DATA PROCESSING ADDENDUM

This Data Processing Addendum (including its Exhibits) ("**Addendum**") forms part of and is subject to the terms and conditions of the Order (including the Terms governing such Order) (the "**Agreement**") between Provider and the Customer that executed the Agreement ("**Customer**") acting on its own behalf and for any Customer Affiliate, and is hereby incorporated by reference.

This Addendum replaces, in its entirety, any existing agreement, addendum, schedule, exhibit agreement or other document governing the processing and protection of Customer Personal Date in relation to the Services.

Defined terms used but not otherwise defined in this Addendum have the meanings given in the Agreement. Except as modified below, the terms of the Agreement shall remain in full force and effect.

This Addendum reflects the parties' commitment to abide by Data Protection Laws concerning the Processing of Customer Personal Data in connection with the Services in the Agreement. If and to the extent language in this Addendum conflicts with the Agreement, this Addendum shall control.

This Addendum will become legally binding upon the effective date of the Agreement or upon the date that the parties sign this Addendum if it is completed after the effective date of the Agreement.

1. **Definitions.**

For the purposes of this Addendum, the following terms and those defined within the body of this Addendum apply.

a) "**Customer Personal Data**" means Personal Data which is owned or controlled by the Customer, and which is provided by or on behalf of the Customer to Provider in connection with the Services.

b) "**Contracted Processor**" means Provider or a Subprocessor.

c) "**Controller**" means the entity which determines the purposes and means of the Processing of Customer Personal Data.

d) "**Data Protection Laws**" means all laws and regulations that are applicable to the Processing of Customer Personal Data in connection with the provision of the Services under the Agreement. "Data Protection Laws" may include, but not limited to, the California Consumer Privacy Act of 2018 ("**CCPA**"); the EU General Data Protection Regulation 2016/679 ("**GDPR**") and its respective national implementing legislations; the Swiss Federal Act on Data Protection; the United Kingdom General Data Protection Regulation ("**UK GDPR**"); and the United Kingdom Data Protection Act 2018 (in each case, as amended, adopted, or superseded from time to time);

e) "**Data Subject**" has the meaning given in Data Protection Laws;

f) "**Personal Data**" means any information that has been provided by or on behalf of Customer for use in the Services that relates to an identified or identifiable person.

g) "**Process**" or "**Processing**" means any operation or set of operations which is performed on Customer Personal Data or sets of Customer Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination, or otherwise making available, alignment or combination, restriction, erasure, or destruction.

h) "**Processor**" means the entity which Processes Customer Personal Data on behalf of the Controller.

i) "**Security Incident(s)**" means the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer Personal Data. A Security Incident shall not include unsuccessful attempts or activities that do not compromise the security of Customer Personal Data, including unsuccessful log-in attempts, pings, port scans, denial of service attacks, and other network attacks on firewalls or networked systems.

j) "**Services**" means the services that Provider performs under the Agreement.

k) "**Standard Contractual Clauses**" (incorporated herein by reference) refers to :

the "2021 Standard Contractual Clauses," defined as the clauses issued pursuant to the EU Commission Implementing Decision (EU) 2021/914 of June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council, available at http://data.europa.eu/eli/dec_impl/2021/914/oj (as amended and updated from time to time).

l) "**Subprocessor(s)**" means Provider's authorized vendors and third-party service providers that Process Customer Personal Data.

m) "**Supervisory Authority**" means an independent public authority established pursuant to Data Protection Laws to supervise compliance with Data Protection Laws

2. **Data Use and Processing.**

a) Roles of the Parties. The Parties acknowledge and agree that (i) where Customer is a Controller, Provider is the Processor, and (ii) where Customer is a Processor, Provider is a Subprocessor to Customer. Furthermore, where the CCPA applies to Provider's Processing of

Customer Personal Data, the parties acknowledge and agree that Customer is a Business, as that term is defined within CCPA and its implementing regulations, and that Provider is Customer's Service Provider, as that term is defined within the CCPA and its implementing regulations.

