

DATA PROCESSING ADDENDUM

API

This data processing addendum (the "**Addendum**"), forms a part of the Terms of Service (the "**ToS**") entered into by and between Xverum LLC., a company incorporated under the laws of Florida, USA ("**XVERUM** "), and You (the "**Customer**") (with XVERUM on the one hand and the Customer, on the other hand, may also be referred to herein as a "**Party**", and collectively they may also be referred to as the "**Parties**").

This Addendum shall be an inseparable part of the Agreement. For the purposes of this Addendum, the term "XVERUM" shall include XVERUM and/or its Affiliates.

By virtue of the Agreement, XVERUM may Process Agreement Personal Data on behalf of Customer.

1. Definitions

In this Addendum, the following words and phrases shall (unless the context otherwise requires) have the meanings set out beside them:

- 1.1. "**Affiliate**" shall mean a person or entity controlling, controlled by or under the common control with XVERUM or Customer (as applicable); the term "control", for the purpose of this definition, shall mean direct or indirect possession of the power to direct or cause the direction of the management or policies of XVERUM or Customer (as applicable), whether through the ability to exercise voting power, by contract or otherwise.
- 1.2. "**Agreement Data Subject**" shall mean natural persons to which Agreement Personal Data relate.
- 1.3. "**Agreement Personal Data**" shall mean any Personal Data Processed by XVERUM or any Subcontractor pursuant to or in connection with the Agreement.
- 1.4. "**Applicable Laws**" shall mean European Union or a Member State law and any other applicable law with respect to any Agreement Personal Data.
- 1.5. "**Applicable Privacy Laws**" shall mean all laws and regulations, including the laws and regulations of the European Union, the European Economic Area and/or their member states, Switzerland, the United Kingdom and the United States and its states, applicable to the Processing of Agreement Personal Data.
- 1.6. "**CCPA**" means the California Consumer Privacy Act, Cal. Civ. Code § 1798.100 et seq., and its implementing regulations.
- 1.7. "**Controller**" means the entity which determines the purposes and means of the Processing of Agreement Personal Data.
- 1.8. "**Customer**" means the entity that executed the Agreement together with its Affiliates, which have signed the Agreement or a part thereof.

- 1.9. "**EEA**" means the European Economic Area.
- 1.10. "**EU Privacy Laws**" means EU Directive 95/46/EC, as transposed into domestic legislation of each EU member state and as amended, replaced or superseded from time to time, including by the GDPR and laws, rules and guidelines implementing or supplementing the GDPR.
- 1.11. "**GDPR**" shall mean 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 and repealing Directive 95/46/EC (General Data Protection Regulation).
- 1.12. "**International Organisation**" means an organization and its subordinate bodies governed by public international law, or any other body which is set up by, or on the basis of, an agreement between two or more countries.
- 1.13. "**Personal Data**" means any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an alias, an identification number, location data, a postal address, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
- 1.14. "**Personal Data Breach**" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Agreement Personal Data transmitted, stored or otherwise Processed.
- 1.15. "**Processing**" means any operation or set of operations which is performed on Personal Data or on sets of 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.
- 1.16. "**Processor**" means the entity which Processes Personal Data on behalf of the Controller, including, as applicable, any "service provider" as this term is defined by the CCPA.
- 1.17. "**Restricted Processing**" shall mean (1) the transferring of Agreement Personal Data outside the EEA or to an International Organization, and (2) any Processing of Agreement Personal Data that was transferred to any country outside the EEA or to an International Organization; in each case, where such transferring or Processing of Agreement Personal Data would be prohibited by Applicable Privacy Laws in the absence of Standard Contractual Clauses.
- 1.18. "**Services**" shall mean the service provided by XVERUM to Customer pursuant to the Agreement.

