

## **DATA PROCESSING ADDENDUM**

Last updated August 26, 2025

This Data Processing Addendum (“**DPA**”) supplements the Athennian Services Agreement and the Order Form(s) (together, the “**Agreement**”) entered into by and between the Customer named therein (together with its Affiliates, “**Customer**”) and Paper Interactive, Inc. or its subsidiary Athennian USA, Inc. (“**Athennian**”). Any capitalized terms not defined in this DPA shall have the meaning set forth in the Agreement.

In the event of a conflict between this DPA and the Agreement, this DPA shall supersede and control.

By signing this DPA, the signing Customer entity enters into this DPA on behalf of itself and, to the extent required under applicable Data Privacy Laws, in the name and on behalf of its Affiliates, if and to the extent Athennian Processes Personal Data for which such Affiliates qualify as the entity that determines the purposes and means of the Processing.

In the course of providing the Services to Customer pursuant to the Agreement, Athennian may Process Personal Data on behalf of Customer. The parties agree to comply with the provisions in this DPA with respect to any such Personal Data, each acting reasonably and in good faith.

### **HOW TO EXECUTE THIS DPA**

1. This DPA has been pre-signed on behalf of Athennian.
2. To complete this DPA, Customer must:
  - a. Complete the information in the signature block for Customer and sign on behalf of Customer, and
  - b. Complete the information in Annex I of the Appendix, and
  - c. Send the signed DPA to Athennian by email to [legal@athennian.com](mailto:legal@athennian.com) indicating the name of the Customer entity signing this DPA and referencing the applicable Agreement or Order Form by date and, in the case of an Order Form, quote number.
3. Upon receipt by Athennian of the validly completed DPA, as set forth above, this DPA will become legally binding.

### **DATA PROCESSING TERMS**

#### **1. DEFINITIONS**

All capitalized terms not defined in this DPA shall have the meanings set forth in the Agreement, and the following terms shall have the following meanings, unless the context otherwise requires:

“**Applicable Laws**” has the meaning set forth in the Agreement and, for the purpose of this DPA, includes Data Protection Laws.

“**Athennian Security Program**” means the Athennian Security Program applicable to the Services purchased by Customer, as updated from time to time, and accessible via Athennian’s Legal Portal, or as otherwise made reasonably available by Athennian.

“**CCPA**” means the *California Consumer Privacy Act*, Cal. Civ. Code § 1798.100 et seq., and its implementing regulations.

“**Controller**” means the entity which determines the purposes and means of the Processing of Personal Data.

**“Data Protection Laws”** means all laws and regulations, including laws and regulations of Canada and its provinces and territories, the United States and its states, the European Union, the European Economic Area (“**EEA**”) and their member states, Switzerland and the United Kingdom, if and to the extent applicable to the Processing of Personal Data under the Agreement. For greater certainty, Data Protection Laws includes the GDPR and the CCPA, to the extent applicable to the Processing of Personal Data under the Agreement.

**“Data Subject”** means the identified or identifiable natural person to whom Personal Data relates.

**“GDPR”** means the (i) General Data Protection Regulation (Regulation (EU) 2016/679, and (ii) UK GDPR (as amended by the Data Protection Act 2018 and the EU Exit Regulations).

**“Personal Data”** means any information relating to an identified or identifiable natural person, where such information is part of the Customer Data Processed under the Agreement.

**“Processing”** means any operation or set of operations which is performed on 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.

**“Processor”** means the entity which Processes Personal Data on behalf of the Controller.

**“Standard Contractual Clauses”** means the Standard Contractual Clauses (Data Controller to Data Processor) attached as an annex to the European Commission Implementing Decision (EU) 2021/914 of 4 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. The Standard Contractual Clauses are set out in Attachment 1 to this DPA.

**“Subprocessor”** means any Processor engaged by Athenian.

## **2. PROCESSING OF PERSONAL DATA**

**2.1 Roles of the Parties.** The parties agree that, with regard to the Processing of Personal Data, Customer is the Controller and Athenian is the Processor, and that Athenian may engage Subprocessors subject to the requirements in the section titled “Subprocessors”.

