CYBERBIT DATA PROCESSING ADDENDUM

(with EU Standard Contractual Clauses)

This Data Processing Addendum (together with it Annexes, the "Addendum") is between Cyberbit and Customer (as such terms are defined in the Terms of Use, each a "party" and together the "parties"). This Addendum is attached to the Terms of Use between Cyberbit and Customer as an integral part thereof and is applicable only if and to the extent that Applicable Data Protection Laws apply to the Processing of any Personal Data by Cyberbit for Customer in relation to the Services ("**Customer Personal Data**"). If and to the extent that this Addendum conflicts with any provision of the Terms of Use, then this Addendum will prevail to the extent of such conflict. Users are not a party to this Addendum nor third party beneficiaries. All capitalized terms not defined herein shall have the meanings ascribed to them in the Terms of Use.

1. **Definitions.** When used in this DPA, the following terms have the meaning ascribed next to them:

1.1. "**Applicable Data Protection Laws**" means the General Data Protection Regulation 2016/679 ("**GDPR**" or "**EU GDPR**") and applicable EU Member State laws implementing or supplementing the GDPR; the Data Protection Act 2018 and the UK General Data Protection Regulation ("**UK GDPR**"); each as amended or replaced from time to time, and to the extent applicable.

1.2. **"Personal Data"**, **"Process/Processing"**, **"Controller"**, **"Processor",** "**Supervisory Authority**", "**Special Categories of Data**" and **"Data Subjects"** shall have the meanings given to them in Applicable Data Protection Law.

1.3. "**Customer Personal Data**" means any Personal Data provided to Cyberbit by the Customer (and its respective Users) in connection with the Services or uploaded to the Services by the Customer (and its respective Users).

1.4. "**Cyberbit Subprocessor(s)**" means any person or entity appointed by or on behalf of Cyberbit to Process Personal Data in connection with the Services, excluding any employee of Cyberbit or its Affiliates. The list of Cyberbit Subprocessors is detailed in Annex III attached hereto.

1.5. "**Government Authority Request**" means any subpoena, warrant or other judicial, regulatory, governmental or administrative order by a government or quasi-governmental or other regulatory authority (including law enforcement or intelligence agencies) seeking or requiring access to or disclosure of Personal Data.

1.6. "**Personal Data Breach**" means a breach of security by Cyberbit leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure or use of, or access to, Customer Personal Data processed by Cyberbit.

1.7. "**Personnel**" shall mean employees, subcontractors or freelance consultants employed by the relevant Party or its Affiliates.

1.8. The following terms shall have the meaning ascribed to them in the Terms of Use: "**Affiliate**", "**Customer**", "**Cyberbit**", "**License Term**", "**User**", "**Services**".

2. **Processing of Personal Data and Parties' Obligations.**

2.1. Each party agrees to comply with the obligations that apply to it under Applicable Data Protection Laws. The Customer is the Controller and Cyberbit is the Processor with respect to the Personal Data processed pursuant to the Services.

2.2. Customer hereby represents that:

2.2.1. The Customer Personal Data provided to Cyberbit pursuant to the Terms of Use was obtained and is provided to Cyberbit lawfully, in accordance with all requirements of Applicable Laws.

2.2.2. There is a documented legal basis for the Processing of Customer Personal Data by Customer and by Cyberbit, respectively and all required privacy notices have been provided by Customer to Users.

2.2.3. If and to the extent that any Customer Personal Data originating from the EEA is provided by Customer to Cyberbit (and not transferred directly by a User to Cyberbit), then Customer will be responsible to notify such Users of the following information, as required by the data protection law applicable to Cyberbit:

2.2.3.1. The Customer Personal Data will be maintained in a database, the controller of which is Cyberbit Ltd., of 22 Zarchin St., Israel and the contact information for any privacy matters is: privacy@cyberbit.com.

2.2.3.2. Details on the purpose of transfer of the Personal Data and types of Personal Data which was transferred, are listed in Sections 2 and 3 of Annex I to the DPA.

2.2.3.3. Users have a right to (1) request deletion of their Personal Data in one of the following cases: (i) the data was created, obtained, accrued or collected in contravention of the provisions of any law, or that the further use of the data is in violation of the law; or (ii) the data is no longer necessary for the purposes for which it was created, obtained, accrued or collected; (2) access their Personal Data, and (3) request the correction of their Personal Data if it is not correct, complete, clear or up to date. These rights are subject to certain exceptions prescribed by applicable law.