- 1.19. "**Standard Contractual Clauses**" shall mean the standard contractual clauses pursuant to the European Commission's decision dated 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council notified under document C(2010) 593) including any amended, extended, re-enacted or consolidated version in force from time to time.

https://www.xverum.com/wp-content/uploads/2022/07/Xverum_Controller_to_Processor_Standard_Contractual_Clauses.pdf

- 1.20. "**Subcontractor**" shall mean any person appointed by or on behalf of XVERUM to Process Agreement Personal Data on behalf of Customer in connection with the Agreement, excluding any employee of XVERUM or of any such appointed person.

2. Authorization and Compliance

- 2.1. By virtue of the Agreement, Customer is considered as the "Controller" and XVERUM is considered as the "Processor" with regards to the Agreement Personal Data.
- 2.2. **Schedule 2.2** to this Addendum sets out certain details regarding XVERUM's Processing of Agreement Personal Data, as required by Article 28(3) of the GDPR.
- 2.3. Customer shall, in the use of the Services, Process Agreement Personal Data in accordance with the requirements of the Applicable Privacy Laws. For the avoidance of doubts, the Customer's instructions for the Processing of Agreement Personal Data shall comply with the Applicable Privacy Laws.
- 2.4. Customer bears the exclusive responsibility for assessing the lawfulness of the Processing of Agreement Personal Data, as well as the lawfulness of the transfer of Agreement Personal Data to XVERUM to Process Agreement Personal Data for the provision of the Services.
- 2.5. Customer specifically declares that its use of the Services will not violate Agreement Data Subjects' rights to opt-out of the sale or other disclosure of their Personal Data, to the extent applicable under the CCPA.
- 2.6. XVERUM shall only Process Agreement Personal Data on behalf of and in accordance with Customer's documented instructions. Customer's instructions for the Processing of Agreement Personal Data shall comply with Applicable Privacy Laws.
- 2.7. The Parties agree that XVERUM shall Process Agreement Personal Data (i) in accordance with this Addendum and the Agreement, which set out the

Customer's instructions to XVERUM in relation to the Processing of Agreement Personal Data, and/or (ii) on documented instructions from Customer unless prohibited to do so by Applicable Laws to which XVERUM is subject. To the extent that XVERUM believes that an instruction given by Customer does not comply with any Applicable Law, it shall refuse to comply with such instruction even if Customer insists on it in spite of the notification of XVERUM.

3. XVERUM's Personnel

- 3.1. XVERUM shall ensure that access to Agreement Personal Data is strictly limited to those individuals who need to know or access the relevant Agreement Personal Data and as strictly necessary for the purpose of the Agreement.
- 3.2. XVERUM shall take all steps reasonably necessary to ensure that the individuals who may have access to Agreement Personal Data on its behalf (i) are informed of the confidential nature of Agreement Personal Data; and (ii) are subject to confidentiality undertakings or appropriate statutory obligations of confidentiality.

4. Subcontractors

- 4.1. Customer acknowledges that (i) XVERUM's Affiliates may be retained as Subcontractors; and (ii) XVERUM and XVERUM's Affiliates may engage third-party Subcontractors in connection with the provision of the Services.
- 4.2. XVERUM shall ensure that the arrangement between XVERUM and any Subcontractor is regulated by a written agreement or other written instrument, imposing on the Subcontractor undertakings that guarantee at least the same level of protection for Agreement Personal Data as those set out in this Addendum to the extent applicable to the nature of the services provided by such Subcontractor.
- 4.3. **Schedule 4.3** lists Subcontractors that are currently engaged by XVERUM to Process Agreement Personal Data on behalf of Customer. At least thirty (30) days before XVERUM engages a new Subcontractor, XVERUM will notify such change to the Customer. If Customer has a legitimate reason under Applicable Privacy Laws to object to the new Subcontractor's Processing of Agreement Personal Data, Customer may terminate the Agreement (limited to the Services for which the new Subcontractor is intended to be used) on written notice to XVERUM. Such termination shall take effect at the time determined by the Customer, which shall be no earlier than seven (7) days from the date of Customer's notice to XVERUM informing XVERUM of its decision to terminate the Agreement. If Customer does not terminate the Agreement within this thirty (30) day period, Customer is deemed to have accepted the new Subcontractor.
- 4.4. Within the thirty (30) day period from the date of XVERUM's notice to Customer informing Customer of the new Subcontractor, Customer may request that the Parties discuss a resolution of the objection. Such discussions shall not extend the

period for termination and do not affect XVERUM's right to use the new Subcontractor after the thirty (30) day period.