b) Documented Instructions. Customer instructs Provider to Process Customer Personal Data in order to enable it to provide the Services and Customer to receive the Services in accordance with the Agreement, this Addendum, any applicable statement of work, and any instructions agreed upon by the parties in writing. The subject matter of the Processing is the use by the Customer and any of its end users of the Services. The categories of Data Subject are users of the Services and occupants of premises where the Services are used and so may include employees and visitors of Customer. Provider will ensure that any transfer of Customer Personal Data out of the EEA and/or the United Kingdom is carried out in accordance with Data Protection Laws, using a lawful transfer mechanism. Customer will ensure that Provider's Processing of Customer Personal Data, when done in accordance with the Customer's instructions, will not cause Provider to violate any applicable law or regulation, including applicable Data Protection Laws. Customer shall have the sole responsibility for the accuracy, quality, and legality of Customer Personal Data, all necessary consents, processes and notices required in order to enable lawful transfer of Customer Personal Data to Provider under the Agreement and this Addendum, and the means by which Customer acquired the Personal Data. The duration for which the Provider will Process Customer Personal Data is the duration of the Agreement plus any applicable retention periods in this Addendum. Provider will, unless legally prohibited from doing so, inform Customer in writing if it reasonably believes that there is a conflict between Customer's instructions and applicable Data Protection Laws.

c) Authorization to Use Subprocessors. To the extent necessary to fulfill Provider's contractual obligations under the Agreement, Customer hereby authorizes Provider to engage Subprocessors. Provider's current list of Subprocessors for the applicable Services is available at www.eptura.com/subprocessors (the "**Subprocessor List**"). Customer agrees to the appointment of those Subprocessors listed in the Subprocessor List. Provider agrees that it shall not transfer Personal Data to any entities not named on the Subprocessor List.

d) Provider and Subprocessor Compliance. Provider agrees to (i) enter into a written agreement with Subprocessors regarding such Subprocessors' Processing of Customer Personal Data that imposes on such Subprocessors data protection requirements for Customer Personal Data that are consistent with this Addendum; and (ii) remain responsible for the acts and omissions of its Subprocessors to the same extent Provider would be liable if performing Services of each Subprocessor directly under the terms of this Addendum.

e) Right to Object to Subprocessors. Provider will, at least 15 days prior to appointing any new Subprocessor, notify Customer of its intent to engage any new Subprocessors by updating the Subprocessor List and Provider shall offer Customer the ability to sign-up for notifications to such changes. Customer may object to Provider's use of the new Subprocessor by notifying Provider promptly in writing 15 days of receipt of Provider's notice. Notification to Customer will be provided to the e-mail address(s) provided in the Order for the Services or otherwise to Provider in the purchasing of Services. If Customer does not object to the engagement of the new Subprocessor in accordance with this Section, the new Subprocessor will be deemed accepted for the purposes of this Addendum. If Customer objects to Provider's appointment or replacement of a Subprocessor based on reasonable grounds relating to data protection, it shall notify Provider in writing detailing such objection prior to the appointment or replacement of the Subprocessor. In such event, Provider will use reasonable efforts to provide the Services to Customer in accordance with the Agreement without using the Sub-processor. If Provider reasonably requires use of the Subprocessor and is unable to satisfy Customer as to the suitability of the Subprocessor within thirty (30) days of Customer's objection, Customer may elect to terminate only the part of the Services or Order(s) which cannot be provided by Provider without the use of the objected-to Subprocessor.

f) Confidentiality. Provider shall ensure that its personnel and those of its Affiliates engaged in the Processing of Customer Personal Data are informed of the confidential nature of the Customer Personal Data and have executed written confidentiality agreements.

g) Data Protection Impact Assessment and Prior Consultation. Provider shall provide reasonable assistance to Customer with any data protection impact assessments (at Customer's expense only if such reasonable cooperation will require Provider to assign significant resources to that effort) and prior consultations with any Supervisory Authority or other competent data privacy authorities to the extent required by applicable Data Protection Laws, in each case solely in relation to Processing of Customer Personal Data, and taking into account the nature of the Processing and information available to Provider.

3. Data Subjects.

Provider shall, to the extent permitted by Data Protection Laws, notify Customer if Provider receives a request from a Data Subject that identifies Customer Personal Data or otherwise identifies Customer, including where the Data Subject seeks to exercise any of its rights under applicable Data Protection Laws (collectively, "**Data Subject Request**"). If Provider receives a Data Subject Request in relation to Customer Personal Data, Provider will advise the Data Subject to submit their request to Customer and Customer will be responsible for responding to such request, including where necessary, by using the functionality of the Services. To the extent Customer is unable to access the relevant Customer Personal Data within the Services using such controls or otherwise, Provider will (upon Customer's written request and taking into account the nature of the Processing) provide commercially reasonable cooperation to assist Customer in responding to Data Subject Requests.