**2.2 Customer’s Processing of Personal Data** Customer will, in its use of the Services, Process Personal Data in accordance with the requirements of Data Protection Laws, including any applicable requirement to provide notice to Data Subjects of the use of Athenian as a Processor. For the avoidance of doubt, Customer’s instructions for the Processing of Personal Data shall comply with all Data Protection Laws. Customer shall have sole responsibility for the legality, reliability, integrity, accuracy and quality of Personal Data and for the means by which Customer acquires Personal Data, and Customer shall be responsible for establishing the legal basis for Processing under all Data Protection Laws. Customer represents and warrants to Athenian that (a) Customer has all rights, consents, permissions and legal authority as may be necessary to provide the Personal Data to Athenian and to authorize Athenian to Process the Personal Data to provide the Services, and (b) Customer’s use of the Services will not violate the rights of any Data Subject under Data Protection Laws.

**2.3 Athenian’s Processing of Personal Data.** The parties agree that this DPA, the Agreement, and the provision by Customer of instructions via features, tools and APIs made available by Athenian for the Services constitute Customer’s documented instructions regarding Athenian’s Processing of Personal Data (“**Documented Instructions**”), including with respect to transfers of personal data to a third country or an international organization. Athenian will Process Personal Data only in accordance with Documented Instructions, unless required to do so under Applicable Laws. Customer agrees that the Documented Instructions are Customer’s complete and final instructions to Athenian in relation to Processing of Personal Data. Additional instructions outside the scope of the Documented Instructions (if any) require prior written agreement between Athenian and Customer, including agreement on any additional fees payable by Customer to Athenian for carrying out such instructions. Customer

will ensure that the Documented Instructions comply with all Applicable Laws, and that the Processing of Personal Data in accordance with the Documented Instructions will not cause Athennian to be in breach of any Applicable Laws.

#### 2.4 Details of the Processing.

- (i) *Subject matter.* The subject matter of the Processing under this DPA is Personal Data provided by Customer to Athennian in connection with the Services.
- (ii) *Duration.* The duration of the Processing under this DPA is the duration of the subscription term for the Services, as provided in the Agreement.
- (iii) *Nature and purpose.* The nature and purpose of the Processing under this DPA is the provision of the Services ordered by Customer under the Agreement, as more particularly described in the Documentation, and which are generally SaaS solutions for legal entity management.
- (iv) *Type of Personal Data.* The type of Personal Data that will be Processed under this DPA is Personal Data provided by Customer to the Services, as more particularly described in the Documentation, including but not limited to name, title, position, personal address, business address, citizenship, relationship to managed legal entity, role within managed legal entity, contact information, and identification.
- (v) *Categories of Data Subjects.* The categories of Data Subjects whose data will be Processed under this DPA may include (i) shareholders, partners, limited partners, directors, officers, employees and other individuals connected with corporations and other legal entities, the records of which are managed by Customer using the Services, and (ii) Customer's employees and end-users.

**2.5 Use and Disclosure of Personal Data.** Athennian will only use Personal Data to provide the Services to Customer, except with the prior written consent of Customer or as otherwise expressly permitted under the Agreement or this DPA, or unless otherwise required under Applicable Laws. Athennian will not disclose Personal Data outside of Athennian or its Affiliates except (a) as Customer directs or as required to provide the Services, (b) to Customer's third party service providers as directed by Customer, (c) to Subprocessors as described in the section titled "Subprocessors", (d) as otherwise described in the Agreement or this DPA, or (e) as required by Applicable Laws.

**2.6 Disclosure of Personal Data under Applicable Laws.** If Athennian is required to disclose Personal Data by Applicable Laws to which Athennian is subject, then Athennian will promptly notify Customer unless prohibited by law. On receipt of any other third-party request for Personal Data, Athennian will promptly notify Customer unless prohibited by law. Athennian will reject the request unless required by law to comply. If the request is valid, Athennian will attempt to redirect the third party to request the Personal Data directly from Customer.