2.2.3.4. Cyberbit may transfer the Personal Data to the Cyberbit Subprocessors in accordance with the provisions of this DPA.

2.2.3.5. In the event a User (i) wishes to delete its Personal Data, or (ii) discovers that any Personal Data is not correct, complete, clear or up to date; User should contact Customer who will, if needed, receive reasonable assistance from Cyberbit.

3. **Processing of Customer Personal Data**

3.1. Cyberbit shall Process Customer Personal Data on Customer's behalf and according to the Customer's lawful written instructions which are hereby provided: (i) Processing for Use of the Services and for collecting analytics for Product improvement; and (ii) improving and optimizing (a) the specific Customer's Use of the Product; (b) specific Customer's and User's experience in connection with the Product; and (c) enhance the deployment of the Product for the specific Customer; and (d) the Services and User's experience.

3.2. The Terms of Use and this DPA shall consist the entirety of the Customer's written Instructions in relation to the Processing with which Cyberbit is required to comply.

3.3. Cyberbit may create de-identified and anonymous data from the Customer Personal Data and process it for an unlimited period of time for improving the Product and/or Services and/or the User's experience and for statistical and analytical purposes, as more fully described in the Terms of Use.

3.4. Customer sets forth the details of the Processing of Customer Personal Data, as required by Article 28(3) of the GDPR in **Annex I** (Details of Processing of Customer Personal Data), attached hereto.

3.5. If Cyberbit receives a Government Authority Request concerning Customer Personal Data, Cyberbit shall: (i) To the fullest extent permitted by law, without undue delay, notify Customer in writing of such Government Authority Request so that Customer may contest or seek to narrow such disclosure or seek a protective order or other appropriate remedy; (ii) reasonably cooperate with and take reasonable steps to assist Customer in its efforts under (i) above; (iii) Where any attempt under (i) above is not successful and some or all of the Customer Personal Data is required to be disclosed, Cyberbit shall take reasonable steps to furnish only the minimum amount of Personal Data legally required to be disclosed; (iv) Cyberbit shall maintain a written record of all Government Authority Requests.

4. **Cyberbit's Personnel; Subprocessors**

4.1. Cyberbit shall ensure that access to the Customer Personal Data by its Personnel is limited to a need to know and/or access basis, and that all such Personnel receiving such access to and/or Processing the Customer Personal Data, are subject to written confidentiality undertakings or statutory obligations of confidentiality.

4.2. Customer consents to Cyberbit engaging Cyberbit Affiliates and Cyberbit Subprocessors to process Customer Personal Data for the provision of the Services. Cyberbit will notify Customer before replacing or adding new Subprocessors.

In the event Customer objects to such new Subprocessors due to reasonable grounds relating to data protection, it may notify Cyberbit of its objection and reasons therefore, during 15 days from Cyberbit's notification. Thereafter, for an additional period of 15 days, the Parties shall attempt to reach an amicable solution with respect to the utilization of such new Subprocessor. Absent such solution, Customer may, during an additional period of 15 days, terminate the Purchase Order with Cyberbit, and Cyberbit shall refund Customer (or the respective Partner) for any prepaid amounts for the terminated period of the Services.

4.3. Cyberbit will enter into appropriate data processing agreements with its Subprocessors.

4.4. To the extent Cyberbit processes any Customer Personal Data originating from the EEA in a country that has not been designated by the European Commission or the UK, as applicable, as providing an adequate level of protection for Personal Data, the Personal Data shall be deemed to have adequate protection by virtue of any one of the transfer mechanisms consistent with the requirements of EU or UK Applicable Law, as applicable, which will be implemented by Cyberbit.

4.5. In the absence of an adequacy decision and in case the EU GDPR applies:

4.5.1. For the purpose of this DPA, the Parties agree that the standard contractual clauses for Controller to Processor (Module 2) as approved by the European Commission Implementing Decision (EU) 2021/914 of 4 June 2021, including all Annexes thereto, as may be amended or replaced from time to time ("SCC") are incorporated herein by reference and the Parties are deemed to have accepted and signed the SCC where necessary in their entirety. For all intents and purposes, Annexes I to III of this DPA, shall be deemed to be Annexes I-III of the SCC.

