Hyros Data Protection Addendum

Last updated Januray 15, 2024

This Data Protection Addendum ("**Addendum**" or "DPA"), forms part of the Terms of Service ("**Terms of Service**") available at https://www.hyros.com/terms-and-conditions.html between: (i) Hyros, Inc. **("Hyros")**; and (ii) you ("**Customer**" or "**you**").

The terms used in this Addendum shall have the meanings set forth in this Addendum. Capitalized terms not otherwise defined herein shall have the meaning given to them in the Terms of Service. Except as modified below, the terms of the Terms of Service shall remain in full force and effect.

HOW TO EXECUTE THIS DPA:

To complete this DPA, you must:

a. Complete the information in the signature box and sign on page 10.
b. Send the signed DPA to Hyros by email to privacy@hyros.com.

In consideration of the mutual obligations set out herein, the parties hereby agree that the terms set out below shall be added as an Addendum to the Terms of Service. Except where the context requires otherwise, references in this Addendum to the Terms of Service are to the Terms of Service as amended by, and including, this Addendum.

1. Definitions

1.1 In this Addendum, the following terms shall have the meanings set out below and cognate terms shall be construed accordingly:

1.1.1 "**Affiliates**" means (i) an entity of which a party directly or indirectly owns fifty percent (50%) or more of the stock or other equity interest, (ii) an entity that owns at least fifty percent (50%) or more of the stock or other equity interest of a party, or (iii) an entity which is under common control with a party by having at least fifty percent (50%) or more of the stock or other equity interest of such entity and a party owned by the same person, but such entity shall only be deemed to be an Affiliate so long as such ownership exists.

1.1.2 "**Applicable Laws**" means (a) European Union or Member State laws with respect to any Customer Personal Data in respect of which Customer is subject to EU Data Protection Laws; (b) the Swiss Federal Act on data Protection,(c) the UK Data Protection Act of 2018, (d) the California Consumer Privacy Act, as amended by the California Privacy Rights Act of 2020 ("CCPA"), (e) other Specific US State Data Protection Law" and (f) any other applicable law with respect to any Customer Personal Data in respect of which Customer is subject to any other Data Protection Laws;

1.1.3 **"Authorized SubProcessor"** means any person (including any third party, but excluding an employee of Hyros, and employee of any wholly-owned subsidiaries, or any of its sub-contractors) appointed by or on behalf of Hyros to Process Personal Data on behalf of the Customer in connection with the Terms of Service as set out in Annex I, or is subsequently authorized under section 5.3 of this DPA.

1.1.4 **"CCPA"** means the California Consumer Privacy Act, Cal. Civ. Code §§ 1798.100 et seq., including any amendments and any implementing regulations thereto that become effective on or after the Effective Date of this Addendum.

1.1.5 "**Contracted Processor**" means Hyros, a wholly-owned subsidiary of Hyros, or a Subprocessor;

1.1.6 "**Customer Account Data**" means personal data that relates to the Customer's relationship with Hyros, including the names or contact information of individuals authorized by Customer to access Customer's account and billing information of individuals associated with its account. Customer Account Data also includes any data Hyros may need to collect for the purpose of managing its relationship with Customer, identity verification, or as otherwise required by applicable laws and regulations.

1.1.7 **"Customer End-User"** means a Data Subject who interacts, submits personal information to, or otherwise uses the Customer's websites and services.

1.1.8 "**Customer Usage Data**" means Service usage data collected and processed by Hyros in connection with the provision of the Services, including without limitation used to identify the source and destination of a communication, activity logs and data used to optimize and maintain performance of the Services, and to investigate and prevent system abuse.

1.1.9 "**Customer Personal Data**" means any Personal Data Processed by a Contracted Processor on behalf of the Customer pursuant to or in connection with the Terms of Service;

1.1.10 "**Data Protection Laws**" means the GDPR, the CCPA and the **S**pecific US State Data Protection Law, the UK GDPR, the FADP, and, to the extent applicable, the data protection or privacy laws of any other country;

1.1.11 "**EEA**" means the European Economic Area;

1.1.12 "**EU Data Protection Laws**" means EU General Data Protection Regulation 2016/679 (the "GDPR") and laws implementing or supplementing the GDPR;

1.1.13 **"EU-US Data Privacy Framework"** means the framework that permits personal data to be transferred from EU countries, and from Iceland, Liechtenstein and Norway to the U.S. when organizations participate in the EU-US Data Privacy Framework;

