HIGHWIRE

Highwire Data Processing Addendum

1. Purpose, Scope, and Users

This Data Processing Addendum (the "Addendum") forms a supplement to the Highwire Privacy Policy. The services provided by Highwire may include the processing, collection, or storage of data on behalf of a contractor or client. As such, Highwire performs its data processing services in compliance with the Data Protection Laws defined below.

2. Definitions

- **Applicable Data Protection Legislation:** the laws and regulations applicable to the respective party's processing of Personal Data, including, where applicable, (i) the General Data Protection Regulation (EU) 2016/679 of the European Parliament and of the Council ("**GDPR**"), as amended and supplemented, as the case may be, by the relevant EU Member States laws and regulations in which a client or contractor directly or indirectly operates, (ii) the UK Data Protection Act 2018 and the UK General Data Protection Regulation ("**UK GDPR**"), (iii) the Australian Privacy Act 1988 and National Privacy Principles, (iv) the California Consumer Privacy Act of 2018, as amended by the California Privacy Rights Act of 2020, and any related regulations or guidance (collectively, the "**CCPA**"), (v) the Canadian Personal Information Protection and Electronic Documents Act ("**PIPEDA**"), and (vi) any other international, federal, state, provincial, and local privacy or data protection laws, rules, regulations, directives and governmental requirements currently in effect and as they become effective.

- **Data Subject**: an individual who is the subject of the Personal Data and to whom or about whom the Personal Data relates or identifies, directly or indirectly.

- **Data Privacy Framework**: the EU-US Data Privacy Framework, the UK Extension to the EU-US Data Privacy Framework, and the Swiss-US Data Privacy Framework which were respectively developed in furtherance of transatlantic commerce by the US Department of Commerce and the European Commission, the UK Government, and the Swiss Federal

Administration to provide US organizations with reliable mechanisms for Personal Data transfers to the United States from the EEA, the UK (and Gibraltar), and Switzerland while ensuring data protection that is consistent with EU, UK, and Swiss law.

- **EEA:** refers to the European Economic Area, consisting of all member states of the European Union and Iceland, Norway, and Liechtenstein.

- **EU SCCs**: the European Commission's standard contractual clauses for the transfer of personal data from the European Union to third countries, as set out in the Annex to Commission Decision (EU) 2021/914, a copy of which is available at https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc/standard-contractual-clauses-international-transfers_en.

- **Personal Data**: any information Highwire processes that (i) identifies or relates to an individual who can be identified directly or indirectly from that data alone or in combination with other information in Highwire's possession or control, or (ii) the Applicable Data Protection Legislation otherwise defines as protected personal data or personal information.

- **Processing, processes, and process**: any activity that involves the use of Personal Data, or as the Applicable Data Protection Legislation may otherwise define the terms “processing,” “processes,” or “process.” It includes obtaining, recording, or holding the data, or carrying out any operation or set of operations on the data, including organizing, amending, retrieving, using, disclosing, erasing, or destroying it. Processing also includes transferring Personal Data to third parties.

- **Security Breach**: a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data.

- **Subject Rights Request**: the exercise by a Data Subject of his or her rights under the Applicable Data Protection Legislation.

- **UK Addendum**: the UK Information Commissioner’s Office’s International Data Transfer Addendum to the European Commission’s Standard Contractual Clauses, a copy of which is available

at https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-data-transfer-agreement-and-guidance/.

3. Roles and Scope of Processing

3.1 Highwire's Role

Highwire acknowledges and agrees that:

(a) Highwire is a data processor to the extent the processing of Personal Data is carried out on behalf of and under the direction of a client or contractor, such as processing of a client or contractor's business email and title to create secure accounts in the Highwire application or processing safety and financial data contained in the prequalification forms provided and uploaded to the Highwire application by a contractor.

(b) Highwire is a data controller to the extent the processing of Personal Data is for Highwire's purposes in connection with the provision of the Highwire Services or for Highwire's legitimate business interests, such as billing, account management, technical support, product development, analytical uses, and sales and marketing (e.g., sending newsletters to client and contractor users).