4.5.2. The Parties agree that with respect to the election of specific terms and/or optional clauses required by the SCC the following shall apply and any optional clauses not expressly selected are not included: (i) if and to the extent the SCC conflict with any provision of this DPA, the SCC will prevail to the extent of such conflict; and (ii) Clause 7 of the SCC is opted out; (iii) In Clause 9 of the SCC option 2 (general written authorization) will apply, the authorization period will be 15 days, the agreed sub processor(s) list is attached as Annex III to this DPA and notification regarding changes to this list shall be provided in accordance with the provisions of this Section 4 above; (iv) In Clause 11 of the SCC the optional language will not apply; (v) In Clause 17 of the SCC, the governing law will be Irish law; (vi) In Clause 18 of the SCC disputes shall be resolved by the courts of Ireland. (vii) In Annex I of the SCC Customer is the 'Data exporter', Cyberbit is the 'Data importer'; The competent supervisory authority is the Irish DPC.

4.6. In the absence of an adequacy decision and in case the UK GDPR applies:

4.6.1. For the purpose of this DPA, the Parties agree that International Data Transfer Addendum to the EU Commission Standard Contractual Clauses as approved by the Information Commissioner's Office (ICO) under S119A(1) Data Protection Act 2018 and in force as of March 21, 2022, as may be amended or replaced from time to time ("**UK Addendum**"), are incorporated herein by reference and the Parties are deemed to have accepted and signed the UK Addendum where necessary in their entirety. For all intents and purposes, Annexes I to III of this DPA, shall be deemed to be Annexes I-III of the UK Addendum.

4.6.2. The Parties agree that with respect to the election of specific terms and/or optional clauses required by the UK Addendum the following shall apply and any optional clauses not expressly selected are not included: In Part 1: Tables – (i) Table 1: Parties – Start date is the start date of the License Term; as between the Parties, Cyberbit will be deemed the "data exporter" and Customer will be deemed the "data importer"; (ii) Table 2: Selected SCCs, Modules and Selected Clauses: the box "the version of the Approved EU SCCs which this Addendum is appended to, detailed below, including the Appendix Information" is checked and the date is the start date of the License Term; (iii) Table 3: Appendix Information - Annex 1A: List of Parties: the Cyberbit and Customer as set out in the Agreement; Annex 1B: Description of Transfer: as set out at **Annex I** of the SCCs; Annex II: Technical and organizational measures including technical and organizational measures to ensure the security of the data: as set out at **Annex II** to the SCCs; **Annex III**: List of Sub processors (Modules 2); (iv) Table 4: Ending this Addendum when the Approved Addendum Changes – the boxes "Importer" and "Exporter" are checked; Part 2: Mandatory Clauses is applicable.

5. **Technical and Organizational Measures**

5.1. Cyberbit shall implement and maintain appropriate technical and organizational measures to ensure a level of security of the Customer Personal Data appropriate to the risk, taking into account the nature, scope and context of the Processing and the costs of implementation. The major information security measures currently implemented by Cyberbit are listed in Annex II hereto, as may be updated from time to time, provided the level of security is not materially degraded.

5.2. Customer shall not upload to the Services Special Categories of Personal Data and Customer is aware that the security of the Services is not adapted to Special Categories of Personal Data.

6. **Personal Data Breach**

6.1. Cyberbit shall promptly and without undue delay notify Customer in writing upon becoming aware of a Personal Data Breach. Notification to the Customer of a Personal Data Breach shall not constitute admitting to any fault or liability with respect to such breach. Any notification to Supervisory Authorities or Data Subjects, if required, will be the responsibility of the Customer.

6.2. Cyberbit shall reasonably assist the Customer with providing available information in Cyberbit's possession relating to a Personal Data Breach.

6.3. The Customer shall not issue any public statement regarding the Personal Data Breach without coordinating with Cyberbit and obtaining its approval, unless required by the Applicable Data Protection Laws.

6.4. If the investigation of the Personal Data Breach raises any security issues to be remediated by Cyberbit, Cyberbit shall implement reasonable industry standard measures for such remediation at Cyberbit's sole discretion.

7. **Data Subject Rights, Data Protection Impact Assessment and Prior Consultation**

7.1. At Customer's request, Cyberbit shall provide commercially reasonable assistance to Customer to comply with (i) any of Customer's obligations under the Applicable Data Protection Laws concerning Customer's Data Subjects' requests to exercise their rights including requests to delete their Personal Data; and (ii) any data protection impact assessments or prior consultations with the Supervisory Authorities or other competent data privacy authorities, related to the Processing activities conducted by Cyberbit.

