

VENDOR DATA PROCESSING AGREEMENT

This Data Processing Agreement ("DPA"), effective as of _____ on this [●] day of [●] 2024 by and between Eton and Vendor sets forth the terms and conditions relating to the privacy, confidentiality, security and protection of Personal Data (as defined below) associated with services rendered by, and/or products provided by, vendor to Eton (and/or its Affiliates) pursuant to any agreement between Eton and Vendor (and/or its Affiliates), regardless of whether such agreement exist as of or after the Effective Date (such agreement as applicable, the "Services Agreement"), which, together with this DPA, the "Agreement")

The Vendor and Eton shall also be referred to collectively as the "**Parties**" and individually as "**Party**".

The Parties hereby agree as follows:

1. Definitions

In this DPA, the following terms shall have the following meanings:

- 1.1. "**Authorised Persons**" shall mean any and all persons formally and properly empowered to perform specified duties associated with an office or an agreement or contract and shall include in this context the Vendor's staff, agents and subcontractors.
- 1.2. "**Controller**" shall mean the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of Personal Data.
- 1.3. "**Data Protection Laws**" means, as applicable to the parties, all applicable data protection laws, rules, regulations, directives and governmental requirements currently in effect and as they become effective relating in any way to the privacy, confidentiality, security or protection of Personal Data, and shall include the GDPR, the PDPA, the CCPA and the CPRA
- 1.4. "**Data Subject**" shall mean an identified or identifiable natural person. An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
- 1.5. "**Personal Data**" shall mean any information relating to a Data Subject.
- 1.6. "**Personal Data Breach**" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise processed.
- 1.7. "**Processor**" shall mean a natural or legal person, public authority, agency or other body which processes Personal Data on behalf of the Controller.
- 1.8. "**Services**" shall mean the work performed by the Vendor for Eton as set forth in a Services Agreement.
- 1.9. "**Services Agreement**" shall mean the agreement between the Vendor and Eton describing and governing the Services to be provided by the Vendor to Eton.
- 1.10. "**Processing/To Process**" means any operation or set of operations which is performed upon Personal Data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.

2. Processing of Data

- 2.1. In connection with providing the Services to Eton, Vendor acknowledges and agrees that it may Process Personal Data solely as necessary to perform its obligations under the Services Agreement and strictly in accordance with the documented instructions of Eton (the "**Permitted Purpose**") as contained in this DPA, In this case, the Vendor shall inform Eton of that legal requirement before Processing, unless the law prohibits this on important grounds of public interest.
- 2.2. Vendor acknowledges that Eton may either be the Controller or the Processor of the Personal Data and where Eton is the Processor, Vendor acknowledges that it will be a sub-processor to Eton. Each Party shall adhere and comply with the obligations that apply to it under applicable Data Protection Laws.
- 2.3. **Sub-processing:** Eton and Vendor agree to the list of sub-processors in Schedule C which can be engaged by the Vendor. Vendor shall obtain explicit written consent from Eton prior to adding or removing a third-party sub-processor to Process Personal Data provided that: (i) Vendor obtains Eton's consent at least 15 days' prior to the addition or removal of any sub-processor (including details of Processing it performs or will perform) to or from the list of existing sub-processors in Schedule C hereto; (ii) Vendor engages third-party sub-processors by way of a contract which imposes on the sub-processor, in substance, the same data protection obligations as the ones imposed on the Vendor in accordance with this DPA, and ensures that the sub-processor complies with the obligations to which the Vendor is subject under this DPA and under applicable Data Protection Laws. The Vendor shall ensure that the sub-processors shall not further engage any third-party sub-processors. At Eton's request, the Vendor shall provide a copy of such a sub-processor agreement and any subsequent amendments to Eton. To the extent necessary to protect business secret(s) or other confidential information, including personal data, the Vendor may redact the text of the agreement prior to sharing the copy. The Vendor shall agree to a third party beneficiary clause with the sub-processor whereby, in the event the Vendor has factually disappeared, ceased to exist in law or has become insolvent, Eton shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the Personal Data; and (iii) the Vendor remains fully liable for any breach of this DPA that is caused by an act, error or omission of its sub-processor. If Eton refuses to consent to Vendor's appointment of a third-party sub-processor on reasonable grounds relating to the protection of Personal Data, Eton may elect to suspend or terminate the Services Agreement without penalty.
- 2.4. **Confidentiality of Processing:** The Vendor will restrict its personnel from Processing Personal Data without authorisation. The Vendor will impose appropriate contractual obligations upon its personnel, including relevant obligations regarding confidentiality, data protection and data security. Vendor shall ensure that it transfers its obligations to any person that it authorises to Process Personal Data (including Vendor's personnel under any capacity, Vendor's staff and subcontractors) (an "**Authorised Person**") shall be subject to a strict duty of confidentiality (whether a contractual duty or a statutory duty) and shall not permit any person to Process Personal Data who is not under such a duty of confidentiality. Vendor shall ensure that all Authorised Persons Process Personal Data only as necessary for the Permitted Purpose.
- 2.5. For the avoidance of doubt, any instructions that would lead to Processing outside the scope of this DPA (e.g., because a new Processing purpose is introduced) will require a prior agreement between the Parties and, where applicable, shall be subject to the contract change procedure under the respective agreement.
- 2.6. Vendor shall, without undue delay, inform Eton in writing if, in Vendor's opinion, an instruction infringes Data Protection Laws, and provide a detailed explanation of the reasons for its opinion in writing.