3.2 Client or Contractor Role

Highwire's clients and contractors acknowledge and agree that:

(a) The client and contractor shall have the sole responsibility for the accuracy, quality, and legality of the Personal Data submitted to Highwire and the Highwire application (either by the client and contractor or by their Data Subjects directly).

(b) The client and contractor shall only upload and submit to Highwire and the Highwire application Personal Data that was obtained from Data Subjects in compliance with the Applicable Data Protection Legislation.

(c) The client and contractor shall ensure they have all necessary consents and notices in place and have satisfied all other requirements under the Applicable Data Protection Legislation to enable lawful transfer of Personal Data (including Sensitive Data) to Highwire and permit Highwire's processing of Personal Data in various jurisdictions pursuant to this DPA.

(d) Where consent is the lawful basis for processing Personal Data or is otherwise required for the use of the Highwire Services, Client and contractor shall, at all times, make available and

maintain (i) a mechanism for obtaining such consent from Data Subjects, and (ii) a mechanism for Data Subjects to withdraw such consent, in each case in accordance with the Applicable Data Protection Legislation.

(e) Client and contractor's use of the Highwire Services will not violate the rights of any Data Subjects.

4. Details of Data Processing

4.1 Nature and Purpose of Processing

Highwire will process Personal Data only as necessary to perform the Services pursuant to all executed client License and Services Agreements and all executed Contractor Participation Agreements.

4.2 Duration of Processing

Highwire will process Personal Data only for the duration of the terms specified in an executed client License and Services Agreement and an executed Contractor Participation Agreement.

4.3 Categories of Data Subjects

Clients and contractors may submit Personal Data to Highwire, the extent of which is determined and controlled by the client and contractor in their sole discretion, and which may include, but is not limited to, the following categories of Data Subjects:

- Authorized administrative users of a client and contractor.
- Employees of a client and contractor, as designated by an administrative user to require access to the Highwire platform.
- A client's general contractor users.
- Other authorized third-party users with whom a client conducts business.

4.4 Categories of Personal Data

Clients and contractors may submit Personal Data to Highwire, the extent of which is determined and controlled by the client and contractor in their sole discretion, and which may include, but is not limited to, the following categories of Personal Data:

- Client and contractor identity data (such as full name and title).
- Client and contractor contact data (such as email, office phone, and cell phone).

- Client and contractor professional data (such as occupation, job competencies, and professional certifications).
- Client and contractor location data (such as IP address and project worksite locations).
- Client and contractor technical and usage data (such as browser type and version, time zone setting and location, and language settings).
- Clients and contractors may upload content to the Highwire platform, which may include special categories of data, the extent of which is determined and controlled by the client and contractor in their sole discretion. Such special categories of data may include, but are not limited to, trade-union memberships and status as a disadvantaged business enterprise.

5. Highwire's Obligations

Highwire will process Personal Data only for the specific purposes of the transfer as set out in Section 4. Highwire may process Personal Data for another purpose (i) where it has obtained the Data Subject's prior consent, (ii) where necessary for the establishment, exercise or defense of legal claims in the context of specific administrative, regulatory or judicial proceedings; or (iii) where necessary to protect the vital interests of the Data Subject or of another natural person.

To the extent Highwire acts as a data processor of a client or contractor, Highwire shall process Personal Data on the instructions of the client or contractor. The parties agree that a client or contractor's instructions shall be within the scope of this Data Processing Addendum. Any additional requested instructions require the prior written consent of Highwire. Highwire shall promptly notify the client or contractor if, in Highwire's opinion, such instruction violates any Applicable Data Protection Legislation. Where applicable, the client or contractor shall be responsible for any communications, notifications, assistance, and authorizations that may be required in connection with its Data Subjects.

5.1 Highwire's Employees

Highwire will ensure that all employees who have access to or are involved in processing Personal Data (i) have undertaken training on the Applicable Data Protection Legislation relating to handling Personal Data and how it applies to their particular duties; and are aware both of Highwire's duties and their personal duties and obligations under the Applicable Data Protection Legislation and this DPA; and (ii) are under appropriate obligation of confidentiality (whether a contractual or statutory duty).