**2.7 Storage and Transfer of Personal Data.** For the purposes of this section, "**Region**" means Canada and the United States, unless a different region is specified in the Order Form. Except as described elsewhere in this DPA or the Agreement, Personal Data that Athennian processes on Customer's behalf may be transferred to, and stored and Processed in, the Region or any other location where Athennian or its Subprocessors operate. All transfers of Personal Data out of the European Union, European Economic Area, and Switzerland by the Services shall be governed by the terms of the section titled "GDPR Specific Provisions." All Personal Data that is Processed directly by Athennian will be stored at rest in the Region and Processed directly by Athennian within the Region, except as provided below. Subprocessors may store or Process Customer Data outside the Region. Athennian may transfer Personal Data from the Region, with the consent of Customer, or as necessary to comply with Applicable Laws or a binding order of a Governmental Authority (such as a subpoena or court order). If Customer provides Personal Data as part of a request for Support Services, Athennian may Process that Personal Data in the locations from which

Athennian provides those Support Services. To investigate fraud, abuse or violations of the Agreement, Athennian may Process Personal Data where Athennian maintains its support and investigation personnel. Athennian does not control or limit the locations from which Customer or Customer's end-users may access Personal Data or to which they may move Personal Data (except as otherwise provided under "Export Compliance" in the Agreement). Customer may interconnect the Services with certain other services provided by third parties. Athennian does not control or limit the locations from such third parties may access Personal Data or to which they may move Personal Data (except as otherwise provided under "Export Compliance" in the Agreement).

### 3. RIGHTS OF DATA SUBJECTS

**3.1 Data Subject Request.** Athennian will, to the extent legally permitted, promptly notify Customer if Athennian receives a request from a Data Subject ("**Data Subject Request**") to exercise any right of the Data Subject under Data Protection Laws, including any right of access, right to rectification, restriction of Processing, erasure, data portability, objection to the Processing, or a right not to be subject to automated individual decision making. Taking into account the nature of the Processing, Athennian will assist Customer by appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of Customer's obligation to respond to a Data Subject Request under Data Protection Laws. In addition, to the extent Customer, in its use of the Services, does not have the ability to address a Data Subject Request, Athennian will on Customer's request provide commercially reasonable efforts to assist Customer in responding to such Data Subject Request, to the extent Athennian is legally permitted to do so and the response to such Data Subject Request is required under Data Protection Laws. Customer will pay for assistance provided by Athennian at the Consulting Services Rates.

### 4. ATHENNIAN PERSONNEL

**4.1 Confidentiality.** Athennian will ensure that its personnel engaged in the Processing of Personal Data are informed of the confidential nature of the Personal Data, have received appropriate training on their responsibilities, and have executed written confidentiality agreements.

**4.2 Limitation of Access.** Athennian will ensure that only those Athennian personnel performing Services in accordance with the Agreement have access to Personal Data.

### 5. SUBPROCESSORS

**5.1 Appointment of Subprocessors.** Customer agrees that Athennian may engage third-party Subprocessors in connection with the provision of the Services.

**5.2 Agreements with Subprocessors.** Athennian will enter into a written agreement with each Subprocessor (a) permitting the Subprocessor to access and use Personal Data only to deliver the services Athennian has retained the Subprocessor to provide and for no other purpose, and (b) requiring the Subprocessor to provide at least the level of data protection required of Athennian under this DPA.

**5.3 List of Current Subprocessors and Notification of New Subprocessors.** A list of the Subprocessors that are currently engaged by Athennian to carry out Processing activities on Personal Data on behalf of Customer is available on the Legal Portal. The Legal Portal also provides a mechanism by which Customer can subscribe to receive notifications of new Subprocessors for the Services. If Customer subscribes, Athennian will provide notification of each new Subprocessor at least 14 days before authorizing the new Subprocessor to Process Personal Data in connection with the provision of the applicable Services.

**5.4 Objection Right for New Subprocessors.** Customer may object to Athennian's use of a new Subprocessor where there are reasonable grounds to believe that the new Subprocessor will be unable to comply with the terms of this DPA or the Agreement. If Customer objects to Athennian's use of a new Subprocessor, Customer will notify Athennian promptly in writing within ten days after notification regarding such Subprocessor (as provided above). Customer's failure to object in writing within such time period will constitute approval to use the new Subprocessor.

Customer acknowledges that Athennian's inability to use a particular new Subprocessor may result in delay in performing the Services, inability to perform the Services, or increased fees. Athennian will notify Customer in writing of any change to Services or fees that would result from Athennian's inability to use a new Subprocessor to which Customer has objected. Customer may either execute a written amendment to the Agreement implementing such change or elect to terminate the Agreement by notice to Athennian. If Customer elects to terminate the Agreement, then Customer will pay to Athennian a termination fee equal to the total of the minimum fees payable for the Services for the remainder of the subscription term applicable to the Services. Such termination will not constitute termination for breach of the Agreement. Athennian will have a right to terminate the Agreement if Customer unreasonably objects to a Subprocessor, or does not agree to a written amendment to the Agreement implementing changes in fees or Services resulting from the inability to use the Subprocessor at issue.

