DATA PROCESSING ADDENDUM

(with EU Standard Contractual Clauses)

This Data Processing DPA (together with it Annexes, the "**DPA**") is between Company and Customer (as such terms are defined below, each a "**Party**" and together the "**Parties**")DPA and forms part of the Terms of Use available at https://www.cyberbit.com/legal/ or other written or electronic agreement between Company and Customer (each as applicable, the "**Terms of Use**") as an integral part thereof, provided that this DPA is applicable only if and to the extent that Applicable Data Protection Laws apply to the Processing of any Personal Data by Company for Customer in relation to the Services ("**Customer Personal Data**"). If and to the extent that this DPA conflicts with any provision of the Terms of Use, then this DPA will prevail to the extent of such conflict. Users are not a party to this DPA nor third party beneficiaries. All capitalized terms not defined herein shall have the meanings ascribed to them in the Terms of Use.

Throughout this DPA, references to "**Company**" shall mean the entity which Customer has contracted with for the Services (including Cyberbit Ltd., Cyberbit, Inc., RangeForce Inc., RangeForce OÜ, or their respective Affiliates).

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

1.1. "**Affiliate**" means, with respect to either Party, any entity that directly, or through one or more intermediaries, Controls, is Controlled by, or is under common control with a Party, where "Control" means the ownership of at least fifty percent (50%) of such company's or entity's share capital or the power to direct or cause the direction of the management of such company or entity, through contract, ownership of securities, or otherwise;

1.2. "**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.

1.3. "**Customer**" means the person or entity which contracted for the Services from the Company through a Purchase Order.

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

1.5. "**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. "**License Term**" means the period of time during which the license for the Services is effective, as specified in the applicable Purchase Order.

1.7. **"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.

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

1.9. "**Personnel**" shall mean employees, directors, officers, subcontractors or freelance consultants employed by the relevant party or its Affiliates.

1.10. "**Purchase Order**" means an applicable agreement or purchase order, sales order, order form, or other ordering document between Company and Customer for purchase of (inter alia) the Services.

1.11. "**Services**" means the cyber security training, simulation and skill development software-as-a-service products and services provided by Company, including but not limited to Cyberbit Cloud and RangeForce Software, as described in the applicable Purchase Order.

1.12. "**Subprocessor(s)**" means any person or entity appointed by or on behalf of Company or its Affiliates to Process Personal Data in connection with the Services, excluding any employee of Company, or its respective Affiliates.

1.13. "**User**" means a user or administrator which is using the 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 Company 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 Company pursuant to the Terms of Use was obtained and is provided to Company 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 Company, 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 European Economic Area (EEA) is provided by Customer to Company (and not transferred directly by a User to Company), then Customer will be responsible to notify such Users of the following information, as required by the data protection law applicable to Company:

2.2.3.1. The Customer Personal Data will be processed by the Company which maintain the following physical addresses: (i) Cyberbit, Inc. of 2810 N Church St, PMB 484469, Wilmington, Delaware 19802-4447 USA; (ii) Cyberbit Ltd. of 22 Zarchin St. Ra'anana 4310602, Israel; (iii) RangeForce, Inc. of 440 Monticello Avenue Suite 1802, Norfolk, VA, USA; and (iv) RangeForce OÜ of Harju maakond, Tallinn, Pirita linnaosa, Kuslapuu tn 11, 12012, Estonia.

2.2.3.2. The contact information for any privacy matters is: privacy@cyberbit.com. Company may modify these addresses at any time upon notice to Customer Personal Data.

2.2.3.3. 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.

2.2.3.4. 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.

2.2.3.5. Company may transfer the Personal Data to the Subprocessors in accordance with the provisions of this DPA.

2.2.3.6. 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 Company.

3. **Processing of Customer Personal Data**

3.1. Company 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; (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 of the entirety of the Customer's written Instructions in relation to the Processing with which Company is required to comply.

3.3. Company 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. Data that has been de-identified at the Customer and individual level will no longer be deemed to be Customer Data.

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 Company receives a Government Authority Request concerning Customer Personal Data, Company 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, Company shall take reasonable steps to furnish only the minimum amount of Personal Data legally required to be disclosed; (iv) Company shall maintain a written record of all Government Authority Requests.

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

4.1. Company 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 Company engaging Company Affiliates and Subprocessors to process Customer Personal Data for the provision of the Services. The Subprocessors applicable to Customer are those designated in Annex III, as applicable to the Services that Customer accesses.

4.3. Company will notify Customer before replacing or adding new Subprocessors to its respective list in Annex III. Such notification may be provided via email (using the email contact provided by Customer) or via the platform through which Customer accesses the Services.

If Customer objects to a new Subprocessor on reasonable grounds relating to data protection, Customer shall notify Company in writing within fifteen (15) days of Company's notification, specifying the reasons for the objection. The Parties shall discuss the objection in good faith for a further fifteen (15) days. If no resolution is reached, Customer's sole and exclusive remedy shall be to terminate, on written notice to Company, only the specific Service that cannot reasonably be provided without the objected-to Subprocessor.