Highwire will take reasonable steps to ensure the reliability, integrity, and trustworthiness of any Highwire employee with access to Personal Data.

6. Security

Highwire has implemented appropriate technical and organizational measures to ensure a level of security appropriate to the risks associated with Highwire's data processing services, including the security measures described below. Highwire may review and update our security measures from time to time, provided that any such updates shall not materially diminish the overall security of the Highwire Services.

6.1 Security Overview

Highwire software-as-a-service applications ("SaaS Services") are designed with security in mind. The security controls detailed below are subject to change from time to time; however, any changes will maintain or improve the overall security posture of the SaaS platform.

6.2 Audits and Certifications

The Highwire application, and related Highwire services, are certified annually under ISO/IEC 27001:2022 and SOC2 Type 1 frameworks. In addition, Highwire contracts with Amazon Web Services (AWS) for cloud storage services. While AWS falls outside the scope of Highwire's certifications, AWS provides top-tier facilities which have achieved multiple accreditations, including SOC2, ISO/IEC 27001:2022, ISO/IEC 27017:2015, ISO/IEC 27018:2019, ISO/IEC 27701:2019, ISO/IEC 22301:2019, ISO/IEC 20000-1:2018, and ISO/IEC 9001:2015. AWS facilities also provide state-of-the-art physical protection safeguards where Highwire's client and contractor data is stored and processed. For more information about AWS, please visit https://aws.amazon.com/compliance/programs/

6.3 Disaster Recovery and Business Continuity

To ensure the Highwire application maintains a high degree of system availability, Highwire uses a designated backup/failover AWS data center that is located in a separate geographic location from its normal production data processing facility. This ensures Highwire can respond quickly to any environmental, physical, or accidental event that may cause interruption to the production AWS facility.

Highwire maintains a comprehensive Disaster Recovery and Business Continuity plan that is reviewed at least annually. This review enables Highwire personnel to be familiar with

emergency planning in case of an event that could potentially cause an interruption to normal business activities.

Highwire also conducts ongoing comprehensive risk assessments to ensure proper risk mitigation strategies and controls have been implemented within the organization.

6.4 Incident Response

Highwire maintains a comprehensive Incident Response Plan. This plan, along with related processes and procedures, enables Highwire personnel to quickly respond to a suspected or potential security breach or other suspicious cybersecurity activity within the Highwire platform. Highwire's Incident Response Team, led by the Vice President of Engineering, performs an assessment of any such situation and develops appropriate action plans and mitigation strategies. If a suspected breach is confirmed, the Incident Response Team will follow designated protocols to immediately act and appropriately respond to mitigate the malicious activity, along with preserving forensic evidence. Notification procedures will also be followed.

6.5 Encryption

Highwire maintains the encryption of data at rest using AES-256. Additional data elements are also encrypted using SALT methods. These encryption processes maintain a high degree of confidentiality and integrity of customer data. Logical data separation is maintained in the Highwire platform so that no customer data can be accessed by unauthorized sources. Customer data access is controlled through unique identity and access management with attributes that disallow unauthorized users from accessing the customer data.

Highwire security measures are implemented based upon a "least privilege" method, meaning that only employees who have a business need have access to specific data and system functions.

6.6 Web Application Security Controls

Client and contractor user access to the Highwire application is only via secure communication protocols, TLS 1.2 or higher. These protocols establish an encryption channel to enable secure data transmission between an end-user and the Highwire platform, protecting client and contractor data during data transmission processes.

A client or contractor Highwire administrator can provision and de-provision their users and associated access as necessary. Highwire allows customers to enable multi-factor

authentication to access Highwire accounts utilizing single sign-on via SAML 2.0 identity providers. Highwire also forces users to adhere to a strict password policy.

6.7 Network

Highwire utilizes AWS network controls to restrict network ingress and egress. Security groups are employed to limit network activity to authorized endpoints. Highwire uses a multi-tier network architecture, including multiple, logically separated virtual environments, leveraging private DMZs and untrusted zones within the AWS cloud service infrastructure.