3. Security of Data

Vendor shall implement appropriate technical and organizational measures to ensure the security of the Personal Data and protect the data against a Personal Data Breach, as specified in Schedule B hereto. In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the nature, scope, context and purposes of Processing and the risks involved for the Data Subjects.

4. Term and Termination

- 4.1. This DPA becomes effective upon signature. It shall continue to be in full force and effect as long as Vendor is Processing Personal Data pursuant to the Services Agreement.
- 4.2. Where amendments are required to ensure compliance of this DPA with Data Protection Laws, the Parties shall make reasonable efforts to agree on such amendments upon request of the Controller. Where the Parties are unable to agree upon such amendments, Eton may terminate the Services Agreement and this DPA with [●] days' prior written notice to the Vendor.
- 4.3. Without prejudice to any provisions under applicable Data Protection Laws, in the event that the Vendor is in breach of its obligations under this DPA, Eton may instruct the Vendor to suspend the Processing of Personal Data until the latter complies with this DPA or the Services Agreement is terminated. The Vendor shall promptly inform Eton in case it is unable to comply with this DPA, for whatever reason.
- 4.4. Eton shall be entitled to terminate the Services Agreement insofar as it concerns Processing of Personal Data in accordance with this DPA if:
 - a. the Processing of Personal Data by the Vendor has been suspended by Eton pursuant to Clause 4.3 and if compliance with this DPA is not restored within a reasonable time and in any event within [●] month following suspension;
 - b. the Vendor is in substantial or persistent breach of this DPA or its obligations under applicable Data Protection Laws;
 - c. the Vendor fails to comply with a binding decision of a competent court or the competent supervisory authority/ies regarding its obligations pursuant to this DPA or to applicable Data Protection Laws.
- 4.5. The Vendor shall notify Eton if it is not able to continue to provide the Services under the Services Agreement pursuant to which, Eton is entitled to terminate this DPA.
- 4.6. The Vendor shall be entitled to terminate the Services Agreement insofar as it concerns Processing of Personal Data under this DPA where, after having informed Eton that its instructions infringe applicable legal requirements in accordance with Clause 2.6, Eton insists on compliance with the instructions.

5. Actions and Access Requests

- 5.1. Vendor shall assist Eton in the event of any action by data protection authorities. Vendor hereby grants permission to Eton to disclose, at its sole discretion, the contents of this DPA with its customers and/or any data protection authorities on their request. Upon Eton's request, Vendor shall provide Eton with a designated contact for all privacy-related queries.
- 5.2. Vendor shall provide all reasonable and timely assistance to Eton to enable Eton to respond to:
 - (i) any request from a Data Subject to exercise any of its rights under applicable laws (including its rights of access, correction, objection, erasure and data portability, as applicable); and
 - (ii) any other correspondence, enquiry or complaint received from a Data Subject, regulator or other third-party in connection with the Processing of the Personal Data.