1.1.14 **"FADP"** means the Swiss Federal Act on Data protection of 19 June 1992, and as revised as of 25 September 2020;

1.1.15 "**Restricted Transfer**" means:

1.1.15.1 a transfer of Customer Personal Data from Customer to a Contracted Processor; or

1.1.15.2 an onward transfer of Customer Personal Data from a Contracted Processor to a Contracted Processor, or between two establishments of a Contracted Processor,

in each case, where such transfer would be prohibited by Data Protection Laws (or by the terms of data transfer agreements put in place to address the data transfer restrictions of Data Protection Laws) in the absence of the Standard Contractual Clauses to be established under section 5.4.3 or 11 below;

1.1.16 "**Services**" means the services and other activities to be supplied to or carried out by or on behalf of Hyros for the Customer pursuant to the Terms of Service;

1.1.17 "**Standard Contractual Clauses**" means the contractual clauses set out in Appendix 1, amended as indicated (in square brackets and italics) in that Appendix and under section 15.6;

1.1.18 '**Specific US State Data Protection Law"** means the CCPA (as defined), the Colorado Privacy Act of 2021 ("CPA"); the Virginia Consumer Data Protection Act of 2021 ("VCDA") ; the Colorado Privacy Act ("CPA"), the Utah Consumer Privacy Act of 2022, as amended ("UCPA") and any other US state laws that may be enacted that adheres to the same of substantially the same requirements of the above laws in this definition;

1.1.19 **"Swiss-US Data Privacy Framework"** means the framework that permits personal data to be transferred from Switzerland to the U.S. when organizations participate in the Swiss-US Data Privacy Framework;

1.1.20 **"UK"** means The United Kingdom of Great Britain and Northern Ireland;

1.1.21 **"UK Extension to the EU-US Data Privacy Framework"** means the framework that permits personal data to be transferred from the UK to the U.S. when organizations participate in the UK Extension to the EU-US Data Privacy Framework;

1.1.22 **"UK GDPR"** means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, The United Kingdom General Data Protection Regulation, as it forms part of the law of England and Wales, Scotland, and Northern Ireland by virtue of section 3 of the EU (Withdrawal) Act of 2018.

1.2 The terms, "**Commission**", "**Controller**", "**Data Subject**", **"Established"**, "**Member State**", "**Personal Data**", "**Personal Data Breach**", "**Processing**", **"Processor"** and "**Supervisory Authority**" shall have the same meaning as in the GDPR and the UK GDPR, and their cognate terms shall be construed accordingly. To the extent that the CCPA is applicable, the definition of "Controller" includes "Business", and the definition of "Processor" includes "Service Provider", as defined under the CCPA.

1.3 The word "**include**" shall be construed to mean include without limitation, and cognate terms shall be construed accordingly.

2. Processing of Customer Personal Data

2.1 Hyros shall:

2.1.1 comply with all applicable Data Protection Laws in the Processing of Customer Personal Data; and

2.1.2 not Process Customer Personal Data other than on the relevant Customer's documented instructions unless Processing is required by Applicable Laws to which the relevant Contracted Processor is subject, in which case Hyros shall to the extent permitted by Applicable Laws inform the Customer of that legal requirement before the relevant Processing of that Personal Data. The documented instructions of the Customer shall be deemed to include any use of Customer Personal Data described in the Terms of Service.

2.2 Customer shall:

2.2.1 instruct Hyros (and authorizes Hyros to instruct each Subprocessor) to:

2.2.1.1 Process Customer Personal Data; and

2.2.1.2 in particular, transfer Customer Personal Data to any country or territory, subject to clauses 5 and 11, as reasonably necessary for the provision of the Services and consistent with the Terms of Service; and

2.2.2 warrants and represents that it is and will at all relevant times remain duly and effectively authorized to give the instruction set out in section 2.2.1.

2.3 Annex I to this Addendum sets out certain information regarding the Contracted Processors' Processing of the Customer Personal Data as required by Article 28(3) of the GDPR (and, possibly, equivalent requirements of other Data Protection Laws). Customer and Hyros may, upon mutual written agreement, make reasonable amendments to Annex I from time to time as they mutually reasonably consider necessary to meet those requirements. Nothing in Annex I (including as amended pursuant to this section 2.3) confers any right or imposes any obligation on any party to this Addendum.

2.4 Specific US State Data Protection Law. The parties acknowledge and agree that the processing of Customer Personal Data that is subject to CCPA, CPA, VCDPA, and UCPA shall be carried out in accordance with the terms set forth in Appendix III.