4. Data Transfers.

If Customer Personal Data originating in the European Economic Area, Switzerland, and/or the United Kingdom is transferred by Customer to Provider in a country that has not been found to provide an adequate level of protection under applicable Data Protection Laws, the parties agree that the transfer shall be governed by the Standard Contractual Clauses, or SCCs. Where the SCCs are applicable and Customer acts as a Controller of Customer Personal Data with Provider acting as a Processor of Customer Personal Data, each party shall comply with its obligations under Module Two of the SCCs. Where the SCCs are applicable and Customer acts as a processor of Customer Personal Data with Provider also acting as a processor of Customer Personal Data, each party shall comply with its obligations under Module Three of the SCCs. The parties agree that: (i) the optional docking clause in Clause 7 does not apply; (ii) the certification of deletion required by Clause 8.5 and Clause 16(d) of the SCCs will be provided upon Customer's written request; (iii) the measures Provider is required to take under Clause 8.6(c) of the SCCs will only cover Provider's impacted systems; (iv) the audit described in Clause 8.9 of the SCCs shall be carried out in accordance with Section 7 of this Addendum; (v) in Clause 9, the minimum time period for prior notice of Subprocessor changes shall be as set forth in section 2(e) of this Addendum (vi) where permitted by Data Protection Laws, Provider may engage existing Subprocessors using European Commission Decision C(2010)593 SCCs for Controllers to Processors and such use of Subprocessors shall be deemed to comply with Clause 9 of the SCCs; (vii) in Clause 11, the optional language does not apply; (viii) the termination right contemplated by Clause 14(f) and Clause 16(c) of the SCCs will be limited to the termination of the SCCs, in which case, the corresponding Processing of Customer Personal Data affected by such termination shall be discontinued unless otherwise agreed by the parties; (ix) the information required under Clause 15.1(c) will be provided upon Customer's written request; (x) in Clause 17, the Parties shall be governed by the laws of the Republic of Ireland; (xi) in Clause 18(b), disputes will be resolved before the courts of the Republic of Ireland; (xii) Exhibit A to this Addendum contains the information required in Annex I of the SCCs; (xiii) Exhibit B to this Addendum contains the information required in Annex II of the SCCs; (xiv) to the extent any Personal Data is subject to any UK Data Privacy Laws, the SCCs are supplemented by Exhibit C; and (xv) notwithstanding anything to the contrary, Customer will reimburse Provider for all costs and expenses incurred by Provider in connection with the performance of Provider's obligations under Clause 15.1(b) and Clause 15.2 of the SCCs. Each party's signature to this Addendum shall be considered a signature to the SCCs to the extent that the SCCs apply hereunder.

5. Information Security Program.

Provider has implemented and will maintain appropriate administrative, technical, and organizational measures to protect Customer Personal Data from a Security Incident, having regard to the state of technological development and the cost of implementing such measures, as well as the nature, scope, context and purposes of Processing and the likelihood and severity of harm to the interests of data subjects that may be expected to result from any such Security Incident (including, where appropriate, the measures referred to in Article 32(1) of the GDPR). Any questions about Provider's security practices can be sent to Provider's Security and Privacy team at privacy@eptura.com.

6. Security Incidents.

a) Provider will provide written notification to Customer without undue delay if it becomes aware of a Security Incident. Any such notification is not an acknowledgement of fault or responsibility. Notification shall so far as possible allow Customer to inform Data Subjects of the Security Incident under Data Protection Laws and, to the extent known by Provider, (i) describe the nature of the Security Incident including where possible, the categories and approximate number of data subjects concerned, and the categories and approximate number of personal data records concerned; and (ii)describe the measures taken or proposed to be taken by Provider to address the Security Incident, including, where appropriate, measures to mitigate.

b) In case of a Security Incident and prior to making any required public statement or required notice, Provider agrees to seek approval from the Customer before any notification is made to affected data subjects or the relevant Supervisory Authorities regarding the Security Incident. Notwithstanding the preceding sentence, Customer will not be required to prejudice its obligations under Data Protection Laws.

c) The obligations described in Section 7(a) and 7(b) shall not apply in the event that a Personal Data breach results from the actions or omissions of Customer.