**5.5 Liability.** Athennian shall be liable for the acts and omissions of its Subprocessors to the same extent that Athennian would be liable if performing the services of each Subprocessor directly under the terms of this DPA, except as otherwise set forth in the Agreement.

## **6. SECURITY**

**6.1 Athennian Security Measures.** Athennian will implement and maintain appropriate technical and organizational measures to protect Personal Data, including measures to protect Personal Data from unauthorized access, use, modification, encryption, deletion, loss or disclosure. Those measures will be described in the Athennian Security Program. Athennian will make that Athennian Security Program available to Customer, along with other information reasonably requested by Customer regarding Athennian security practices and policies.

**6.2 Customer Responsibilities.** Customer is solely responsible for making an independent determination as to whether Athennian's technical and organizational measures for the Services meet Customer's requirements, including any of its security obligations under Applicable Laws. Customer agrees that (taking into account the state of the art, the costs of implementation, and the nature, scope, context and purposes of the Processing, as well as the risks to individuals) Athennian's technical and organizational measures for the Services provide a level of security appropriate to the risk.

**6.3 Third-Party Certifications and Audits.** Athennian has obtained the third-party certifications and audits set forth in the Athennian Security Program. On Customer's written request at reasonable intervals, and subject to the confidentiality obligations set forth in the Agreement, Athennian will make available to Customer a copy of Athennian's then most recent third-party audits or certifications, as applicable.

## **7. AUDITS**

**7.1 Athennian Audits.** For the purpose of evaluating Athennian's compliance with the terms of this DPA, Athennian will provide Customer's internal or external auditors with escorted access to Athennian's office premises and to documents and records related to the Services, at Customer's expense. For greater certainty, Customer auditors will not be entitled to access the data centers of the data center service provider from which the Services are provided without the consent of the data center service provider (which Athennian will request if asked to do so by Customer). Athennian will provide the Customer auditors with any assistance that they may reasonably request in connection with such audits. The audits must be conducted in a manner that minimizes the disruption on Athennian's operations, during normal business hours, on at least 30 days' prior notice, and not more than once each calendar year. External auditors must enter into a nondisclosure agreement with Athennian substantially similar to the confidentiality provisions of the Agreement. Customer will pay for assistance provided by Athennian at the Consulting Services Rates.

**7.2 Demonstration of Compliance.** At Customer's reasonable written request, Athennian will provide Customer with information to demonstrate Athennian's compliance its obligations under this DPA. Customer will pay for work performed by Athennian in response to the request at the Consulting Services Rates.

## 8. PERSONAL DATA INCIDENT MANAGEMENT AND NOTIFICATION

Athennian maintains security incident management policies and procedures specified in the Athennian Security Program. Athennian will notify Customer without undue delay, and in any event within 24 hours, after becoming aware of the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data transmitted, stored or otherwise Processed by Athennian or its Subprocessors (a **“Personal Data Incident”**), as well as any specific attempted Personal Data Incident. Athennian will make reasonable efforts to identify the cause of such Personal Data Incident and take those steps as Athennian deems necessary and reasonable to remediate the cause of such a Personal Data Incident to the extent the remediation is within Athennian’s reasonable control. These obligations shall not apply to incidents that are caused by Customer or Customer’s Users.

## 9. RETURN AND DELETION OF PERSONAL DATA

On request by Customer made within 90 days after the expiry or termination of the Agreement, Athennian will make any Personal Data in Athennian’s possession or control available to Customer for export or download in JSON/BSON or similar open source format as reasonably agreed between the parties. After such 90-day period, Athennian will have no obligation to maintain or provide any Personal Data, and will delete or destroy all copies of Personal Data in its systems or otherwise in its possession or control, unless legally prohibited by Applicable Laws.

## 10. LIMITATION OF LIABILITY

Each party’s and all of its Affiliates’ liability, taken together in the aggregate, arising out of or related to this DPA, whether in contract, tort or under any other theory of liability, is subject to the ‘Limitation of Liability’ section of the Agreement, and any reference in such section to the liability of a party means the aggregate liability of that party and all of its Affiliates under the Agreement and this DPA together.