3. Hyros Personnel

Hyros shall take reasonable steps to ensure the reliability of any employee, agent or contractor of any Contracted Processor who may have access to the Customer Personal Data, ensuring in each case that access is strictly limited to those individuals who need to know and access the relevant Customer Personal Data, as strictly necessary for the purposes of the Terms of Service, and to comply with Applicable Laws in the context of that individual's duties to the Contracted Processor, ensuring that all such individuals are subject to confidentiality undertakings or professional or statutory obligations of confidentiality.

4. Security

4.1 Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, Hyros shall in relation to the Customer Personal Data implement appropriate technical and organizational measures to ensure a level of security appropriate to that risk, including, as appropriate, the measures referred to in Article 32(1) of the GDPR.

4.2 In assessing the appropriate level of security, STS shall take into account in particular the risks that are presented to the Processing from a Personal Data Breach.

5. Subprocessing

5.1 The Customer authorizes Hyros to appoint (and permit each Subprocessor appointed in accordance with this section 5 to appoint) Subprocessors in accordance with this section 5 and any restrictions in the Terms of Service.

5.2 Hyros may continue to use those Subprocessors already engaged by Hyros as at the date of this Addendum, as set out in Annex II, subject to Hyros in each case as soon as practicable meeting the obligations set out in section 5.4.

5.3 Subprocessor notification and authorization

5.3.1 Customer hereby provides general authorization for Hyros to engage Subprocessors identified on the List (defined below) to access and process Customer Personal Data in connection with the Services and (2) from time to time engage additional third parties for the purposes of providing the Services, including without limitation the processing of Customer Personal Data.

5.3.2 A list of the Hyros' current Authorized Sub-Processors, as provided at the following link: https://hyros.com/sub-processors.html (the "List"), will be made available to Customer, via email or through other means. Such List may be updated by Hyros from time to time. If, within (20) days after receipt of such List, Customer notifies Hyros in writing of any objections on reasonable grounds related to the data privacy of any Subprocessor, Hyros shall take commercially reasonable steps to address the objections raised by the Customer and shall provide to Customer a reasonable written explanation of the steps taken. If Hyros cannot provide a commercially reasonable alternative within a commercially reasonable time, Customer may discontinue the use of the affected Service by providing written notice to Hyros. Customer acknowledges that certain sub-processors are essential to providing the Services and that objecting to the use of certain sub-processors may prevent Hyros from offering the Services to Customer. Any such discontinuation shall not relieve the Customer of any fees owed to Hyros up to the point of discontinuance.

5.3.3 If Customer does not object to the engagement of a third party in accordance with this section 5.3 within (10) days notice by Hyros, that third party shall be deemed an Authorized Sub-Processor for the purposes of this DPA.

5.4 With respect to each Subprocessor, Hyros shall:

5.4.1 before the Subprocessor first Processes Customer Personal Data (or, where relevant, in accordance with section 5.2), carry out adequate due diligence to ensure that the Subprocessor is capable of providing the level of protection for Customer Personal Data required by the Terms of Service;

5.4.2 ensure that the arrangement between Hyros, and the relevant intermediate Subprocessor is governed by a written contract including terms which offer at least the same level of protection for Customer Personal Data as those set out in this Addendum and meet the requirements of Article 28(3) of the GDPR;

5.4.3 if that arrangement involves a Restricted Transfer, unless such Subprocessor is certified under the EU-US Data Privacy Framework, the Swiss-US Data Privacy Framework, or the UK Extension to the EU-US Data Privacy Framework, where applicable, ensure that the Standard Contractual Clauses are at all relevant times incorporated into the agreement between Hyros and the relevant intermediate Subprocessor before the Subprocessor first Processes Customer Personal; and

5.4.4 provide to Customer for review such copies of the Contracted Processors' agreements with Subprocessors (which may be redacted to remove confidential commercial information not relevant to the requirements of this Addendum) as Customer may request from time to time, unless Hyros is prevented from doing so by applicable contractual obligations.

5.5 Hyros shall ensure that each Subprocessor performs the obligations under sections 2.1, 3, 4, 6.1, 7.2, 8 and 10.1, as they apply to Processing of Customer Personal Data carried out by that Subprocessor, as if it were party to this Addendum in place of Hyros.

6. Data Subject Rights

6.1 Taking into account the nature of the Processing, Hyros shall assist the Customer by implementing appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of the Customer's obligations, as reasonably understood by Customer, to respond to requests to exercise Data Subject rights under the Data Protection Laws.