6.8 Monitoring and Auditing

Highwire systems and networks are monitored for security incidents, system health, network abnormalities, processing activity, infrastructure processing levels, and availability. Highwire uses an intrusion detection system to monitor network activity, which will alert Highwire's designated team members of suspicious behavior. Web application firewalls are also implemented for all public web services.

Highwire logs application, network, user, and operating system events, and these logs are automatically analyzed and reviewed for suspicious activity and threats. Any system activity anomalies are escalated with the appropriate action that may be required. Highwire utilizes security information and event management systems, providing continuous security analysis of the Highwire networks and security environment, where alerting, detecting, and reporting of indicators of possible or suspicious activity are recorded. Highwire's DevOps staff administers all of these capabilities and activities under the direction of the Vice President of Engineering.

6.9 Vulnerability Management

Highwire performs periodic web application vulnerability assessments, static code analysis, and external security assessments as part of its comprehensive security program to help ensure proper security controls are implemented and operating effectively. On an annual basis, Highwire hires an independent third-party penetration tester to perform both network and web vulnerability assessments. The scope of this external audit includes compliance against the Open Web Application Security Project (OWASP) Top 10 Web Vulnerabilities. Vulnerability assessment results are incorporated into the Highwire software development lifecycle ("SDLC") and risk assessment process to remediate identified vulnerabilities. Specific vulnerabilities are prioritized and entered into the Highwire internal ticket system for tracking through resolution.

6.10 Secure Software Development

Highwire follows secure development practices within its SDLC. These practices include real-time code analysis tools. Peer reviews are also conducted before code is deployed into the production environment. Separate processing environments have been implemented at Highwire: production, development, testing, and demo. Highwire software developers receive ongoing training in secure coding.

6.11 Privacy and Data Protection

Highwire maintains robust Information Security and Personal Data Protection Policies that are referenced in the Highwire Privacy Policy. These policies outline the procedures that are followed to ensure the safeguarding of customer information. They further outline the controls that are implemented, which include data retention, accessibility and authentication guidelines, acceptable use guidelines, and data privacy guidelines.

7. Security Breach and Personal Data Loss

Highwire will notify clients and contractors immediately via email of any personal data breach (and never later than 72 hours after becoming aware of it). This notification will include any necessary documentation to enable clients to notify the competent supervisory authority if required, including:

- The nature and description of the breach, including the number of users who are affected.
- Analysis and root cause of the failure.
- Immediate corrective action to address the breach and mitigate the adverse effects.
- Other corrective actions proposed or taken to prevent any future breaches of the same nature and type.

If a client or contractor suspects a security breach, they can report it immediately to support@highwire.com.

8. Cross-Border Transfers of Personal Data and Required Contractual Clauses

Clients and contractors acknowledge and agree that Highwire may transfer, access, and process Personal Data globally as necessary to provide the Highwire Services.

Where the Applicable Data Protection Legislation has prescribed specific mechanisms for the transfer of Personal Data to Highwire and contract clauses for processing of Personal Data by Highwire (collectively, "Transfer Mechanisms"), Highwire will support such specific Transfer Mechanisms as detailed below.

8.1 Data Privacy Framework

For transfers of Personal Data to the United States, Highwire has self-certified to the EU-US Data Privacy Framework, the UK Extension to the EU-US Data Privacy Framework, and the Swiss-US Data Privacy Framework administered by the US Department of Commerce. For further information, please refer to Highwire's Data Privacy Framework Notice.

8.2 EU Standard Contractual Clauses (EU SCCs)

When the processing involves transfers of Personal Data outside the EEA to Highwire, and there is no other legitimate basis for the international transfer (for example, if the applicable Data Privacy Framework has been invalidated), such transfers are subject to the EU SCCs, specifically:

a. In circumstances where Highwire acts as a data controller, Module One of the EU SCCs (for controller-to-controller transfers), supplemented by the terms below, shall apply to the transfers of Personal Data between a supplier and Highwire:

i. Optional language at clause 7 (docking clause) is used.

ii. The optional language at clause 11(a) (redress) is not used.

iii. For clause 17, the first option is used, and the law of Germany is the governing law.

iv. For clause 18(b), the selected forum shall be the courts of Germany.

b. In circumstances where the supplier is a data controller and Highwire is a data processor with respect to the processing, Module Two of the EU SCCs (for controller-to-processor transfers), supplemented by the terms below, shall apply:

i. Optional language at clause 7 (docking clause) is used.

ii. For clause 9(a), option 2 (general written authorization) is selected and the specified time period is ten (10) days.

iii. The optional language at clause 11(a) (redress) is not used.

iv. For clause 17, the first option is used, and the law of Germany is the governing law.

v. For clause 18(b), the selected forum shall be the courts of Germany.

c. Annex I, Annex II, and Annex III of the EU SCCs shall be deemed completed with the information set out in Section 4.