## 11. GDPR SPECIFIC PROVISIONS

**11.1 Application.** This section titled “GDPR Specific Provisions” shall apply only if and to the extent that Processing of Personal Data is governed by the GDPR. In the event of any inconsistency between a term of this section and another term of this DPA, the term of this section shall apply for GDPR-Subject Personal Data.

**11.2 Definition.** In this section titled “GDPR Specific Provisions”, the following terms shall have the following meanings:

**“GDPR-Subject Personal Data”** shall mean Personal Data (1) that is Processed by Athennian, and (2) for which the Processing by Athennian is governed by the GDPR.

**11.3 GDPR Requirements.** Athennian will Process GDPR-Subject Personal Data in accordance with the GDPR requirements directly applicable to Athennian’s provision of the Services.

**11.4 Processing of GDPR-Subject Personal Data under Applicable Laws of Europe.** Athennian will Process GDPR-Subject Personal Data only in accordance with Documented Instructions, unless required to do so under Applicable Laws of a member state of the European Union or the EEA to which Athennian is subject. If Athennian is required to Process GDPR-Subject Personal Data by Applicable Laws of a member state of the European Union or the EEA to which Athennian is subject, then Athennian will promptly notify Customer unless prohibited by law.

**11.5 Records of Processing Activities.** Athennian will maintain all records required by Article 30(2) of the GDPR and, to the extent applicable to the Processing of Personal Data on behalf of Customer, will make those records available to Customer on request.

**11.6 Data Protection Impact Assessment and Prior Consultation.** Taking into account the nature of the Services and the information available to Athennian, Athennian will assist Customer in complying with Customer’s obligations in respect of data protection impact assessments and prior consultation pursuant to Articles 35 and 36 of the GDPR, to

the extent Customer does not otherwise have access to the relevant information and to the extent such information is available to Athennian. Customer will pay for assistance provided by Athennian at the Consulting Services Rates.

**11.7 Application of Standard Contractual Clauses.** The Standard Contractual Clauses will not apply to GDPR Subject Personal Data that is transferred, either directly or by onward transfer, to (a) any country that is a member of the European Union or the EEA, (b) any country recognised by the European Commission as providing an adequate level of protection for personal data (as described in the GDPR), (c) any organization within the Athennian group of companies that is subject to binding corporate rules under the GDPR, or (d) any country or organization where the transfer is otherwise permitted under the GDPR. The Standard Contractual Clauses will apply to all other transfers of GDPR-Subject Personal Data to a country that is not a member of the European Union or the EEA.

**11.8 Standard Contractual Clauses, Terms.** If and to the extent that the Standard Contractual Clauses apply, then:

- (i) For the purposes of Clauses 8.1 and 8.8 of the Standard Contractual Clauses, the Documented Instructions are deemed to be Customer's complete and final instructions to Athennian in relation to Processing of Personal Data.
- (ii) For the purposes of Clauses 8.9 of the Standard Contractual Clauses, the parties agree that the obligation of Athennian to permit audits shall be satisfied by Athennian's provision of third-party audits or certifications under the section titled "Third-Party Certifications and Audits."
- (iii) For the purposes of Clause 9 of the Standard Contractual Clauses, Customer agrees that Athennian may engage Subprocessors as described in the section titled "Subprocessors."
- (iv) For the purposes of Clause 9(c) of the Standard Contractual Clauses, copies of any Subprocessor agreement that must be provided by Athennian to Customer may have all commercial information, or clauses unrelated to the Standard Contractual Clauses or their equivalent, removed by Athennian beforehand; and, that such copies will be provided by Athennian, in a manner to be determined in its discretion, only on request by Customer.
- (v) For the purposes of Clause 16(d) of the Standard Contractual Clauses, the parties agree that the certification of deletion of Personal Data will be provided by Athennian to Customer only on Customer's request.
- (vi) In the event of any inconsistency between a term of the Standard Contractual Clauses as amended by this section and another term of this DPA, the term of the Standard Contractual Clauses shall apply.