6.2 Hyros shall:

6.2.1 promptly notify Customer if any Contracted Processor receives a request from a Data Subject under any Data Protection Law in respect of Customer Personal Data; and

6.2.2 ensure that, except for providing an acknowledgement of the request, the Contracted Processor does not respond to that request except on the documented instructions of Customer or as required by Applicable Laws to which the Contracted Processor is subject, in which case Hyros shall to the extent permitted by Applicable Laws inform Customer of that legal requirement before the Contracted Processor responds to the request.

7. Personal Data Breach

7.1 Hyros shall notify Customer without undue delay upon Hyros or any Subprocessor becoming aware of a Personal Data Breach affecting Customer Personal Data, providing Customer with sufficient information to allow Customer to meet any obligations to report or inform Data Subjects of the Personal Data Breach under the Data Protection Laws.

7.2 Hyros shall cooperate with Customer and each Customer Affiliate and take such reasonable commercial steps as are directed by Customer to assist in the investigation, mitigation and remediation of each such Personal Data Breach.

8. Data Protection Impact Assessment and Prior Consultation

Hyros shall, at Customer's expense, provide reasonable assistance to the Customer with any data protection impact assessments, and prior consultations with Supervising Authorities or other competent data privacy authorities, which Customer reasonably considers to be required by Article 35 or 36 of the GDPR or equivalent provisions of any other Data Protection Law, in each case solely in relation to Processing of Customer Personal Data by, and taking into account the nature of the Processing and information available to, the Contracted Processors.

9. Deletion of Customer Personal Data

9.1 Subject to section 9.2, Hyros shall promptly and in any event within thirty (30) days of the date of cessation of any Services involving the Processing of Customer Personal Data (the "Cessation Date"), delete and procure the deletion of all copies of those Customer Personal Data, unless Customer requests, by written notice given within five (5) days of the Cessation Date, that Hyros return all of the Customer Personal Data to Customer.

9.2 Each Contracted Processor may retain Customer Personal Data to the extent required by Applicable Laws and only to the extent and for such period as required by Applicable Laws and always provided that Hyros shall ensure the confidentiality of all such Customer Personal Data and shall ensure that such Customer Personal Data is only Processed as necessary for the purpose(s) specified in the Applicable Laws requiring its storage and for no other purpose.

10. Security assessment rights

10.1 Upon written request by Customer, Customer shall have the right directly or through its representative(s) (provided however, that such representative(s) shall enter into written obligations of confidentiality and non-disclosure directly with Hyros), to access all reasonable and industry recognized documentation evidencing Hyros' policies and procedures governing the security of Customer Personal Data. Hyros reserves the right to refuse to provide Customer (or its representatives) with any information which would pose a security risk to Hyros or its customers, or that Hyros is prohibited to provide or disclose under applicable law or contractual obligation.

11. Restricted Transfers

11.1 Subject to section 11.3, the Customer (as "data exporter") and each Contracted Processor, as appropriate, (as "data importer") hereby enter into the Standard Contractual Clauses in respect of any Restricted Transfer from the Customer to that Contracted Processor, unless such Contracted Processor is certified under the EU-US Data Privacy Framework, the Swiss-US Data Privacy Framework, or the UK Extension to the EU-US Data Privacy Framework, where applicable, or unless another appropriate safeguard applies pursuant to Article 46 of the GDPR or other provisions of applicable Data Protection Laws, or a derogation applies pursuant to Article 49 of the GDPR.

11.2 The Standard Contractual Clauses shall come into effect under section 11.1 on the later of:

11.2.1 the data exporter becoming a party to them;

11.2.2 the data importer becoming a party to them; and

11.2.3 commencement of the relevant Restricted Transfer.

11.3 Section 11.1 shall not apply to a Restricted Transfer that takes place solely within the EEA.

12. Audit Rights:

Upon Customer's written request at reasonable intervals, and subject to reasonable confidentiality controls, Hyros shall, either (i) make available for Customer's review copies of certifications or reports demonstrating Hyros' compliance with prevailing data security standards applicable to the processing of Customer Personal Data, or (ii) if the provision of reports or certifications pursuant to (i) is not reasonably sufficient under Data Protection Laws, allow Customer's independent third party representative to conduct an audit or inspection of Hyros' data security infrastructure and procedures that is sufficient to demonstrate Hyros' compliance with its obligations under Data Protections Laws, provided that (a) Customer provides reasonable prior written notice of any such request for an audit and such inspection shall not be unreasonably disruptive to Hyros' business; (b) such audit shall only be performed during business hours and occur no more than once per calendar year; and (c) such audit shall be restricted to data relevant to Customer. Customer shall be responsible for the costs of any such audits or inspections. If Hyros and Customer have entered into Standard Contractual Clauses, the parties agree that the audits described in Clause 8.9 of the EU SCCs shall be carried out in accordance with this Section 12.