7. Audits.

a) Provider uses independent, third-party auditors to verify the adequacy of its Processing of Customer Personal Data. This audit will: (i) be performed at least annually; (ii) be performed by a qualified professional at Provider's selection and expense; and (iii) demonstrate Provider's compliance with prevailing data security standards applicable to the processing of Personal Data ("**Report**"). Upon Customer's written request, Provider will provide Customer with an executive summary of its Report so that Customer can reasonably verify Provider's compliance with the security obligations in this Addendum. Any provision of such Report shall be subject to reasonable confidentiality procedures.

b) If Provider is unable to promptly provide current Reports, Customer may, upon written request, perform (at its own expense) an information security assurance audit. Any such audit shall be subject to the following conditions: (i) Customer must give a minimum thirty (30) days' notice of its intention to audit; (ii) no later than two (2) weeks prior to audit activity, a mutually agreed upon scope and timeline shall be determined; (iii) any independent auditor will be required to sign a non-disclosure agreement as is reasonably required by Provider prior to the audit; (iv) the audit must be conducted during Provider's normal business hours; (v) the audit must be completed in one (1) business day; (vi) the right to audit includes the right to inspect but not copy or otherwise remove any records, other than those that relate specifically and exclusively to the Customer; and (vii) the audit shall not include penetration testing, vulnerability scanning, or other security tests. Customer may exercise the right to audit no more than once per twelve (12) month period; provided, however, that Customer may conduct additional audits in the event of (i) a Security Incident involving Customer Personal Data; or (ii) a request by a Supervisory Authority or any similar regulatory responsible for the enforcement of Data Protection Laws in any country or territory. Provider and Customer shall meet and discuss any audit findings with any remediation activities and timelines to be determined by Provider in its sole discretion.

8. Data Deletion.

Provider shall make Customer Personal Data available for export by Customer upon written request made within thirty (30) days of the date of termination/expiration of the Agreement. Thereafter, Provider will within sixty (60) days delete all Customer Personal Data (excluding any back-up or archival copies which shall be deleted in accordance with Provider's data retention schedule), except where Provider is required to retain copies under Data Protection Laws, in which case Provider will protect that Customer Personal Data from any further Processing. Where Customer requests a copy of the Customer Personal Data, Provider will comply with such request within 45 days of the date of request.

9. Liability.

This Addendum is without prejudice to the rights and obligations of the parties under the Agreement which shall continue to have full force and effect, including any limitations and exclusions on liability contained therein which shall apply to this Addendum as if fully set forth herein. In the event of any conflict between the terms of this Addendum and the terms of the Agreement, the terms of this Addendum shall prevail so far as the subject matter concerns the processing of Customer Personal Data.

10. Miscellaneous.

a) This Addendum shall be governed by and construed in accordance with the law and the jurisdiction of the country or territory which governs the Agreement, except as otherwise specified in this Addendum or required by Data Protection Laws.

b) Provider may update the terms of this Addendum where the changes (a) are required to comply with Data Protection Laws, applicable regulation, a court order or guidance issued by a regulator or agency; or (b) do not have a material adverse impact on Customer's rights under the Addendum. Provider will provide thirty (30) days' notice prior to making any material change to the provisions of this Addendum. If the updates materially impact the Customer's use of the Services, Customer has the right to terminate the affected Services within thirty (30) days of receiving written notice of the changes.

[Remainder of document intentionally left blank]

Exhibit A

ANNEX I

A. LIST OF PARTIES

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

Data exporter(s):

Name:	The Customer identified in the Agreement and/or Order Form(s)/Statement(s) of Work and all Affiliates of Customer
Address:	Customer's address, as identified in the Agreement and/or Order Form(s)/Statement(s) of Work
Contact Person:	Customer's email address, as identified in the Agreement and/or Order Form(s)/Statement(s) of Work
Activities Relevant to Transferred Data:	Purchase of Services from Provider
Role:	Controller (Module Two); Processor (Module Three)

Data importer(s):

Name:	The Provider identified in the Agreement and/or Order(s)/Statement(s) of Work and all Affiliates of Provider
Address:	Provider's address, as identified in the Agreement and/or Order(s)/Statement(s) of Work
Contact Person:	privacy@eptura.com
Activities Relevant to Transferred Data:	Provider is a provider of enterprise cloud workspace and asset management solutions, which Processes Personal Data upon the instructions of the Data Exporter in accordance with the terms of the Agreement and Addendum.
Role:	Processor

B. DESCRIPTION OF TRANSFER

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

Subject Matter of the Processing:	The subject matter of the Processing of Personal Data by Provider is the provision of Services to Data Exporter pursuant to the Agreement.
Nature and Purpose of Processing:	The Processing is related to the provision of SaaS solutions to the Customer, as further detailed within the Agreement, and Provider and its Subprocessors will perform such acts of Processing of Personal Data as are necessary to provide those Services according to Data Exporter's instructions, including but not limited to the transmission, storage, and other Processing of Personal Data submitted to the Services.
Duration of Processing:	Provider will process Personal Data on behalf of the Data Exporter until Data Exporter ceases use of the Services.
Categories of Data Subjects:	Data subjects whose Customer Personal Data will be Processed pursuant to the Agreement.
Categories of Personal Data:	Customer Personal Data that is Processed pursuant to the Agreement.