8. **Retention, Deletion or Return of Customer Personal Data**

8.1. Within 30 days of the end of the License Term or earlier at Customer's written request and to the extent commercially reasonable, Cyberbit shall promptly delete, return, or destroy all copies of any Customer Personal Data, provided they are not required to perform the Services, and unless required to retain such Personal Data under applicable law. Customer hereby agrees that Cyberbit may retain a copy of the Customer Personal Data for a period of 7 years following the termination of the Processing, to establish, exercise, or defend legal claims, provided that such copy of the Customer Personal Data, will be under strict access authorizations.

8.2. To the extent deletion of the Customer Personal Data requires disproportionate effort, Cyberbit shall make best efforts to segregate and secure the non-active Customer Personal Data, such that it cannot be processed; and ensure that it may be accessed only by the minimum necessary number of authorized Personnel solely if required for internal administrative purposes such as data management, compliance and data security.

9. **Inspection and Audit Rights**

9.1. Cyberbit shall, subject to a 30 days' prior written notice and advance coordination, reasonably cooperate with audits or inspections (the "**Audit**") conducted by Customer or any independent third party appointed by the Customer for conducting such audit, provided such third party is not a competitor of Cyberbit (the Customer or its appointee shall be referred to as the "**Auditor**"). The Audit shall be limited to verifying Cyberbit's compliance with this DPA regarding the Processing of Customer Personal Data by Cyberbit under this DPA. Audits will not be conducted more than once annually except in the event of a Personal Data Breach.

9.2. Cyberbit shall make commercially reasonable efforts to provide the Auditor with materials and information requested by the Auditor which are necessary for the purpose of the Audit and which are available to Cyberbit.

9.3. Cyberbit's cooperation with any such Audit shall be subject to the following conditions: (i) The Auditor shall sign, prior to the Audit, a confidentiality undertaking covering all information which the Auditor and/or its personnel may have access to in performance of the Audit; (ii) the Audit shall be conducted at

Cyberbit's normal working hours; (iii) the Auditor's personnel shall abide by the security policies and procedures of Cyberbit and conduct the Audit with minimal disturbance to Cyberbit's operations and business; (iv) the Audit shall be conducted solely in premises under the direct control of Cyberbit in which the Customer Personal Data is stored. In relation to the Cyberbit Subprocessors, Cyberbit may provide only the information received from such Subprocessors, subject to confidentiality obligations Cyberbit may have towards such Subprocessors.

9.4. Cyberbit may satisfy its obligations under this Section by answering Customer's security questionnaire or by providing Customer with attestations, certifications and summaries of audit reports conducted by third party auditors.

9.5. Cyberbit shall be entitled to take any reasonable precautions at its sole discretion to prevent disclosure of: (i) other Customers' Personal Data and confidential or proprietary information; (ii) Cyberbit's internal financial information; (iii) Cyberbit's trade secrets; (iv) any information that in Cyberbit's sole discretion, could compromise the security of any of Cyberbit's systems or premises or cause Cyberbit to breach obligations under any applicable laws or its obligations to any third party.

10. **Information processed as independent Controllers**

10.1. Each Party shall Process the contact details of the other Party's Personnel tasked with the administration of the Services as an independent Controller. With respect to such Personal Data, each Party shall be responsible to fulfil all of its obligations under the Applicable Data Protection Laws and shall cooperate with the other party as reasonably necessary to assist with the fulfilment of the other Party's obligations under the Applicable Data Protection Laws.

11. **Term**

11.1. This DPA shall terminate automatically upon the termination or expiration of the License Term, provided however, that Cyberbit's obligations under this DPA will remain in force for as long as Cyberbit processes Customer Personal Data.

Last updated: October 20, 2024

Annex I to the DPA

Details of Processing of Customer Personal Data

This **Annex I** includes certain details of the Processing of Customer Personal Data as required by Article 28(3) of the GDPR.

1. **Subject matter and duration of the Processing of Customer Personal Data:**

   Performance of the Services for the duration of the License Term

2. **The nature and purpose of the Processing of Customer's Personal Data:**

   Provision of the Services as detailed in the Terms of Use and (i) collecting analytics for Product improvement; and (ii) improving and optimizing (a) the specific Customer's Use of the Product; (b) specific Customer's and User's experience in connection with the Product; and (c) enhance the deployment of the Product for the specific Customer; and (d) the Services and User's experience.