13. CCPA No Sale or Sharing of Personal Information

As to any Customer Personal Data to which the CCPA applies, ("CCPA Personal Data") Contracted processor, who is acting solely as a Service Provider, as defined in the CCPA with respect to CCPA Personal Data, acknowledges and confirms that it does not receive or process any Customer Personal Data as consideration for any services that the Contracted processor provides to the Customer. The Contracted Processor shall not have, derive, or exercise any rights or benefits regarding Customer Personal Data processed on Customer's behalf, and may use and disclose Customer Personal Data only for the purposes for which the Customer Personal data was provided, as described in the Terms of Services and this Addendum. The Contracted Processor certifies that it understands the rules, requirements and definitions of the CCPA, and agrees to refrain from "selling" or "sharing" (as such terms are defined by the CCPA) any Customer Personal Data without prior written authorization by the Customer, or cause any action that would qualify as "selling" or "sharing" Customer Personal Data under the CCPA.

14. Hyros' Role As a Controller.

The parties acknowledge and agree that with respect to Customer Account Data and Customer Usage Data, Hyros is an independent controller, not a joint controller, with Customer. Hyros will process Customer Account Data as a controller (i) to manage the relationship with Customer, (ii) to carry out Hyros' core business operations, such as accounting, audits, tax preparation and filing and compliance purposes, (iii) to monitor, investigator, present and detect fraud, security incidents and other misuse of the Services, and to prevent harm to Customer, (iv) for identity verification purposes; (v) to comply with legal or regulatory obligations applicable to the processing and retention of Customer Personal Data to which Hyros is subject; and (vi) as otherwise permitted under Data Protection Laws in accordance with this DPA and the Terms of Service. Any processing by Hyros as a controller shall be in accordance with Hyros' privacy policy set forth at https://hyros.com/privacy.html.

15. General Terms

Governing law and jurisdiction

15.1 Without prejudice to clauses 17 (Governing Law) and 18 (Choice of forum and jurisdiction) of the Standard Contractual Clauses:

15.1.1 the parties to this Addendum hereby submit to the choice of jurisdiction stipulated in the Terms of Service with respect to any disputes or claims howsoever arising under this Addendum, including disputes regarding its existence, validity or termination or the consequences of its nullity; and

15.1.2 this Addendum and all non-contractual or other obligations arising out of or in connection with it are governed by the laws of the country or territory stipulated for this purpose in the Terms of Service.

15.2 Where clause 17 (Governing Law) of the Standard Contractual Clauses is applicable, parties agree to the following:

15.2.1 where the Customer is Established in the EEA. the law of the Member State in which the Customer is Established, provided such Member State law allows for third-party beneficiary rights, shall apply;

15.2.2 where the Customer is Established in the UK, the law of England and Wales shall apply;

15.2.3 where the Customer is Established other than in the UK or the EEA, the law of the Member State in which the Customer has appointed its representative under Article 27 of the GDPR shall apply;

15.2.4 otherwise, the law of Belgium shall apply.

15.3 Where clause 18 (Choice of forum and jurisdiction) of the Standard Contractual Clauses is applicable, parties submit themselves to the jurisdiction of the courts of that country whose law applies as specified in section 15.2 of the Addendum.

Order of precedence

15.4 Nothing in this Addendum reduces Hyros obligations under the Terms of Service in relation to the protection of Personal Data or permits Hyros to Process (or permit the Processing of) Personal Data in a manner which is prohibited by the Terms of Service. In the event of any conflict or inconsistency between this Addendum and the Standard Contractual Clauses, the Standard Contractual Clauses shall prevail.

15.5 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 Terms of Service and including (except where explicitly agreed otherwise in writing, signed on behalf of the parties) agreements entered into or purported to be entered into after the date of this Addendum, the provisions of this Addendum shall prevail.

Changes in Data Protection Laws, etc.