Special Categories of Personal Data:	Special Categories of Personal Data is not permitted in the Services.
Subject Matter, Nature, and Duration of Subprocessor Processing:	Any transfers to Subprocessors will be in order to perform the Services pursuant to the Agreement.

C. COMPETENT SUPERVISORY AUTHORITY

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

The supervisory authority mandated by Clause 13 of the SCCs. If no supervisory authority is mandated by Clause 13, then the Irish Data Protection Commission (DPC), and if this is not possible, then as otherwise agreed by the parties consistent with the conditions set forth in Clause 13.

Exhibit B

ANNEX II

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

Description of the technical and organisational measures implemented by the data importer(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.

In determining the technical and organizational security measures ("Security Standards") required under the Agreement, Provider will take into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons. Provider shall maintain processes for regularly testing, assessing, and evaluating the effectiveness of the Security Standards for ensuring the security of the processing of Customer Personal Data.

Provider agrees to the following with respect to Customer Personal Data:

1. Safeguards – Program. Provider will implement appropriate safeguards that are consistent with industry standards designed to protect Customer Personal Data – preserving its confidentiality, integrity and availability. Provider will ensure that all such safeguards comply with applicable Laws and the Agreement, including the data processing addendum (DPA) where applicable.

2. Safeguards – Specific. At a minimum, Provider's Security Standards will include: (a) secure facilities, data centers, paper files, servers, back-up systems and computing equipment including, but not limited to, all mobile devices and other equipment with information storage capability; (b) network, device application, database and platform security; (c) secure transmission, storage and disposal; (d) authentication and access controls within applications, operating systems and equipment; (e) logging material access and retention of such access control logs for a period sufficient to allow for investigation; (f) encryption of Customer Personal Data at rest including when stored on any electronic notebook, portable hard drive, or removable electronic media with information storage capability; (g) encryption of Customer Personal Data when transmitted over public or wireless networks; (h) separation of Customer Personal Data from information of Provider's other customers; (i) personnel security and integrity including, but not limited to, background checks consistent with applicable law; (j) annual external and internal testing and vulnerability scans and promptly implementing, at Provider's sole cost and expense, a corrective action plan (including timeline) to correct material issues that are identified through testing; and (k) limiting access of Customer Personal Data, and providing privacy and information security training, to Provider's Authorized Personnel. "Authorized Personnel" means Provider's personnel who have a need to know or otherwise access Customer Data to enable Provider to perform its obligations under the Agreement, and who are bound in writing by obligations of confidentiality sufficient to protect Customer Personal Data in accordance with the terms of the Agreement, including the DPA where applicable.

3. Malware. Provider's software as delivered will not contain any virus, malware, ransomware, keylogger, logic bomb, Trojan horse, worm, or other software routines designed to disable, erase, or otherwise harm software, hardware, or data owned or controlled by Customer.

4. Banned Hardware or Equipment. Provider shall not utilize hardware or equipment that does not comply with Section 889(a)(1)(B) of the National Defense Authorization Act for Fiscal Year 2019. Provider will provide representation of compliance with this provision upon request. If Provider can no longer comply with this provision, Provider will notify Customer immediately by sending an email to the security contact on file.

5. Disaster Recovery and Business Continuity. Provider will maintain and implement a business continuity and disaster recovery plan ("BCDR Plan") which shall include at a minimum: (a) documentation of applicable business processes, procedures and responsibilities; (b) back-up methodology; (c) identification of disaster recovery scenarios and service level agreements for service recovery; (d) responsibilities of Sub-Processors in the event of a disaster; (e) a communications strategy; and (f) procedures for reverting to normal service. The BCDR Plan shall be reviewed annually. Provider shall ensure it is able to implement the BCDR Plan at any time in accordance with its terms. Provider shall test the BCDR Plan

on a regular basis (and, in any event, not less than annually). Upon request, Provider shall send a written report summarizing the results of the most recent test and shall promptly implement any actions or remedial measures which the parties mutually agree to be necessary as a result of those tests.