## **12. CCPA SPECIFIC PROVISIONS**

**12.1 Application.** This section titled "CCPA Specific Provisions" shall apply only if and to the extent that Processing of Personal Data is governed by the CCPA. In the event of any inconsistency between a term of this section and another term of this DPA, the term of this section shall apply for CCPA-Subject Personal Data.

**12.2 Definitions.** In this section titled "CCPA Specific Provisions", the following terms shall have the following meanings:

**"CCPA-Subject Personal Data"** shall mean Personal Information (1) that is Processed by Athennian as part of the Services, and (2) for which the Processing by Athennian is governed by the CCPA.

**"Personal Information"** shall have the meaning provided under the CCPA.

**"Sell"** shall have the meaning provided under the CCPA.

**12.3 CCPA Requirements.** For the purposes of this DPA, Athennian is a “service provider” to Customer under the CCPA. Customer may be either a “business” or a “service provider” under the CCPA. Athennian will Process CCPA-Subject Personal Data in accordance with the CCPA requirements directly applicable to Athennian’s provision of the Services. Athennian will not: (a) retain, use, or disclose CCPA-Subject Personal Data except as permitted in the Agreement, this DPA, or the CCPA; or (b) Sell CCPA-Subject Personal Data.

**IN WITNESS WHEREOF**, the parties have executed this DPA by persons duly authorized.

**PAPER INTERACTIVE, INC dba “Athennian”**


DocuSigned by:  
  
Per: \_\_\_\_\_  
FB05D0213E114A5...

Name: **Adrian Camara**

Title: **Chief Executive Officer**

Date: 26<sup>th</sup> August 2025.

**ATHENNIAN USA, INC.**

DocuSigned by:  
  
Per: \_\_\_\_\_  
293F8C73BC3245B...

Name: **Carlos Ramos**

Title: **VP of Revenue**

Date: 26<sup>th</sup> August 2025.

**CUSTOMER**

Per: \_\_\_\_\_  
Name: \_\_\_\_\_  
Title: \_\_\_\_\_  
Date: \_\_\_\_\_

Customer Name:	
Date of Customer’s Agreement with Athennian:	
Order Form Number:	



## **Attachment 1 to the Data Processing Addendum**

### **The Standard Contractual Clauses (Processors)**

#### **SECTION I Clause 1 Purpose and scope**

- a. The purpose of these standard contractual clauses is to ensure compliance with the requirements of 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) for the transfer of personal data to a third country.
- b. The Parties:
  - i. the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter 'entity/ies') transferring the personal data, as listed in Annex I.A (hereinafter each 'data exporter'), and
  - ii. the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A (hereinafter each 'data importer') have agreed to these standard contractual clauses (hereinafter: 'Clauses').
- c. These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.
- d. The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

#### **Clause 2 Effect and invariability of the Clauses**

- a. These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 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, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.
- b. These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

#### **Clause 3 Third-party beneficiaries**

- a. Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:
  - i. Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;
  - ii. Clause 8 – Clause 8.1(b), 8.9(a), (c), (d) and (e);
  - iii. Clause 9 – Clause 9(a), (c), (d) and (e); iv. Clause 12 – Clause 12(a), (d) and (f);
  - v. Clause 13;
  - vi. Clause 15.1(c), (d) and (e);
  - vii. Clause 16(e);
  - viii. Clause 18 – Clause 18(a) and (b).
- b. Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

#### **Clause 4 Interpretation**

- a. Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.
- b. These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.
- c. These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

#### **Clause 5 Hierarchy**

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

#### **Clause 6 - Description of the transfer(s)**

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

#### **Clause 7 – Docking clause**

- a. An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.
- b. Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.
- c. The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

### **SECTION II – OBLIGATIONS OF THE PARTIES Clause 8 - Data protection safeguards**

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

#### **8.1 Instructions**

- a. The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.
- b. The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

#### **8.2 Purpose limitation**

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the data exporter.

#### **8.3 Transparency**

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

#### 8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

#### 8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

#### 8.6 Security of processing

- a. The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter 'personal data breach'). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.
- b. The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.
- c. In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all 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.
- d. The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

#### 8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter 'sensitive data'), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

## 8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

- i. the onward transfer is to a country benefiting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;
- ii. the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;
- iii. the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or
- iv. the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

## 8.9 Documentation and compliance

- a. The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.
- b. The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.
- c. The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.
- d. The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.
- e. The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

## Clause 9 Use of subprocessors

- a. GENERAL WRITTEN AUTHORISATION. The data importer has the data exporter's general authorisation for the engagement of subprocessor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of subprocessors at least 14 days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the subprocessor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.
- b. Where the data importer engages a subprocessor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the subprocessor complies with the obligations to which the data importer is subject pursuant to these Clauses.