In the event that any such request, correspondence, enquiry or complaint is made directly to Vendor, Vendor shall promptly inform Eton and, where appropriate, the Controller, providing full details of the same.

- 5.3. The Vendor shall cooperate with and assist Eton, for Eton to comply with its obligations under Data Protection Laws including Data Subject Rights Requests, taking into account the nature of Processing and the information available to the Vendor.

6. International Transfers

Eton and Vendor shall implement technical and organizational measures in a manner to ensure that any cross-border data transfers of Personal Data are protected with measures adequate to the Data Protection Laws including but not limiting to adequacy assessment, transfer impact assessment, data governance structure, etc. or any other measures as mentioned in Schedule B of the DPA. It is hereby clarified that the technical and organizational measures in Schedule B are indicative in nature and should not be considered as exhausted. The Parties may mutually agree to amend the measures as per prevalent industry best practices and / or applicable laws.

7. Breach Notification

- 7.1. In the event of a Personal Data Breach concerning data Processed by the Vendor or sub-processor, the Vendor shall notify Eton of the Personal Data Breach without undue delay and in any event within 48 hours of the Vendor having become aware of the breach. Such notification shall contain, at least:
 - (a) a description of the nature of the breach (including, where possible, the categories and approximate number of Data Subjects and data records concerned);
 - (b) the details of a contact point where more information concerning the Personal Data Breach can be obtained;
 - (c) its likely consequences and the measures taken or proposed to be taken to address the breach, including to mitigate its possible adverse effects.
- 7.2. Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.
- 7.3. The Parties shall set out in Schedule C all other elements to be provided by the Vendor when assisting Eton in compliance with Eton's obligations under applicable Data Protection Laws.

8. Deletion or Return of Data

At any time during the term of the Services Agreement at Eton's written request or upon the termination or expiration of the Services Agreement for any reason, Vendor shall instruct all Authorised Persons to, securely dispose of all copies of Personal Data and certify in writing to Eton that such Personal Data has been disposed of securely. The Vendor shall comply with all directions provided by Eton with respect to the return or disposal of Personal Data and shall provide a certificate of return / deletion upon return of disposal of Personal Data. The Vendor agrees that it shall be in breach of this DPA if it is found that there are copies of Personal Data in the possession of the Vendor after such a certificate has been issued. Until the data is deleted or returned, the Vendor shall continue to ensure compliance with this DPA.

9. Audit Rights

The Vendor shall be able to demonstrate compliance with this DPA. The Vendor shall maintain complete and accurate records in connection with the Vendor's performance under this DPA

and shall retain such records for such period as may be communicated by Eton as per applicable law of the Services Agreement. The Vendor shall permit Eton (or its appointed third-party auditors) to audit the Vendor's compliance with this DPA, and shall make available to Eton all information, systems and staff necessary for Eton (or its third-party auditors) to conduct such audit. The Vendor acknowledges that Eton (or its third-party auditors) may enter its premises for the purposes of conducting this audit, provided that Eton gives the Vendor reasonable prior notice of its intention to audit, conducts its audit during normal business hours, and takes all reasonable measures to prevent unnecessary disruption to the Vendor's operations. Eton shall be responsible for the costs of such audits unless the Vendor is found to be in breach of this DPA. The Vendor agrees, at its cost, to make any changes requested by Eton to correct inadequacies discovered in such audits or tests.

10. Data Protection Impact Assessment

The Vendor shall provide Eton with all such reasonable and timely assistance as Eton may require in order to conduct a data protection impact assessment and, if necessary, to consult with relevant data protection authorities.

11. Indemnity

Vendor will indemnify, defend, and hold harmless Eton and its Affiliates and their respective shareholders, directors, officers, employees and agents from and against all expenses, liabilities, damages and costs (including settlement costs and reasonable attorneys' fees) arising out of a third-party claim related to breach by Vendor of its obligations under this DPA.