6. Security Incidents. Upon Provider's discovery of any actual or reasonably suspected (i) unauthorized access to or disclosure of Customer Data; (ii) unauthorized access to applications or systems owned, managed or subcontracted by Provider ("Provider's Systems") on which Customer Personal Data is processed (each a "Security Incident"), Provider will promptly and without undue delay:

(i) take steps to mitigate and/or remediate the Security Incident to protect Customer Personal Data from further risk or harm, and initiate an investigation;

(ii) institute appropriate controls to maintain and preserve all electronic evidence relating to the Security Incident in accordance with industry standards;

(iii) report the nature of the Security Incident to Customer (including, where possible, the categories of data breached and categories of data loss methods, and to the extent that Customer Personal Data is involved, the categories and approximate number of data subjects concerned and the approximate number of Customer Personal Data records concerned);

(iv) provide the name and contact details of Provider's contact point where more information can be promptly obtained, the likely consequences of the Security Incident if known, and the measures taken or proposed to be taken to address the Security Incident, including (where appropriate) measures to mitigate its possible adverse effects;

(v) take steps to prevent any similar Security Incident from occurring in the future. For the avoidance of doubt, Provider shall not be required to report pings on firewalls, port scans, and malware that is highly unlikely to result in unauthorized access, use, disclosure, modification, or destruction of information or interference with Provider's Systems shall not be taken as a reportable Security Incident for Provider to report to Customer; and

(vi) consult and cooperate with any investigations, disputes, inquiries, claims, litigation, or regulatory actions arising from Security Incident.

7. Certifications and Security Assessments. Provider shall engage independent third-party security assessment (audit) firms to perform certification audit and security testing on an annual basis. Upon Customer's request, Provider shall provide Customer with evidence of current certification and testing, including certificates, executive summaries, and other records deemed relevant in Provider's sole but reasonable discretion (the "Assessment Records") to demonstrate compliance with the Agreement and Laws.

8. Security Questionnaires. No more than once per twelve (12) month period and upon request, Provider shall respond to a vendor cybersecurity questionnaire or similar inquiry that is of reasonable length and does not require the production of supporting evidence in addition to the current Assessment Records.

Assistance with Data Subject Requests. Customer will be responsible for communicating with data subjects pursuant to Clause 15.1(a) of the SCCs.

Exhibit C

This Addendum has been issued by the Information Commissioner for Parties making Restricted Transfers. The Information Commissioner considers that it provides Appropriate Safeguards for Restricted Transfers when it is entered into as a legally binding contract.

PART 1: TABLES

TABLE 1: PARTIES

Start date	The date on which the Customer or its Affiliate identified in the Agreement and/or Order Form(s)/Statement(s) of Work enters into the Agreement	
The Parties	**Exporter (who sends the Restricted Transfer)**	**Importer (who receives the Restricted Transfer)**
Parties' details	Full legal name: The Customer identified in the Agreement and/or Order Form(s)/Statement(s) of Work and all Affiliates of Customer Trading name (if different): Main address (if a company registered address): Customer's address, as identified in the Agreement and/or Order Form(s)/Statement(s) of Work Official registration number (if any) (company number or similar identifier): The registered number of the Customer or Affiliate of the Customer identified in the Agreement and/or Order Form(s)/Statement(s) of Work	Full legal name: The Provider identified in the Agreement and/or Order Form(s)/Statement(s) of Work Trading name (if different): Main address (if a company registered address): Provider's address, as identified in the Agreement and/or Order Form(s)/Statement(s) of Work Official registration number (if any) (company number or similar identifier): The registered number of the Provider identified in the Agreement and/or Order Form(s)/Statement(s) of Work
Key Contact	Contact details including email: Customer's email address, as identified in the Agreement and/or Order Form(s)/Statement(s) of Work	Full Name (optional): James Carder Job Title: Chief Information Security Officer Contact details including email: privacy@eptura.com
Signature (if required for the purposes of Section 2)	Not required	Not required

TABLE 2: SELECTED SCCS, MODULES AND SELECTED CLAUSES

Addendum EU SCCs	☐ The version of the Approved EU SCCs which this Addendum is appended to, detailed below, including the Appendix Information: Date:

	Reference (if any):
	Other identifier (if any):
	Or
	x the Approved EU SCCs, including the Appendix Information and with only the following modules, clauses or optional provisions of the Approved EU SCCs brought into effect for the purposes of this Addendum:

Module	Module in operation	Clause 7 (Docking Clause)	Clause 11 (Option)	Clause 9a (Prior Authorisation or General Authorisation)	Clause 9a (Time period)	Is personal data received from the Importer combined with personal data collected by the Exporter?
1						
2	x			General Authorisation	14 days	
3	x			General Authorisation	14 days	
4						