4.4. Company will enter into appropriate data processing agreements with its Subprocessors.

4.5. To the extent Company 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 Company.

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

4.6.1. 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.

4.6.2. 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', Company is the 'Data importer'; The competent supervisory authority is the Irish DPC.

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

4.7.1. 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.

4.7.2. 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, Company will be deemed the "data importer" and Customer will be deemed the "data exporter"; (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 Company 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. Company 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 Company 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 Special Categories of Personal Data to the Services 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. Company shall notify Customer in writing without undue delay after confirming a Personal Data Breach affecting Customer Personal Data. Such notification shall not constitute an acknowledgment or admission of fault, liability, or wrongdoing by Company. Any notifications to Supervisory Authorities, Data Subjects, or other third parties shall be the sole responsibility of Customer.

6.2. Taking into account the nature of the Processing and the information available to Company, Company shall provide reasonable assistance to Customer with information in Company's possession that is reasonably necessary to enable Customer to meet its notification obligations under Applicable Data Protection Laws in respect of a Personal Data Breach.

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

6.4. If the investigation of a Personal Data Breach identifies remediation reasonably required to be undertaken by Company, Company shall implement commercially reasonable, industry-standard remediation measures, with the selection and timing of such measures determined by Company in its reasonable discretion.

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

7.1. Taking into account the nature of the Processing and the information available to Company, and at Customer's sole cost and expense, Company shall provide commercially reasonable assistance to Customer in complying with (i) Data Subjects' requests to exercise their rights under Applicable Data Protection Laws, to the extent Customer is unable to address such requests through the self-service functionality of the Services; and (ii) data protection impact assessments or prior consultations with Supervisory Authorities, in each case solely with respect to the Processing activities conducted by Company on Customer's behalf.

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

8.1. Within sixty (60) days following the end of the License Term, Company shall, at Customer's written election made prior to the end of the License Term, delete or return Customer Personal Data, except (i)

to the extent retention is required by applicable law, (ii) as necessary for the establishment, exercise, or defense of legal claims, and (iii) with respect to Customer Personal Data residing in routine backups, disaster recovery systems, or archival storage in the ordinary course of business, which shall be deleted or overwritten in accordance with Company's standard retention practices. Customer agrees that Company may retain Customer Personal Data for up to seven (7) years following termination for the purposes described above, subject to the confidentiality and security obligations of this DPA.

8.2. To the extent deletion of the Customer Personal Data requires disproportionate effort, Company 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. Subject to thirty (30) days' prior written notice and advance scheduling agreed in writing by Company, and at Customer's sole cost and expense, Company shall reasonably cooperate with audits (the "**Audit**") conducted by Customer or by an independent third party appointed by Customer that (a) is not a competitor of Company, and (b) has executed a confidentiality agreement reasonably acceptable to Company (Customer or its appointee, the "**Auditor**"). The Audit shall be limited to verifying Company's compliance with this DPA in respect of the Processing of Customer Personal Data, and shall not include access to other customers' data, Company source code, or Company's internal financial information. Audits shall be conducted no more than once in any twelve (12) month period, except where specifically required by a Supervisory Authority following a confirmed Personal Data Breach materially affecting Customer Personal Data.

9.2. Company 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 Company.

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

9.4. Company may, at its election, satisfy its obligations under this Section 8 by responding to Customer's reasonable security questionnaire or by providing Customer with attestations, certifications (e.g., ISO 27001), summaries of audit reports, or equivalent third-party assessments. Where Company makes such materials available, Customer shall accept them in lieu of an on-site Audit absent demonstrated, material concerns that cannot be addressed through such materials.

9.5. Company 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) Company's internal financial information; (iii) Company's trade secrets; (iv) any information that in Company's sole discretion, could compromise the security of any of Company's systems or premises or cause Company 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 Company's obligations under this DPA will remain in force for as long as Company processes Customer Personal Data.

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 applicable 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 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 sixty (60) 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 Ltd. implements and operates information security in accordance with ISO 27001.

1.2. Review of information security. Company'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. Company 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. Company 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.

4. Data Encryption. Company employs industry-standard encryption for Customer Personal Data both at rest and in transit, using algorithms and protocols consistent with then-current industry practice. Company may update or modify the encryption methods it uses from time to time, provided that the overall level of protection is not materially diminished.

5. Personnel Access Controls

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

5.2. Least Privilege user accounts. Company creates and deletes user accounts with appropriate approval based on Least Privilege principles.

5.3. Need-to-know-Access. Company will not access the Customers' Personal Data for any purpose other than as necessary to perform its obligations to Customer or as otherwise expressly permitted under the Terms of Use.

5.4. Multifactor Authentication. Company uses multi-factor authentication and encrypted channels for all administrative account access. Company may update or modify its authentication methods it uses from time to time, provided that the overall level of protection is not materially diminished.

6. Management of Information Security Incidents and Improvements

6.1. Reporting Information Security Incident. Company implements procedures for Personal Data Breach incidents to be reported through appropriate management channels without undue delay following confirmation of the incident.