15.6 Customer may:

15.6.1 by at least thirty (30) days written notice to Hyros from time to time make any variations to the Standard Contractual Clauses (including any Standard Contractual Clauses entered into under section 11.1), as they apply to Restricted Transfers which are subject to a particular Data Protection Law, which are required, as a result of any change in, or decision of a competent authority under, that Data Protection Law, to allow those Restricted Transfers to be made (or continue to be made) without breach of that Data Protection Law; and

15.6.2 propose any other variations to this Addendum which Customer reasonably considers to be necessary to address the requirements of any Data Protection Law.

15.7 If Customer gives notice under section 15.6.2 , Customer shall not unreasonably withhold or delay agreement to any consequential variations to this Addendum proposed by Hyros to protect the Contracted Processors against additional risks associated with the variations made under section 15.6.1.

15.8 If Customer gives notice under section 15.6.2, the parties shall promptly discuss the proposed variations and negotiate in good faith with a view to agreeing and implementing those or alternative variations designed to address the requirements identified in Customer's notice as soon as is reasonably practicable.

Severance

15.9 Should any provision of this Addendum be invalid or unenforceable, then the remainder of this Addendum shall remain valid and in force. The invalid or unenforceable provision shall be either (a) amended as necessary to ensure its validity and enforceability, while preserving the parties' intentions as closely as possible or, if this is not possible, (b) construed in a manner as if the invalid or unenforceable part had never been contained therein.

IN WITNESS WHEREOF, this Addendum is entered into and becomes a binding part of the Terms of Service with effect from the date first set out above.

Customer: _____

Signature _____

Name: _____

Title: _____

Date: _____

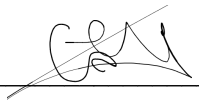
Customer address:

_____

_____

_____

Hyros, Inc.

Signature 

Name: Calin Petru Alexandru

Title: Chief Customer Officer

Date: 01 / 16 / 2024

APPENDIX I - STANDARD CONTRACTUAL CLAUSES

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.

(e) 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 8.1(b), 8.9(a), (c), (d) and (e);

(iii) Clause 9(a), (c), (d) and (e);

(iv) Clause 12(a), (d) and (f);

(v) Clause 13;

(vi) Clause 15.1(c), (d) and (e);

(vii) Clause 16(e);

(viii) 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

(Intentionally left blank)

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 benefitting 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 sub-processors

(a) The data importer has the data exporter's general authorisation for the engagement of sub-processor(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 sub-processors at least 20 days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(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 sub-processor 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 sub-processor 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 sub-processor 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 sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor 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 sub-processor contract and to instruct the sub-processor 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 sub-processor 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 sub-processor), 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 sub-processor to avoid its own liability.

Clause 13

Supervision

(a) 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.

(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.

(a) 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.

(b) 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.).

(c) 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.

(d) 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 the EU Member State in which the data exporter is established. Where such law does not allow for third-party beneficiary rights, they shall be governed by the law of another EU Member State that does allow for third-party beneficiary rights. The Parties agree that this shall be the law of ……..……..…….. (*specify Member State*).

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 Belgium.

(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.

ANNEX I

A. LIST OF PARTIES

The full name, address and contact details for the data exporter and data importer (as defined below) are set out in the Agreement(s) between the parties.

Data exporter(s): The data exporter and Controller is the Customer and its relevant Affiliates which are established in the EEA, the UK, or Switzerland.

Data importer(s): The data importer and processor is Hyros and its Affiliates located in third countries.

Activities relevant to the data transferred under these Clauses:

Provision of marketing services to the Data Exporter, specifically, correlating the ad traffic data with Customer End-Users inside data exporters business, and ensuring proper attribution is being allocated to their sales.

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

Customer End-Users **of the Data Exporter**

Categories of personal data transferred

First name
Last name
Phone number
Email address
IP Address
Session ID
Site event and activity
Current and referrer URLs, including all URL parameters
Coupon codes

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

N/A

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

Continuous basis for the duration of the contract

Nature of the processing

The provision of the Data Importer's services for which the Data Importer is a processor (e.g. tracking and back feeding)

Purpose(s) of the data transfer and further processing

Provision of the services to the Data Importer by the Data Exporter

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

Tracked data will be held indefinitely until the data exporter closes account and requests a full cancellation.

Untracked data has an approximate retention period of 3 months.

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

Same as above to the extent such categories of personal information are provided to subprocessors for purposes of providing the Services.