TABLE 3: APPENDIX INFORMATION

“**Appendix Information**” means the information which must be provided for the selected modules as set out in the Appendix of the Approved EU SCCs (other than the Parties), and which for this Addendum is set out in:

Annex 1A: List of Parties: As identified in Exhibit A

Annex 1B: Description of Transfer: As identified in Exhibit A

Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data: As identified in Exhibit B

Annex III: List of Sub processors (Modules 2 and 3 only): See www.eptura.com/subprocessors

TABLE 4: ENDING THIS ADDENDUM WHEN THE APPROVED ADDENDUM CHANGES

Ending this Addendum when the Approved Addendum changes	Which Parties may end this Addendum as set out in Section **Error! Reference source not found.**: ☐ Importer x Exporter ☐ neither Party

PART 2: MANDATORY CLAUSES

ENTERING INTO THIS ADDENDUM

1. Each Party agrees to be bound by the terms and conditions set out in this Addendum, in exchange for the other Party also agreeing to be bound by this Addendum.

2. Although Annex 1A and Clause 7 of the Approved EU SCCs require signature by the Parties, for the purpose of making Restricted Transfers, the Parties may enter into this Addendum in any way that makes them legally binding on the Parties and allows data subjects to enforce their rights as set out in this Addendum. Entering into this Addendum will have the same effect as signing the Approved EU SCCs and any part of the Approved EU SCCs.

INTERPRETATION OF THIS ADDENDUM

3. Where this Addendum uses terms that are defined in the Approved EU SCCs those terms shall have the same meaning as in the Approved EU SCCs. In addition, the following terms have the following meanings:

Addendum	This International Data Transfer Addendum which is made up of this Addendum incorporating the Addendum EU SCCs.
Addendum EU SCCs	The version(s) of the Approved EU SCCs which this Addendum is appended to, as set out in Table 2, including the Appendix Information.
Appendix Information	As set out in Table 3.
Appropriate Safeguards	The standard of protection over the personal data and of data subjects' rights, which is required by UK Data Protection Laws when you are making a Restricted Transfer relying on standard data protection clauses under Article 46(2)(d) UK GDPR.
Approved Addendum	The template Addendum issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section **Error! Reference source not found.**.
Approved EU SCCs	The Standard Contractual Clauses set out in the Annex of Commission Implementing Decision (EU) 2021/914 of 4 June 2021.
ICO	The Information Commissioner.
Restricted Transfer	A transfer which is covered by Chapter V of the UK GDPR.
UK	The United Kingdom of Great Britain and Northern Ireland.
UK Data Protection Laws	All laws relating to data protection, the processing of personal data, privacy and/or electronic communications in force from time to time in the UK, including the UK GDPR and the Data Protection Act 2018.

UK GDPR	As defined in section 3 of the Data Protection Act 2018.

4. This Addendum must always be interpreted in a manner that is consistent with UK Data Protection Laws and so that it fulfils the Parties' obligation to provide the Appropriate Safeguards.

5. If the provisions included in the Addendum EU SCCs amend the Approved SCCs in any way which is not permitted under the Approved EU SCCs or the Approved Addendum, such amendment(s) will not be incorporated in this Addendum and the equivalent provision of the Approved EU SCCs will take their place.

6. If there is any inconsistency or conflict between UK Data Protection Laws and this Addendum, UK Data Protection Laws applies.

7. If the meaning of this Addendum is unclear or there is more than one meaning, the meaning which most closely aligns with UK Data Protection Laws applies.

8. Any references to legislation (or specific provisions of legislation) means that legislation (or specific provision) as it may change over time. This includes where that legislation (or specific provision) has been consolidated, re-enacted and/or replaced after this Addendum has been entered into.

HIERARCHY

9. Although Clause 5 of the Approved EU SCCs sets out that the Approved EU SCCs prevail over all related agreements between the parties, the parties agree that, for Restricted Transfers, the hierarchy in Section 10 will prevail.

10. Where there is any inconsistency or conflict between the Approved Addendum and the Addendum EU SCCs (as applicable), the Approved Addendum overrides the Addendum EU SCCs, except where (and in so far as) the inconsistent or conflicting terms of the Addendum EU SCCs provides greater protection for data subjects, in which case those terms will override the Approved Addendum.

11. Where this Addendum incorporates Addendum EU SCCs which have been entered into to protect transfers subject to the General Data Protection Regulation (EU) 2016/679 then the Parties acknowledge that nothing in this Addendum impacts those Addendum EU SCCs.