3. **The types of Customer Personal Data to be Processed are as follows:**

   The Personal Data relating to Customer Data Subjects is provided by the Customer and may include Personal Data collected directly from Customer Data Subjects and/or automatically generated as Customer Data Subjects' use the Services, as follows:

   Customer Personal Data: Training history and records, professional background, username, email, password, contact information, position, IP address, usage data (e.g., Browser, Operating System, Search Keyword, Last Seen), Member ID in (ISC)2 (for CPE credits), User score, User level.

4. **The categories of Data Subjects to whom the Customer's Personal Data relates to are as follows:**

   Categories of Data Subjects: Customer's representatives and Users of the Product designated by the Customer.

5. **Duration of Processing:**

   During the License Term and 30 days thereafter

6. **Subprocessor's processing:** see Annex III

Annex II to the DPA

Technical and Organizational Measures

1. Information Security Management System

1.1. Industry security standards. Cyberbit implements and operates information security in accordance with ISO 27001.

1.2. Review of information security. Cyberbit's information security management system (i.e., control objectives, controls, policies, processes, and procedures) are reviewed on an annual basis by appropriate external assessors.

2. Organization of Information Security

2.1. Security Roles and Responsibilities. Cyberbit defines and allocates information security responsibilities in accordance with approved policies for information security. Such policies are published and communicated to employees and relevant external parties required to comply with such policies.

2.2. Cyberbit maintains a team of dedicated data security Personnel responsible for maintaining industry standard infrastructure security controls.

3. Data and record security

3.1. Logical Separation of data. Customer's Personal Data is logically separated based on individual tenants for other customers.

3.2. Data Encryption. Cyberbit employs encryption at rest and transit of Customer's Personal Data. Data at rest encryption is performed with AES256 and encryption in transit is performed using TLS 1.2 or higher.

4. Personnel Access Controls

4.1. Authorization. Cyberbit restricts access to Customers' Personal Data only to Personnel whose access is necessary for performing the Services and any other obligations to the Customer.

4.2. Least Privilege user accounts. Cyberbit creates and deletes user accounts with appropriate approval based on Least Privilege principles.

4.3. Need-to-know-Access. Cyberbit will not access the Customers' Personal Data for any purpose other than as necessary to perform its obligations to Customer.

4.4. Multifactor Authentication. Cyberbit uses multi-factor authentication and encrypted channels for all administrative account access.

5. Communications Security, Transfer and Decommissioning

5.1. Web Application Firewall (WAF). Cyberbit has deployed appropriate WAF to protect all services exposed to the internet.

6. Penetration Testing

6.1. Penetration Testing. Cyberbit performs annual penetration tests on its external perimeter network by a 3rd party vendor.

7. Management of Information Security Incidents and Improvements

7.1. Reporting Information Security Incident. Cyberbit implements procedures for Personal Data Breach incidents to be reported through appropriate management channels as quickly as reasonably possible. Such a report will be sent up to 72 from the confirmed breach.

Annex III to the DPA

List of Sub-processors

Subprocessor's Name	***Services***	***Location***
Amazon Web Services	Hosting of the Services.	US
Auth0	Authentication of Users.	US
Mixpanel	Analytics purposes for improving the Cyberbit Cloud and the User experience.	Netherlands
Zoho	Providing support and chat services to our Users.	US
User Pilot	Online User guides, assistance in navigating the Cyberbit Cloud, and getting Users' feedback.	France
Sendgrid	Sending emails to Users and to administrators or managers of the Account.	US
ISC(2)	Enables Users to obtain CPE Credits (optional at User's choice).	US
Vitally	Customer success management platform	US

Annex IV to the DPA

CPRA Provisions

This Annex shall apply only if and to the extent that Customer has Users that are California residents and in relation to their Personal Information. Users are not a party to this Addendum nor are they third party beneficiaries. All capitalized terms not defined herein shall have the meanings ascribed to them in the Terms of Use or the Addendum.

This Annex shall apply to "Personal Information" of a "Consumer" as those terms are defined under the California Consumer Privacy Act of 2018, including as modified by the California Privacy Rights Act of 2020 (together "**CPRA**"), that Cyberbit processes in the course of providing Customer the Services under the Terms of Use. This Annex overrides any conflicting terms in the Terms of Use and the Addendum only with respect to Personal Information of California residents.

