Cyberbit remains liable under the DPF Principles if our agents process personal data received under the DPF in a manner inconsistent with the Principles, unless we can prove that we are not responsible for the event giving rise to the damage.

3. How is your personal information transferred outside of the European Economic Area ("EEA") and Israel?

3.1 The personal information will be used, stored and/or accessed by staff operating outside the EEA working for us, other members of the Cyberbit Group or third-party suppliers. These non-EEA countries include the State of Israel, where our parent company is based, the USA and India. This will be for the purposes listed in section 1 above, the provision of our Services to you or to your organization, the processing of transactions and/or the provision of support services. Further details about who we share personal information with are set out in section 2 above.

3.2 When transferring personal information outside the EEA, we will usually:

(a) in accordance with Article 45 of the General Data Protection Regulation (GDPR), ensure that the country in which your personal information will be handled (such as the State of Israel, where our ultimate parent company is based) has been deemed "adequate" by the European Commission; or

(b) in the absence of an adequacy decision, in accordance with Article 46.2 of the GDPR, include the standard contractual clauses approved by the European Commission for transferring personal information outside the EEA into our contracts with those third parties.

3.3 When transferring personal information outside the EEA, the transfer takes place on the basis of:

(a) a country declared as offering equivalent level of protection by the Israeli Privacy Protection Authority;

(b) another approved transfer mechanism under the Israeli regulations; or

(c) your consent through this privacy policy to transfer your personal information to other jurisdictions, understanding that in some countries the level of protection may be lower than in Israel.

3.4 In any case, our transfer, storage and handling of your personal information will continue to be governed by this privacy policy.

3.5 Further details on the steps we take to protect your personal information, in these cases, is available from us on request by contacting us by email at **privacy@cyberbit.com** at any time.

4. How long do we keep your personal information for?

We retain personal information for as long as we deem it as reasonably necessary in order to provide you with our Services.

We retain your personal information in accordance with our Data Retention and Records Management Policy (which can be provided upon contacting privacy@cyberbit.com), the length of time we retain your personal information depends on the purposes for which we collect and use it. Other circumstances in which we will retain your personal information for longer periods of time include: (i) as required to comply with applicable laws; (ii) to establish, exercise or defend our legal rights; or (iii) for us to have an accurate record of your interaction with us in the event of any inquiries or contact requests.

5. How do we keep your personal information secure?

5.1 We use appropriate technical and organizational measures to protect personal information against accidental or unlawful destruction or accidental loss, alteration unauthorized disclosure or access. All information that is collected through the Cyberbit Cloud and Services is processed on secure data servers located in the EU, Israel and the US. In order to keep personal information secure, we use 2 factor authentications for our administrators, run 3rd party penetration tests, use a web application firewall, update latest patches, limit administrators' access only to Cyberbit's IP address.

5.2 In the course of provision of your personal information to us, your personal information is likely to be transferred over the internet and/or stored on a cloud-based server. Although we make every effort to protect the personal information which you provide to us, the transmission of information over the internet and storage in a cloud-based server is not completely secure. As such, you acknowledge and accept that we cannot guarantee the security of your personal information transmitted to or automatically created by the Cyberbit Cloud and that any such transmission is at your own risk.

6. What rights do you have regarding your personal information?

6.1. If you wish to exercise your rights in relation to such personal information under applicable law, you may contact us at **privacy@cyberbit.com**.

6.2. **Rights of individuals in the EEA:**

If our processing of your personal information is subject to the General Data Protection Regulation (GDPR), you are entitled to request us to:

(a) access your personal information in order to confirm whether or not personal information about you is being processed; provide you with further details about how we process your personal information and provide you with a copy of any personal information which we hold about you;

(b) rectify any of your personal information in case your personal information are obsolete, inaccurate or incomplete;

(c) in certain circumstances under GDPR, delete any personal information which we hold about you;

(d) in certain circumstances under GDPR, restrict the way that we process your personal information during a limited period of time;

(e) in certain circumstances under GDPR, data portability, meaning that you can receive the personal information originally provided by you in a structured and commonly used format or that you can request the transfer of the personal information provided by you to another data controller;

(f) object to our use of your personal information when the processing is based on Cyberbit's legitimate interest. Cyberbit will no longer process your personal information unless Cyberbit demonstrates compelling legitimate grounds for the processing which override your interests, rights and freedoms, such as the respect of a legal obligation (e.g. legal obligation involving the retention of documents), or for the establishment, exercise or defense of legal claims;

(g) withdraw your consent when it has been obtained and processing is based on consent

We will consider all such requests and provide our response within a reasonable period (and in any event within any time period required by applicable law). Please note that those rights do not always apply and there are certain exceptions to them. We will also need to confirm your identity before acting on certain requests.

If you have a complaint about how we use your personal information, we would always prefer you to contact us first. However, you may also make a complaint to your local data protection authority in the EEA country where we are based or where we monitor your behavior. If you are unsure which data protection authority to contact, please contact us at **privacy@cyberbit.com**.