INCORPORATION OF AND CHANGES TO THE EU SCCS

12. This Addendum incorporates the Addendum EU SCCs which are amended to the extent necessary so that:

    a. together they operate for data transfers made by the data exporter to the data importer, to the extent that UK Data Protection Laws apply to the data exporter's processing when making that data transfer, and they provide Appropriate Safeguards for those data transfers;

    b. Sections 9 to 11 override Clause 5 (Hierarchy) of the Addendum EU SCCs; and

    c. this Addendum (including the Addendum EU SCCs incorporated into it) is (1) governed by the laws of England and Wales and (2) any dispute arising from it is resolved by the courts of England and Wales, in each case unless the laws and/or courts of Scotland or Northern Ireland have been expressly selected by the Parties.

13. Unless the Parties have agreed alternative amendments which meet the requirements of Section 12, the provisions of Section 15 will apply.

14. No amendments to the Approved EU SCCs other than to meet the requirements of Section 12 may be made.

15. The following amendments to the Addendum EU SCCs (for the purpose of Section 12) are made:

    a. References to the "Clauses" means this Addendum, incorporating the Addendum EU SCCs;

b. In Clause 2, delete the words:

> "and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679";

c. Clause 6 (Description of the transfer(s)) is replaced with:

> "The details of the transfers(s) and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred) are those specified in Annex I.B where UK Data Protection Laws apply to the data exporter's processing when making that transfer.";

d. Clause 8.7(i) of Module 1 is replaced with:

> "it is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer";

e. Clause 8.8(i) of Modules 2 and 3 is replaced with:

> "the onward transfer is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer;"

f. References to "Regulation (EU) 2016/679", "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)" and "that Regulation" are all replaced by "UK Data Protection Laws". References to specific Article(s) of "Regulation (EU) 2016/679" are replaced with the equivalent Article or Section of UK Data Protection Laws;

g. References to Regulation (EU) 2018/1725 are removed;

h. References to the "European Union", "Union", "EU", "EU Member State", "Member State" and "EU or Member State" are all replaced with the "UK";

i. The reference to "Clause 12(c)(i)" at Clause 10(b)(i) of Module one, is replaced with "Clause 11(c)(i)";

j. Clause 13(a) and Part C of Annex I are not used;

k. The "competent supervisory authority" and "supervisory authority" are both replaced with the "Information Commissioner";

l. In Clause 16(e), subsection (i) is replaced with:

> "the Secretary of State makes regulations pursuant to Section 17A of the Data Protection Act 2018 that cover the transfer of personal data to which these clauses apply;";

m. Clause 17 is replaced with:

> "These Clauses are governed by the laws of England and Wales.";

n. Clause 18 is replaced with:

> "Any dispute arising from these Clauses shall be resolved by the courts of England and Wales. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of any country in the UK. The Parties agree to submit themselves to the jurisdiction of such courts."; and

o. The footnotes to the Approved EU SCCs do not form part of the Addendum, except for footnotes 8, 9, 10 and 11.

AMENDMENTS TO THIS ADDENDUM

16. The Parties may agree to change Clauses 17 and/or 18 of the Addendum EU SCCs to refer to the laws and/or courts of Scotland or Northern Ireland.

17. If the Parties wish to change the format of the information included in Part 1: Tables of the Approved Addendum, they may do so by agreeing to the change in writing, provided that the change does not reduce the Appropriate Safeguards.

18. From time to time, the ICO may issue a revised Approved Addendum which: a. makes reasonable and proportionate changes to the Approved Addendum, including correcting errors in the Approved Addendum; and/or b. reflects changes to UK Data Protection Laws; The revised Approved Addendum will specify the start date from which the changes to the Approved Addendum are effective and whether the Parties need to review this Addendum including the Appendix Information. This Addendum is automatically amended as set out in the revised Approved Addendum from the start date specified.

19. If the ICO issues a revised Approved Addendum under Section 18, if any Party selected in Table 4 “Ending the Addendum when the Approved Addendum changes”, will as a direct result of the changes in the Approved Addendum have a substantial, disproportionate and demonstrable increase in: a its direct costs of performing its obligations under the Addendum; and/or b its risk under the Addendum, and in either case it has first taken reasonable steps to reduce those costs or risks so that it is not substantial and disproportionate, then that Party may end this Addendum at the end of a reasonable notice period, by providing written notice for that period to the other Party before the start date of the revised Approved Addendum.

20. The Parties do not need the consent of any third party to make changes to this Addendum, but any changes must be made in accordance with its terms.

p.