8.3. UK Addendum

When the processing involves transfers of Personal Data outside the UK to Highwire, and there is no other legitimate basis for the international transfer (for example, if the applicable Data Privacy Framework has been invalidated), such transfers are subject to the UK Addendum, supplemented by the terms below:

a. The parties to this UK Addendum shall be the parties to the DPA.

b. The EU SCCs that this UK Addendum amends shall be the applicable EU SCCs referenced in Section 2 of this DPA, and Tables 1-3 of the UK Addendum shall be completed with the relevant information accordingly.

c. For the purpose of Table 4 of the UK Addendum, "Importer" shall be selected.

d. The part 2 of the UK Addendum shall be: "Part 2: Mandatory Clauses of the Approved Addendum, being the template Addendum B.1.0 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 18 of those Mandatory Clauses."

8.4. Swiss Standard Contractual Clauses

When the processing involves transfers of Personal Data outside Switzerland to Highwire, and there is not another legitimate basis for the international transfer (for example, if the applicable Data Privacy Framework has not been recognized as/is no longer a valid transfer mechanism), such transfers are subject to the EU SCCs, except that:

a. The term "member state" must not be interpreted in such a way as to exclude Data Subjects in Switzerland from the possibility of suing for their rights in their place of habitual residence (Switzerland) in accordance with clause 18 (c) of these standard contractual clauses.

b. In circumstances where the transfers are exclusively subject to the Federal Act on Data Protection ("**FADP**"), references to the GDPR are to be understood as references to the FADP.

c. In circumstances where the transfers are subject to both the FADP and the GDPR, the references to the GDPR are to be understood as references to the FADP insofar as the transfers are subject to the FADP.

9. Sub Processors

Client and contractor agree that, to the extent Highwire acts as a data processor, Highwire may use Amazon Web Services as a sub-processor for the processing and cloud storage of Personal Data in connection with the provision of the Highwire Services. The complete list of Highwire subprocessors can be found here.

10. Data Subject Rights Requests

All parties agree to provide such assistance as is reasonably required to enable another party to comply with any Subject Rights Requests within the time limits imposed by the Applicable Data Protection Legislation.

Highwire shall notify a client or contractor of any request for the disclosure of a client's or contractor's Personal Data by a governmental or regulatory body or law enforcement authority, unless otherwise prohibited by law or a legally binding order of such body or agency.

11. Term and Termination

This DPA shall come into force on the effective date of the client license and services agreement or the Contractor Participation Agreement or the first provision of Personal Data to Highwire, whichever is earlier, and shall remain in full force and effect so long as the client or contractor agreement remains in effect.

Any provision of this DPA that expressly or by implication should come into force on or after the termination of a client or contractor agreement to protect Personal Data will remain in full force and effect.

12. Review and Development

The author of this policy is considered the owner and is responsible for updating it whenever changes are dictated by the work. In addition, the Vice President of Compliance will conduct an annual review of this policy to ensure that it remains appropriate considering any relevant changes to the law, organizational policies, and contractual obligations.

HIGHWIRE

For reference, all previous versions of an ISMS document are stored on the personal user drive of the Highwire Vice President of Compliance. The versioning history for this document is defined in the table below:

Version History	Date	Author	Approver	Classification
Version 2	9/19/24	K. Sardone	B. Householder Hengeler Mueller	Publicly available on Help Center
Version 1	5/14/24	K. Sardone	B.Householder Hengeler Mueller	Publicly available on Help Center
This policy will be reviewed annually by the Vice President of Compliance.				