- c. The data importer shall provide, at the data exporter's request, a copy of such a subprocessor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.
- d. The data importer shall remain fully responsible to the data exporter for the performance of the subprocessor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the subprocessor to fulfil its obligations under that contract.
- e. The data importer shall agree a third-party beneficiary clause with the subprocessor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter shall have the right to terminate the subprocessor contract and to instruct the subprocessor to erase or return the personal data.

#### **Clause 10 - Data subject rights**

- a. The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.
- b. The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.
- c. In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

#### **Clause 11 - Redress**

- a. The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.
- b. In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.
- c. Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:
  - i. lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;
  - ii. refer the dispute to the competent courts within the meaning of Clause 18.
- d. The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.
- e. The data importer shall abide by a decision that is binding under the applicable EU or Member State law.
- f. The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

#### **Clause 12 - Liability**

- a. Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.
- b. The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its subprocessor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

- c. Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its subprocessor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.
- d. The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its subprocessor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.
- e. Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.
- f. The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.
- g. The data importer may not invoke the conduct of a subprocessor to avoid its own liability.

#### **Clause 13 - Supervision**

- a. SUPERVISORY AUTHORITIES
  - i. where the data exporter is established in an EU Member State, the supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.
  - ii. where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679, the supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.
  - iii. where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679, the supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.
- b. The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

### **SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES**

#### **Clause 14 - Local laws and practices affecting compliance with the Clauses**

- a. The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

- b. The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:
  - i. the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;
  - ii. the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards;
  - iii. any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.
- c. The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.
- d. The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.
- e. The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).
- f. Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

## **Clause 15 - Obligations of the data importer in case of access by public authorities**

### **15.1 Notification**

- a. The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:
  - i. receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or
  - ii. becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.
- b. If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

- c. Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).
- d. The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.
- e. Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

#### **15.2 Review of legality and data minimisation**

- a. The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).
- b. The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.
- c. The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

#### **SECTION IV – FINAL PROVISIONS Clause 16 - Non-compliance with the Clauses and termination**

- a. The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.
- b. In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).
- c. The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:
  - i. the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;
  - ii. the data importer is in substantial or persistent breach of these Clauses; or
  - iii. the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

- d. Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer



warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

- e. Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

**Clause 17 - Governing law**

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of Ireland.

**Clause 18 - Choice of forum and jurisdiction**

- a. Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.
- b. The Parties agree that those shall be the courts of Ireland.
- c. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.
- d. The Parties agree to submit themselves to the jurisdiction of such courts.

APPENDIX

EXPLANATORY NOTE: It must be possible to clearly distinguish the information applicable to each transfer or category of transfers and, in this regard, to determine the respective role(s) of the Parties as data exporter(s) and/or data importer(s). This does not necessarily require completing and signing separate appendices for each transfer/category of transfers and/or contractual relationship, where this transparency can be achieved through one appendix. However, where necessary to ensure sufficient clarity, separate appendices should be used.


ANNEX I


A. LIST OF PARTIES

**Data exporter(s):** You are the data exporter, and the purpose of the export is to obtain the Services ordered by You under the Agreement, as more particularly described in the Documentation, and which are generally SaaS solutions for legal entity management.

Name:	
Address:	
Contact person’s name, position and contact details:	
Activities relevant to the data transferred under these Clauses:	Processing of personal data related to legal entity management.
Signature:	
Date:	
Role:	Controller

**Data importer(s):** The data importer is Paper Interactive, Inc., dba Athennian, a provider of SaaS solutions for legal entity management.