12. Miscellaneous

- 12.1. In case of any conflict, the provisions of this DPA shall take precedence over the Services Agreement or provisions of any other agreement between Eton and Vendor. In case of any conflict between this DPA and the applicable Data Protection Laws, the applicable Data Protection Laws shall take precedence over the provisions of the rest of the DPA.
- 12.2. No Party shall receive any remuneration for performing its obligations under this DPA except as explicitly set out in the Services Agreement.
- 12.3. Where this DPA requires a "written notice" such notice can also be communicated per email to the other Party.
- 12.4. Any supplementary agreements or amendments to this DPA must be made in writing and signed by both Parties.
- 12.5. Should individual provisions of this DPA become void, invalid or non-viable, this shall not affect the validity of the remaining conditions of this DPA.

ACCEPTED AND AGREED BY THE PARTIES:

For: [Eton Entity Name]	For [Vendor Name]
Signature:	Signature:
Title:	Title:

SCHEDULE A

A. LIST OF PARTIES

Eton: [*Identity and contact details of Eton and, where applicable, of its/their data protection officer and/or representative*]

1. Name:

Address:

Contact person's name, position and contact details:

Activities relevant to the data transferred under these Clauses: As set out in Part B.

Signature and date:

Role (Controller/Processor): Controller/Processor

Vendor(s): [*Identity and contact details of the Vendor(s), including any contact person with responsibility for data protection*]

1. Name:

Address:

Contact person's name, position and contact details:

Activities relevant to the data transferred under these Clauses:

Signature and date:

Role (Controller/Processor): Processor/Sub-Processor

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

Eton may submit Personal Data to the Services, the extent of which is determined and controlled by Eton in its sole discretion, and which may include, but is not limited to Personal Data relating to the following categories of Data Subjects:

[To List the data subjects whose personal data is transferred (E.g., HNI, Employee, etc.)]

Categories of personal data transferred

Eton may submit Personal Data to Vendor, the extent of which is determined and controlled by Eton in its sole discretion, and which may include, but is not limited to, the following categories of Personal Data: (Names...), titles, position, employer, contact information (email, phone, fax, physical address etc.), identification data, connection data, or localization data (including IP addresses), application data of Eton's customers.

[To fill in personal data which is being shared with vendor (Eg – name, email, phone number, etc.)]

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures

[To list the categories of sensitive data transferred, if any]

The frequency of the transfer (e.g., whether the data is transferred on a one-off or continuous basis)

Personal Data is transferred on a continuous basis

Purpose(s) of the data transfer and further processing

Personal Data is transferred in the course of access and use by Eton of the Services so that the Vendor may provide the Services.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

Upon termination of Eton's account, the Vendor will delete all Personal Data in accordance with clause 8 of the DPA. This requirement shall not apply to the extent that the Vendor is permitted by applicable law to retain some or all of the Personal Data, in which event Eton shall isolate and protect the Personal Data from any further Processing.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

As described in Schedule C.

SCHEDULE B

TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

Description of the technical and organisational measures implemented by the Vendor(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.

People

- Cybersecurity awareness and hygiene
- Background verification (Criminal, education, previous employment, credit checks to name a few)
- Employee Handbook
- Newsletters and emails to reinforce Cybersecurity awareness.

Process

- Information Security Policy and Procedures
- Acceptable use policy
- Disciplinary process for breaches
- Change Management Policy
- Incident Response Policy
- BCP and DR practices
- Third Party (vendor) management policy
- Data Classification Policy
- Access to the data on least privileges principle:
- Need-to-Do
- Right-to-Know
- Clear Desk Clear Screen policy.

Technical

- Physical access controls
- Role Based Access Controls with granular role definition.
- Encryption of data at rest, in process and in transit
- Laptop encryption using Windows Bit Locker encryption.
- All remote access through VPN
- Multi-Layered network protection by using routers, proxy servers, L7 Firewall, WAF
- Intrusion Detection System
- Monitoring of logs, incident detection and response
- Device hardening policy.
- Backup and Recovery
- Security Centre
- Key Vault
- Patch Management
- Anti-Malware and AV engine

SCHEDULE C

LIST OF SUB-PROCESSORS

Eton has authorised the use of the following sub-processors:

1. Name:

Address:

Contact person's name, position and contact details:

Description of processing (including a clear delimitation of responsibilities in case several sub-processors are authorised):

2. Name:

Address:

Contact person's name, position and contact details:

Description of processing (including a clear delimitation of responsibilities in case several sub-processors are authorised):

3. etc.