5. Rights of Agreement Data Subjects

- 5.1. Without derogating from the generality of the above, XVERUM shall (i) notify Customer without undue delay of any request raised by an Agreement Data Subject in relation to Agreement Personal Data concerning him or her to XVERUM; and (ii) refrain from responding to any such request, except on a written instruction of Customer or as required by Applicable Law to which XVERUM is subject.
- 5.2. Taking into account the nature of the Processing of Agreement Personal Data by XVERUM, XVERUM shall assist Customer by reasonably appropriate technical and organizational measures, insofar as this is possible, for the fulfillment of Customer's obligations to respond to a request raised by an Agreement Data Subject in relation to Agreement Personal Data concerning him or her. To the extent permitted under Applicable Law, Customer shall be responsible for any costs arising from XVERUM's provision of such assistance.

6. Personal Data Breaches

- 6.1. XVERUM will notify Customer of any Personal Data Breach affecting Agreement Personal Data without undue delay after becoming aware of the Personal Data Breach.
- 6.2. Unless the Personal Data Breach is entirely not under the responsibility of XVERUM, XVERUM will take those steps as XVERUM deems necessary and reasonable in order to mitigate the effects and to minimize any damage resulting from the Personal Data Breach, to the extent mitigation is within XVERUM's reasonable control.

7. Data Security

- 7.1. XVERUM has implemented and will apply the technical and organizational measures set forth in **Schedule 7.1** to protect the security of Agreement Personal Data. Customer has reviewed such measures and agreed that as to the Services the measures are appropriate taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of the Processing of Agreement Personal Data.
- 7.2. XVERUM may change the measures in **Schedule 7.1** at any time without notice so long as it maintains a comparable or better level of security.

8. Deletion or Return of Agreement Personal Data

Upon a written request of Customer at any time, XVERUM shall, at Customer's option, (i) delete all Agreement Personal Data in its possession or control, along with all copies, extracts and other objects or items in which it may be contained or embodied; or (ii) return to Customer by secure file transfer in such format as available for the Services all Agreement Personal Data in its possession or control and, delete all such Agreement Personal Data, along with all copies, extracts and other objects or items in which it may be contained or embodied; *provided, however*, that to the extent that XVERUM is required by Applicable Law or by the order of a governmental or regulatory body to retain Agreement Personal Data, it shall be maintained for as long as such requirement apply.

9. Information Rights

Subject to confidentiality obligations XVERUM shall make available to Customer any information reasonably necessary to Customer to demonstrate compliance with this Addendum.

10. Audit Rights

XVERUM will allow for and contribute to audits to demonstrate compliance with this Addendum in accordance with the following provisions:

- 10.1. Customer shall provide at least six (6) weeks' prior written notice to XVERUM of a request to audit, provided that any such request shall occur no more than once in any twelve (12) calendar month period.
- 10.2. Upon receipt of the request under Article 10.1 above, XVERUM will inform Customer if XVERUM has conducted an audit of its data protection and data security procedures in the preceding twelve (12) calendar month period, in which case Customer agrees to exercise any right it may have to conduct an audit under this Addendum or under the Standard Contractual Clauses (if they apply) by instructing XVERUM to provide Customer with a summary of such most recent relevant audit report, which shall be considered XVERUM's confidential information.
- 10.3. To the extent that the Customer requested an audit under Article 12.1 and XVERUM has not performed an audit pursuant to Article 10.2 during the twelve (12) calendar month period prior to the request, the audit shall be conducted by a mutually agreed upon independent third party auditor who is engaged and paid by Customer, and is under a non-disclosure agreement requiring the auditor to maintain the confidentiality of all XVERUM's confidential information and all audit findings. The audits pursuant to this Article 10.3 and to the Standard Contractual Clauses (if they apply) shall be limited to XVERUM's data processing procedures and documentation, and they shall be conducted during normal business hours. Any such audit will result in the generation of an audit report, which shall be considered XVERUM's confidential information. At

Customer's written request, XVERUM will make available to Customer a summary of the relevant audit report.