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with Clause 13

The competent supervisory authority shall be the Belgian DPA, the:

Autorité de la protection des données - Gegevensbeschermingsautoriteit (APD-GBA)
Rue de la Presse 35 – Drukpersstraat 35
1000 Bruxelles - Brussel
Tel. +32 2 274 48 00
Fax +32 2 274 48 35
Email: **contact@apd-gba.be**
Website: **https://www.autoriteprotectiondonnees.be** **https://www.gegevensbeschermingsautoriteit.be**

ANNEX II - TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

Description of the technical and organisational security measures implemented by the data importer:

1. **Personnel**. Hyros personnel will not process Customer Personal Data without authorisation. Personnel are obligated to maintain the confidentiality of any Customer Personal Data in accordance with the Terms of Service.

2. **Technical and Organizational Measures:** Hyros has implemented, and will continue to maintain, appropriate physical, technical and administrative controls and procedures intended to protect Customer Personal Data against accidental loss, destruction, alteration or unauthorised disclosure or access.

ANNEX III – LIST OF AUTHORIZED SUB-PROCESSORS

The following Sub-processors, and any sub-processors authorized pursuant to section 5.3 of this DPA, are authorized by the data exporter to process customer data, which may contain personally identifiable information, in order to provide and operate the services to which data exporter has subscribed to under the Terms of Service:

https://hyros.com/sub-processors.html

APPENDIX II - UK and Swiss Cross Border Transfers

ANNEX I - UK Cross Border Transfers

The International Data Transfer Addendum to the EU Commission Standard Contractual Clauses, VERSION B1.0, in force 21 March 2022 (the "IDTA"), issued by the UK Information Commissioner's Office (the "ICO") is included by reference to this Addendum, and is available at this hyperlink: https://ico.org.uk/media/for-organisations/documents/4019539/international-data-transfer-addendum.pdf . The Information Commissioner considers that it provides Appropriate Safeguards for Restricted Transfers when it is entered into as a legally binding contract.

The IDTA is further amended as follows:

Part 1: Tables

Table 1: The Parties: As described in APPENDIX I, ANNEX I of this Addendum.

Table 2: Selected SCCs, Modules and Selected Clauses: As described in 'ANNEX I - Standard Contractual Clauses' of this Addendum.

Table 3: Appendix Information: As set out in APPENDIX I, ANNEX I (other than the Parties), ANNEX II and ANNEX III of this Addendum.

Table 4: Ending this Addendum when the Approved Addendum Changes: Which Parties may end this Addendum as set out in Section 19: Exporter.

ANNEX II - Swiss Cross Border Transfers

The parties agree that the Standard Contractual Clauses as described in 'ANNEX I - Standard Contractual Clauses' of this Addendum shall be adjusted as set out below where the FADP applies to Swiss Transfers.

1) The Standard Contractual Clauses shall mean the Standard Contractual Clauses as amended by this APPENDIX II, ANNEX II;

2) The Swiss federal Data Protection and Information Commissioner shall be the sole Supervisory Authority for Swiss Transfers, subject to the FADP;

3) References to the “GDPR” in the Standard Contractual Clauses shall be interpreted to include the FADP, further:

    a) where Swiss transfers are exclusively subject to the FADP, all references to the GDPR in the Standard Contractual Clauses shall be understood to mean the FADP;

    b) where Swiss transfers are subject to both the FADP and the GDPR, all references to the GDPR in the Standard Contractual Clauses shall be understood to mean the FADP where the Swiss transfer is subject to the FADP;

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

5) Swiss transfers subject to both the FADP and GDPR shall use the EU Supervisory Authority named in APPENDIX 1, ANNEX 1.C of this Addendum;

6) References to the “EU” shall not be interpreted as excluding data subjects in Switzerland from the possibility of exercising their rights in their place of habitual residence (Switzerland) under clause 18(c) of the Standard Contractual Clauses;

APPENDIX III

United States Privacy Law Exhibit

This United States Privacy Law Exhibit supplements the DPA and includes additional information required by the Specific US State Data Protection Law, in each case, as updated, amended or replaced from time to time. Any terms not defined in this Appendix III shall have the meanings set forth in the DPA and/or the Terms of Service.

A. CALIFORNIA

1. Definitions

1.1. For purposes of this Section A, the terms "Business," "Business Purpose," "Commercial Purpose," "Consumer," "Personal Information," "Processing," "Sell," "Service Provider," "Share," and "Verifiable Consumer Request" shall have the meanings set forth in the CCPA.

1.2. All references to "Personal Data," "Controller," "Processor," and "Data Subject" in the DPA shall be deemed to be references to "Personal Information," "Business," "Service Provider," and "Consumer," respectively, as defined in the CCPA.