Name:	Paper Interactive, Inc. dba Athennian
Address:	Suite 202, 838 11th Avenue SW, Calgary, AB T2R 0E5.
Contact person’s name, position and contact details:	<b>Adrian Camara, Chief Executive Officer.</b> <a href="mailto:privacy@athennian.com">privacy@athennian.com</a>
Activities relevant to the data transferred under these Clauses:	Processing of personal data related to legal entity management.
Signature:	<div>DocuSigned by:  FB05D0213E114A5...</div>
Date:	26th August 2025.
Role:	Processor

Name:	Athennian USA, Inc.
Address:	c/o Paper Interactive, Inc. Suite 202, 838 11th Avenue SW, Calgary, AB T2R 0E5.
Contact person's name, position and contact details:	<b>Carlos Ramos, VP of Revenue.</b> <a href="mailto:privacy@athennian.com">privacy@athennian.com</a>
Activities relevant to the data transferred under these Clauses:	Processing of personal data related to legal entity management.
Signature:	DocuSigned by:  293F8C73BC3245D...
Date:	26th August 2025.
Role:	Processor

## B. DESCRIPTION OF TRANSFER

**Categories of data subjects whose personal data is transferred:** The personal data transferred concern the following categories of data subjects: (i) shareholders, partners, limited partners, directors, officers, employees and other individuals connected with corporations and other legal entities, the records of which are managed by Customer using the Services, and (ii) Customer's employees and end-users.

**Categories of personal data transferred:** The personal data transferred concern the following categories of data: Personal Data provided by Customer to the Services, as more particularly described in the Documentation, including but not limited to name, title, position, personal address, business address, citizenship, relationship to managed legal entity, role within managed legal entity, contact information, and identification.

**Sensitive data transferred:** The personal data transferred concern the following special categories of data: the use of the service for legal entity management would not typically include special categories of data, but the functionality of the Services allows Customer to submit special categories of data in some circumstances, in its sole discretion.

**The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis):** The data will be transferred on a continuous basis, for the duration of the subscription term for the Services, as provided in the Agreement.

**Nature of the processing:** The nature of the processing includes creation, organisation, structuring, storage, retrieval, archiving, and other functions as described in the Agreement and the Documentation.

**Purpose(s) of the data transfer and further processing:** The personal data transferred will be subject to the following basic processing activities: the personal data transferred will be processed for the purpose of providing Services to Customer under the Agreement.

**The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period:** Personal data will be retained according to Our documented data retention policies and procedures.

**For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing:** The subject matter and nature of the processing undertaken by each subprocessor shall be identified in the list of subprocessors provided pursuant to Clause 9 and Section 5.3 of the DPA.

### C. COMPETENT SUPERVISORY AUTHORITY

In accordance with Clause 13 above (choose one only):

- ☐ The data exporter is established in an EU Member State, so the supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer is: \_\_\_\_\_; OR
- ☐ The data exporter is **not** established in an EU Member State, **but falls within the territorial scope** of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679, so the supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established shall act as competent supervisory authority, namely: DUTCH DATA PROTECTION AUTHORITY ; OR
- ☐ The data exporter is **not** established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679, so **the supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located shall act as competent supervisory authority**, namely: \_\_\_\_\_; OR
- ☐ The Standard Contractual Clauses do not apply to the Data Subjects for whom Customer is Data Controller.

### ANNEX II

#### TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA EXPLANATORY NOTE:

The technical and organisational measures must be described in specific (and not generic) terms. See also the general comment on the first page of the Appendix, in particular on the need to clearly indicate which measures apply to each transfer/set of transfers.

**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:**

Athennian will implement and maintain appropriate technical and organizational measures to protect personal data, including measures to protect personal data from unauthorized access, use, modification, encryption, deletion, loss or disclosure. Those measures will be described in the Athennian Security Program. Athennian will make that Athennian Security Program available to Customer, along with other information reasonably requested by Customer regarding Athennian security practices and policies.

Relevant Certifications:

- SOC2 Type II (12-month)

Technical and Organizational Measures include but are not limited to:

- Measures for encryption of personal data
- Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services
- Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident

- Processes for regularly testing, assessing, and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing
- Measures for user identification and authorisation
- Measures for the protection of data during transmission
- Measures for the protection of data during storage
- Measures for ensuring physical security of locations at which personal data are processed
- Measures for ensuring events logging
- Measures for ensuring system configuration, including default configuration
- Measures for internal IT and IT security governance and management
- Measures for certification/assurance of processes and products
- Measures for ensuring limited data retention
- Measures for ensuring accountability
- The sufficiency of Technical and Organizational Measures of Subprocessors shall be evaluated by the processor on an annual basis.