10.4. The scope of any audit will be limited to XVERUM's policies, procedures, systems and controls relevant to the Processing of Agreement Personal Data.

10.5. If the Standard Contractual Clauses apply, nothing in this Article varies or modifies the Standard Contractual Clauses nor affects any supervisory authority's or Agreement Data Subject's rights under the Standard Contractual Clauses.

11. Limitation of liability

Each Party's and all of its Affiliates' liability, taken together in the aggregate, arising out of or related to this Addendum 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 the Addendum together.

12. European Specific Provisions

The following provisions shall only apply to the Processing of Personal Data on which the GDPR applies:

12.1. If pursuant to Applicable Privacy Laws, Customer is required to perform a data protection impact assessment or prior consultation with, at Customer's request, XVERUM shall provide such documents as are generally available for the Services. Any additional assistance shall be mutually agreed between the Parties.

12.2. Restricted Processing

12.2.1. The Parties hereby enter into the Standard Contractual Clauses that are incorporated into this Addendum by reference. In the event of any conflict or inconsistency between this Addendum and the Standard Contractual Clauses, the Standard Contractual Clauses shall prevail.

12.2.2. Other Controllers, whose use of the Services has been authorized by Customer under the Agreement, also enter into the Standard Contractual Clauses with XVERUM. In such a case, Customer will enter into the Standard Contractual Clauses on behalf of other Controllers.

12.2.3. The following provisions shall apply to any such Restricted Processing: (i) with regard to the Standard Contractual Clauses entered into by Customer and/or the other Controllers, on one hand, and XVERUM, on the other hand, Customer and/or the other Controllers as set out in Article 12.2.2 above are considered as "data exporter" and XVERUM is considered as "data importer"; (ii) Schedule 2.2 to this Addendum shall apply as Appendix 1 of the Standard Contractual Clauses entered into by Customer and/or the other Controllers, on one hand, and

XVERUM, on the other hand; and (iii) Schedule 7.1 to this Addendum shall apply as Appendix 2 of the Standard Contractual Clauses entered into by Customer and/or the other Controllers, on one hand, and XVERUM, on the other hand.

- 12.2.4. For the avoidance of doubt, Articles 12.2.1, 12.2.2 and 12.2.3 shall not apply in respect of Restricted Processing that is allowed by Applicable Privacy Laws without entering into the Standard Contractual Clauses or an agreement incorporating the Standard Contractual Clauses.

13. Miscellaneous

- 13.1. This Addendum shall continue to be in force until the termination of the Agreement.
- 13.2. With regard to the subject matter of this Addendum, in the event of inconsistencies between the provisions of this Addendum and any other agreements between the Parties, including the Agreement, the provisions of this Addendum shall prevail.
- 13.3. This Addendum and all non-contractual or other obligations arising out of or in connection with it are governed the laws and subject to the jurisdiction of the courts of the country in which the Customer or the relevant Controller is incorporated.
- 13.4. If any provision of this Addendum is held by a court of competent jurisdiction to be unenforceable under Applicable Law, then such provision shall be excluded from this Addendum and the remainder of this Addendum shall be interpreted as if such provision was so excluded and shall be enforceable in accordance with its terms; *provided, however*, that in such event this Addendum shall be interpreted so as to give effect, to the greatest extent consistent with and permitted by applicable law, to the meaning and intention of the excluded provision as determined by such court of competent jurisdiction.