Annex III to the DPA

To the extent Customer is accessing the Cyberbit Readiness platform via readiness.cyber-range.com or portal.rangeforce.com, the following Subprocessors shall apply:

Subprocessor's Name	***Description***	***Location***
Anthropic	Internal operations and data analytics	USA
Atlassian (Jira Service Management)	Customer support requests and technical support	EU
Contabo	Baremetal hosting provider for KVM & Docker based labs	USA
EdInvent, Inc., D.B.A. as Accredible	Digital credential management platform for creating, issuing, managing, and verifying digital certificates and badges	USA
FlowXO	Integration between portal and collaboration environments for feedback	Canada, USA, EU
Google Cloud	Hosting of the Services	USA, EU
Hetzner	Baremetal hosting provider for KVM & Docker based labs	EU
HotJar	Behavioral analytics and user interaction analysis	EU
HubSpot	Customer-relationship management, marketing automation, and support operations platform	USA
ISC(2)	Enables Users to obtain CPE Credits (optional at User's choice)	USA
Microsoft 365	Productivity, collaboration, and communication services, including email, document storage, and internal operations support.	EU
Microsoft Azure	Module and team exercising infrastructure	Global
OpenAI	Administration and customer support	USA
OVH Canada	Baremetal hosting provider for KVM & Docker based labs	Singapore
OVH US	Baremetal hosting provider for KVM & Docker based labs	USA
Salesforce	Customer-relationship management and internal communication	EU
Twilio	Transactional and operational messaging	EU
Sentry	Application error tracking and performance monitoring	USA
Virtualbadge.io	Digital badges and credentials	EU

	management	
Vitally	Customer success management platform	EU
Zoho	Providing support and chat services to our Users	USA

To the extent Customer is accessing the Cyberbit Original platform via cyberbitrange.com the following Subprocessors shall apply:

Subprocessor's Name	***Description***	***Location***
Amazon Web Services	Hosting of the Services	USA
Anthropic	Internal operations and data analytics	USA
Auth0	Authentication of Users	USA
EdInvent, Inc., D.B.A. as Accredible	Digital credential management platform for creating, issuing, managing, and verifying digital certificates and badges	USA
HubSpot	Customer-relationship management, marketing automation, and support operations platform	USA
ISC(2)	Enables Users to obtain CPE Credits (optional at User's choice)	USA
Mixpanel	Analytics purposes for improving the Services and user experience.	EU
Salesforce	Customer-relationship management and internal communication	EU
Twilio	Transactional and operational messaging	EU
Vitally	Customer success management platform	EU
Zoho	Providing support and chat services to our Users	USA

Notwithstanding anything to the contrary, to the extent your Purchase Order indicates that your data will be stored and processed in the EU and you access the service at readiness.eu.cyber-range.com or portal.rangeforce.eu only the following list of Subprocessors shall apply.

Subprocessor's Name	***Description***	***Location***
Atlassian (Jira Service Management)	Customer support requests and technical support	EU
Google Cloud	Hosting of the Services	EU
Hetzner	Baremetal hosting provider for KVM & Docker based labs	EU
Microsoft Azure	Range exercise infrastructure, administration and customer support	Global
Salesforce	Customer-relationship management and Internal communication	EU
Twilio	Transactional and operational messaging	EU
Sentry	Application error tracking and performance monitoring	USA with EU Governance
Virtualbadge.io	Digital badges and credentials management	EU
Vitally	Customer success management platform	EU

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 DPA 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 DPA.

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 Company 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 DPA 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 Company solely for the limited and specified business purpose of Company performing the Services (including without limitation, analytics for Product improvement), as described in this Annex.

2. **Company's Role**. Company is a Service Provider (as such term is defined under CPRA), and as such Company shall provide the Services and process any Personal Information in accordance with the Terms of Use. Company 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. Company will refrain from taking any action that would cause any transfers of Personal Information to or from Company 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, Company will not combine Personal Information that Company receives from, or on behalf of a Consumer, or which Company collects from its own interaction with a Consumer with that of another person.

3.3. Company 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 Company, unless (i) it has expressly notified Company in writing of such anticipated transfer or disclosure; and (ii) provided Company specific instructions regarding such sensitive personal information, and in such a case, Company will not retain or use such sensitive personal information other than in accordance with such instructions.

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

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

4. **Security**. Company 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 Company's minimum security procedures can be found in Annex II of the DPA.

5. **Retention**. Company will retain Personal Information only for as long as it is providing Services to the Customer, or as required by applicable laws. Within sixty (60) days from the termination of the Services, or upon Customer's written request, Company will either destroy or return Personal Information to the Customer, unless legal obligations require storage of the Personal Information.

6. **Breach of Personal Information.** Company 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.

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

8. **Assistance with Consumers' Rights Requests**. If Company, 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.

9. **Inability To Comply With CPRA**. Company will notify Customer within thirty (30) days after Company determines that it can no longer meet its material obligations under this Annex or the CPRA. Upon receipt of such notice, Customer's sole and exclusive remedy shall be to terminate the affected Services on written notice to Company provided that Customer exercises this right within thirty (30) days of its receipt of notice from Company.