2. Obligations

2.1. The parties acknowledge and agree that Hyros is a Service Provider for the purposes of the CCPA (to the extent it applies) and Hyros is receiving Personal Information from Customer in order to provide the Services pursuant to the Terms of Service, which constitutes a Business Purpose.

2.2. Customer shall disclose Personal Information to Hyros only for the limited and specified purposes described in section 2 of this DPA.

2.3. Hyros shall not Sell or Share Personal Information provided by Customer under the Terms of Service.

2.4. Hyros shall not retain, use, or disclose Personal Information provided by Customer pursuant to the Terms of Service for any purpose, including a Commercial Purpose, other than as necessary for the specific purpose of performing the Services for Customer pursuant to the Terms of Service, or as otherwise set forth in the Terms of Service or as permitted by the CCPA.

2.5. Hyros shall notify Customer if it makes a determination that it can no longer meet its obligations under the CCPA.

2.6. Hyros will not combine Personal Information received from, or on behalf of, Hyros with Personal Information that it receives from, or on behalf of, another party, or that it collects from its own interaction with the Consumer.

2.7. Hyros shall comply with all obligations applicable to Service Providers under the CCPA, including by providing Personal Information provided by the Customer under the Terms of Service the level of privacy protection required by CCPA.

2.8. Hyros shall only engage a new sub-processor to assist Hyros in providing the Services to Customer under the Terms of Service in accordance with section 5 of the DPA, including, without limitation, Hyros shall: (i) notify Customer of such engagement via the notification mechanism described in section 5 of the DPA at least twenty (20) days before enabling a new Sub-Processor; and (ii) enter into a written contract with the sub-processor requiring sub-processor to observe all of the applicable requirements set forth in the CCPA.

3. Consumer Rights

3.1. Hyros shall assist Customer in responding to Verifiable Consumer Requests to exercise the Consumer's rights under the CCPA as set forth in section 6 of the DPA.

4. Audit Rights

4.1. To the extent required by CCPA, Hyros shall allow Customer to conduct inspections or audits in accordance with section 12 of the DPA.

B. VIRGINIA, COLORADO, UTAH & OTHER STATES

1. Definitions

1.1. For purposes of this Section B, the terms "Consumer," "Controller," "Personal data," "Processing," and "Processor" shall have the meanings set forth in the Specific US State Data Protection Laws.

1.2. All references to "Data Subject" in this DPA shall be deemed to be references to "Consumer" as defined in the Specific US State Data Protection Laws.

1.3. The parties acknowledge and agree that Customer is a Controller and Hyros is a Processor for the purposes of the Specific US State Data Protection Laws (to the extent they apply).

2. Obligations

2.1. The nature, purpose, and duration of Processing, as well as the types of Personal Data and categories of Consumers are described in Annex 1 to this DPA.

2.2. Hyros shall adhere to Customer's instructions with respect to the Processing of Customer Personal Data and shall assist Customer in meeting its obligations under the Specific US State Data Protection Laws by:

2.2.1. Assisting Customer in responding to Consumer rights requests under the Specific US State Data Protection Law as set forth in section 6 of the DPA;

2.2.2. Complying with section 4 ("Security") of the DPA with respect to Personal Data provided by Customer;

2.2.3. In the event of a Personal Data Breach, providing information sufficient to enable Customer to meet its obligations pursuant to the Specific US State Data Protection Laws; and

2.2.4. Providing information sufficient to enable the Customer to conduct and document data protection assessments to the extent required by the Specific US State Data Protection Laws.

2.3. Hyros shall maintain the confidentiality of Personal Data provided by Customer and require that each person Processing such Personal Data be subject to a duty of confidentiality with respect to such Processing.

2.4. Upon Customer's written request, Hyros shall delete or return all Personal Data provided by Customer in accordance with section 9 of the DPA, unless retention

of such Customer Personal Data is required or authorized by law or the DPA and/or Terms of Service.

2.5. In the event that Hyros engages a new sub-processor to assist Hyros in providing the Services to Customer under the Terms of Service, Hyros shall enter into a written contract with the sub-processor requiring sub-processor to observe all of the applicable requirements of a Processor set forth in the Specific US State Data Protection Laws.

3. Audit Rights

3.1. Upon Customer's written request at reasonable intervals, Hyros shall, as set forth in section 12 of the DPA, (i) make available to Customer all information in its possession that is reasonably necessary to demonstrate Hyros' compliance with its obligations under the Specific US State Data Protection Law; and (ii) allow and cooperate with reasonable inspections or audits as required under the Specific US State Data Protections.