Schedule 2.2 to the Addendum and, if applicable, Appendix 1 to the Standard Contractual Clauses

Data exporter

The data exporter is the entity identified as the Customer in the Addendum.

Data importer

The data importer is XVERUM LLC., a provider of a platform, developed for the purpose of extracting public web pages from the internet anonymously.

Nature and purpose of the data processing

XVERUM will Process Agreement Personal Data as necessary to perform the Services pursuant to the Agreement.

Categories of data subjects

Individuals who published personal data in publicly available webpages.

Categories of data

The types of personal data that may be collected, processed and/or used under the Agreement may include the following: Personal Data published by Agreement Data Subjects in publicly available webpages.

Special categories of data

The Services are not intended to include the collection or transfer of special categories of personal data, which includes personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data, data concerning health or data concerning a natural person's sex life or sexual orientation.

Processing operations and subject matter of processing

Extraction, transmission and parsing of Personal Data.

Duration of the data processing

Agreement Personal Data shall be Processed throughout the duration of the Agreement, unless otherwise agreed upon in writing.

The obligations and rights of the customer

As set out in the Agreement and the Addendum.

Data importer

[REDACTED]

Data exporter

Data Protection Officer



Email: privacy@xverum.us

Schedule 4.3

Current Subcontractors

Amazon (AWS)

Hetzner Online GmbH

Schedule 7.1 to the Addendum and, if applicable, Appendix 2 to the Standard
Contractual Clauses

:Minimum technical and organizational requirements

1. **Information security program.** A written security program is implemented, maintained and complied with. As part of the program, Customer will: (i) implement an audit program to test and, if necessary, remediate identified gaps of all security controls at least annually or whenever there is a material change in business practices that may reasonably implicate the security or integrity of records containing Agreement Personal Data; (ii) conduct, in line with ISO27001 or similar standards, an annual risk assessment that assesses the threats and vulnerabilities associated with systems; and (iii) produce (pursuant to the results of (i) and (ii)) a documented risk assessment and, where appropriate, risk remediation plan.
2. **Security official.** A designated management level or above security official is responsible for the development, implementation, and ongoing maintenance of the information security program. The appointed official has appropriate recognized information security credentials and qualifications.
3. **Access control.** Access rights are assigned according to the principle that employees and third-parties are only granted the level of access they need to perform their activities (need-to-know principle). Access rights are granted according to defined (role-based) permissions. The access rights granted are reviewed regularly. Rights that are no longer required are withdrawn immediately.
4. **Physical access control.** Secure areas are defined on the basis of information security and data protection requirements and protected against unauthorized access by appropriate physical safeguards, defined based on the protection needs of the information located or accessed within them.
5. **Incident response plan.** Policies and procedures are implemented, designed to detect, respond to, and otherwise address incidents, including specific points of contact in the event of an incident, and procedures to: (i) monitor and detect actual and attempted attacks on, or intrusions into, the processing systems, (ii) identify and respond to suspected or known incidents, (iii) immediately mitigate the harmful effects of any incidents without detriment to measures or actions necessary to determine the seriousness of the breach.
6. **System Testing and Maintenance.** Customer tests and maintained systems to protect data including, without limitation: (i) installing of critical security patches for operating systems and applications within thirty (30) days of publication, and within three (3) months for other types of patches and updates, (ii) installing the latest recommended versions of operating systems, software and firmware for all system components, and (iii) ensuring that up-to-date system security agent software includes malware protection set to receive automatically updated (at least daily) patches and virus definitions.

7. **Audit logging.** Hardware, software, or procedural mechanisms are implemented and maintained to record and examine activity in processing systems that contain or use electronic information, including appropriate logs and reports concerning the security requirements set for the in this Schedule.
8. **Security awareness and privacy training.** An ongoing security and privacy awareness and training program is maintained for all employees (including management, employees, contractors and other agents), which includes training on how to implement and comply with the information security program and setting forth disciplinary measures for violation of the security program. Security and privacy awareness training are conducted at least annually.