6.3. DPF Complaints and Recourse

In compliance with the EU-U.S. DPF and the UK Extension to the EU-U.S. DPF and the Swiss-U.S. DPF, Cyberbit commits to cooperate and comply respectively with the advice of the panel established by the EU data protection authorities (DPAs) and the UK Information Commissioner's Office (ICO) and the Swiss Federal Data Protection and Information Commissioner (FDPIC) with regard to unresolved complaints concerning our handling of personal data received in reliance on the EU-U.S. DPF and the UK Extension to the EU-U.S. DPF and the Swiss-U.S. DPF.

6.4. Binding Arbitration

Under certain conditions, individuals may invoke binding arbitration for complaints regarding DPF compliance not resolved by other recourse mechanisms. This arbitration option is available by delivering notice to Cyberbit and following the procedures and subject to conditions set forth in Annex I of the DPF Principles.

6.5. Rights of California Residents:

If our processing of your personal information is subject to the California Consumer Privacy Act, as amended by the California Privacy Rights Act of 2020 (together, "CCPA") you are entitled to the following rights:

(a) Right to Access. You have the right to request what personal information we have collected, used, disclosed, and sold about you within the preceding twelve (12) months and to request a copy of the specific pieces of personal information that we maintain about you.

(b) Right to Deletion. You have the right to request the deletion of your personal information that we collect or maintain, subject to certain exceptions.

(c) Right to Opt-Out. You have the right to opt-out of the "sale" or "sharing" of your personal information to third parties. Cyberbit Group does not have actual knowledge that it sells personal information of minors under the age of sixteen (16) years.

(d) Right to Non-Discrimination. You have the right to not receive discriminatory treatment if and when you exercise your rights to access, delete, or opt-out under the CCPA.

(e) Right to Correct. You have the right to request the correction of your inaccurate personal information.

(f) Right to Information About Disclosures of Personal Data for Direct Marketing Purposes. Under applicable law. California consumers can request information from us about whether we have disclosed personal information to any third parties for the third parties' direct marketing purposes. We will not sell your personal information with, or disclose it to, third-party companies for their direct marketing purposes without your consent.

(g) Right to Limit the Use or Disclosure of Sensitive Personal Information ("**SPI**"). Under certain circumstances, to the extent we use or disclose SPI, you have the right to limit the use or disclosure of SPI.

To exercise such rights regarding your personal information, you may submit a request by email to: privacy@cyberbit.com. You may only make a request for access twice within a 12-month period. To opt-out of the sale of your information via cookies, please follow the instructions in **Section 1.2**.

For requests submitted via telephone or email, you must provide us with sufficient information that allows us to reasonably verify you are the person about whom we collected the personal information and describe your request with sufficient detail to allow us to properly evaluate and respond to it. If we are not able to verify your identity for access and deletion requests with the information provided, we may ask you for additional pieces of information. Any information that is sent to you in response to your request, will be encrypted.

Only you, or a person registered with the California Secretary of State that you authorize to act on your behalf, may make a request related to your personal information. If you are an authorized agent making a request on behalf of another individual, you must provide us with signed documentation that you are authorized to act on behalf of that individual.

7. Does this privacy policy apply to third party links?

You may, during your use of the Services, access links to or other websites operated by third parties outside of the Cyberbit Group. Please note that this privacy policy only applies to the personal information that we (or third parties on our behalf or any other member of the Cyberbit Group) collect from or about you and we cannot be responsible for personal information collected and stored by third parties. Third party websites have their own terms and conditions and privacy policies, and you should read these carefully before you submit any personal information to these websites. We do not endorse or otherwise accept any responsibility or liability for the content of such third-party websites or third-party terms and conditions or policies.

8. How do we approach changes to this privacy policy?

We will change this privacy policy from time to time. Any changes we make to our privacy policy in the future will be posted on this page and, if we have your e-mail address, we may also, notify you by email. If we make changes that materially affect your privacy rights, we will notify you by email or posting on the Cyberbit Cloud main page.

9. **Do we respond to Do Not Track?**

We do not support Do Not Track (DNT). Do Not Track is a preference you can set in your web browser to inform websites that you do not want to be tracked. You can enable or disable Do Not Track by visiting the Preferences or Settings page of your web browser.

10. **Contact us and data controllers' details**

If you have any comments or questions regarding this Privacy Policy or the information practices in connection with the Services or personal information that Cyberbit processes as data controller, please contact us at:

By Postal Mail:

Cyberbit Ltd.

22 Zarchin St., P.O.Box 4410, Ra'anana 4366241, Israel

By Email:

privacy@cyberbit.com.

If you have questions regarding personal information that Cyberbit processes on behalf of your organization for the provision of Cyberbit's Services, please contact your organization directly which is the relevant data controller.

The practices described in this privacy policy statement are current personal information protection policies, as of June 26, 2025.

Last updated as of December 9, 2025