1. **Customer's Role.** The Customer is a Business (as such term is defined under CPRA), and as such Customer determines the purpose and means of processing Personal Information. Customer will disclose Personal Information to Cyberbit solely for the limited and specified business purpose of Cyberbit performing the Services (including without limitation, analytics for Product improvement), as described in this Annex.

2. **Cyberbit's Role**. Cyberbit is a Service Provider (as such term is defined under CPRA), and as such Cyberbit shall provide the Services and process any Personal Information in accordance with the Terms of Use. Cyberbit may not retain, use, or disclose Personal Information for any purpose other than for providing the Services (including without limitation, analytics for Product improvement) and performing the Terms of Use.

3. **Processing of Personal Information, Transfers and Sales**.

   3.1. Cyberbit will refrain from taking any action that would cause any transfers of Personal Information to or from Cyberbit which qualifies as "selling personal information" or "sharing personal information" as those terms are defined under the CPRA.

   3.2. Except as permitted by CPRA, Cyberbit will not combine Personal Information that Cyberbit receives from, or on behalf of a Consumer, or which Cyberbit collects from its own interaction with a Consumer with that of another person.

   3.3. Cyberbit will ensure that its Personnel are subject to a duty of confidentiality with respect to Personal Information, either by a written agreement or by a statutory duty of confidentiality.

   3.4. Customer will not transfer and/or disclose "sensitive personal information" (as defined in the CPRA) to Cyberbit, unless (i) it has expressly notified Cyberbit in writing of such anticipated transfer or disclosure; and (ii) provided Cyberbit specific instructions regarding such sensitive personal information, and in such a case, Cyberbit will not retain or use such sensitive personal information other than in accordance with such instructions.

   3.5. Cyberbit will make available, upon Customer's reasonable request, all information in its possession reasonably necessary to demonstrate compliance with the CPRA.

4. **Cyberbit Subprocessors**. Notwithstanding the restrictions in Section 3, Customer agrees that Cyberbit may engage the Cyberbit Subprocessors, to assist in providing the Services to Customer. A list of the Cyberbit Subprocessors can be found in the Annex III of the Addendum, provided always that such engagement shall be subject to a written contract binding each such Cyberbit Subprocessor to terms no less protective than those contained within this Annex and as is required by CPRA, as applicable. Cyberbit shall notify Customer of any such new Cyberbit Subprocessor before Cyberbit discloses any Personal Information to it.

5. **Security**. Cyberbit will use commercially reasonable security procedures that are reasonably designed to maintain an industry-standard level of security, and to prevent unauthorized access and/or disclosure of

Personal Information. An outline of Cyberbit's minimum security procedures can be found in Annex II of the Addendum.

6. **Retention**. Cyberbit will retain Personal Information only for as long as it is providing Services to the Customer, or as required by applicable laws. Within 30 days from the termination of the Services, or upon Customer's written request, Cyberbit will either destroy or return Personal Information to the Customer, unless legal obligations require storage of the Personal Information.

7. **Breach of Personal Information.** Cyberbit will notify Customer promptly upon discovery of unauthorized access to or use of Personal Information and take reasonable steps to stop or remediate the unauthorized use of Personal Information.

8. **Consumer Rights Requests**. Cyberbit shall reasonably cooperate with Customer in responding to verifiable Consumer requests, including deleting Personal Information or enabling Customer to do so, and requesting Cyberbit's Subprocessors to delete the Personal Information.

9. **Assistance with Consumers' Rights Requests**. If Cyberbit, directly or indirectly, receives a request submitted by a Consumer to exercise a right it has under CPRA in relation to that Consumer's Personal Information, it will provide a copy of the request to the Customer. The Customer will be responsible for handling and communicating with Consumers in relation to such requests.

10. **Inability To Comply With CPRA**. Cyberbit will notify Customer no later than (10) ten business days after Cyberbit determines that it no longer can meet its obligations under this Annex or the CPRA. Upon receipt of any such notice, Customer may either (i) take reasonable and appropriate steps to stop and remediate any unauthorized use of Personal Information, or (ii) terminate the Services and the Terms of Use and as its sole remedy, receive a refund of any prepaid fees paid for the terminated part of the License Term.

Last updated: Oct 20, 2024