

## DATA PROCESSING ADDENDUM

### *Liquid Web as Processor*

This Data Processing Addendum (“**Addendum**”) amends, and forms a part of, the Terms of Service found at <https://www.liquidweb.com/about-us/policies/terms-of-service/> or other written agreement for web hosting or related services (in either case, the “**Agreement**”) between Liquid Web, LLC, or one or more of its brands or Affiliates (“**Liquid Web**”) and the undersigned customer of Liquid Web (“**Customer**”). All capitalized terms not defined herein shall have the meanings set forth in the Agreement. Liquid Web and Customer may be referred to herein as a “party” and together as the “parties.”

#### APPLICATION AND EXECUTION OF THIS DPA:

1. If the Customer signing this DPA is a party to the Agreement, this DPA is an addendum to and forms part of the Agreement.
2. If the Customer signing the DPA is not a party to the Agreement directly with Liquid Web, including as customer indirectly through an authorized reseller of Liquid Web, this DPA does not apply.
3. There are three parts to this DPA: 1) the main body of the DPA, 2) Exhibit A (Description of Processing Activities), 3) Exhibit B (EU SCCs, including Annexes I-III), 4) Exhibit C (UK IDTA), and Exhibit D (Swiss Addendum).
4. This DPA has been pre-signed on behalf of Liquid Web as the data processor/importer.
5. To complete this DPA, Customer must:
  - a. Complete the information and sign Page 5.
  - b. Send the completed and signed DPA to Liquid Web by email at [dpa@liquidweb.com](mailto:dpa@liquidweb.com).

Upon Liquid Web’s receipt of the validly completed DPA, this DPA will become legally binding.

#### DATA PROCESSING TERMS

In the course of providing Services under the Agreement, Liquid Web may process certain personal data on behalf of Customer or Customer’s Affiliates to which Customer or Customer’s Affiliates may be, as applicable, a data controller/business or data processor/service provider under applicable Privacy Laws. Accordingly, Liquid Web and Customer agree to comply with this DPA in connection with such Personal Data.

##### 1. Definitions.

- a. “**Affiliate**” means any entity that directly or indirectly controls, is controlled by, or is under common control with the subject entity. “Control,” for purposes of this definition, means direct or indirect ownership or control of more than 50% of the voting interests of the subject entity.
- b. “**Controller**” means an entity which alone or jointly with others determines the purposes and the means of the Processing of Personal Data. For the purposes of this Addendum, Customer is the “Controller.”
- c. “**Data Subject**” means a natural person whose Personal Data is Processed in the context of the Agreement.
- d. “**EU GDPR**” means 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, together with (i) applicable national implementations of GDPR; or (iii) in respect of Switzerland, Swiss Federal Data Protection Act on 19 June 1992 and its Ordinance; in each case, as may be amended, superseded, or replaced.
- e. “**EU SCCs**” means the agreement executed by and between Processor and Customer and attached hereto as **Exhibit B** pursuant to the European Commission’s decision (EU) 2021/915 4 June 2021 on Standard Contractual Clauses for the transfer of Personal Data to Processors established in Third Countries which do not ensure an adequate level of data protection or any set of clauses approved by the European Commission which amends, replaces, or supersedes the same. With respect to the Personal Data of Swiss Data Subjects, EU SCCs means Exhibit B, as modified by Exhibit D (Swiss Data Addendum).

f. **“FADP”** means the Federal Act on Data Protection of 19 June 1992 in Switzerland, together with the August 31, 2022 Data Protection Ordinance.

g. **“GDPR”** means the EU GDPR, FADP, and UK GDPR.

h. **“Law(s)”** means any statute, regulation, ordinance, rule, order, decree, or governmental requirement enacted, promulgated, or imposed by any governmental authority at any level (e.g., municipal, county, province, state or national). Law(s) includes all Privacy Laws.

i. **“Personal Data”** means any information that Liquid Web or its Personnel collect, receive or obtain, from or on behalf of Customer, Customer’s affiliates, or any customer of Customer or a Customer affiliate which qualifies as personal data, personal information, or personally identifiable information under one or more of the Privacy Laws.

j. **“Personal Data Breach”** means a breach of security leading to the accidental or unlawful loss, destruction, alteration, unauthorized disclosure of, or access to Personal Data.

k. **“Personnel”** means any employees, agents, consultants, or contractors of Liquid Web or Customer or Customer’s affiliates, respectively.

l. **“Privacy Laws”** means Laws relating to the security and protection of Personal Data, data privacy, trans-border data flow or data protection, including, without limitation, the GDPR and similar laws in any other applicable jurisdiction, including the California Privacy Rights Act, and including any rules, regulations, directives, principles and policies of Customer.

m. **“Process”** or **“Processing”** means, with respect to Personal Data, any operation or set of operations performed upon Personal Data or 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.

n. **“Processor”** means an entity which Processes Personal Data on behalf of a Controller. For the purposes of this Addendum, Liquid Web is the “Processor.”

o. **“Standard Contractual Clauses”** or **“SCCs”** means, as applicable, the EU SCCs and UK IDTA.

p. **“Subprocessor”** means the entity engaged by the Processor or any further sub-contractor to Process Personal Data on behalf of and under the instructions of the Controller.

q. **“UK GDPR”** means the United Kingdom's adoption of the EU GDPR and the 2018 Data Protection of 2018.

r. **“UK IDTA”** means the agreement executed by and between Processor and Customer and attached hereto as **Exhibit C** pursuant to the UK Information Commissioner’s Office’s issuance that came into force on 21 March 2022 or any set of clauses approved by the UK Information Commissioner’s Office which amends, replaces, or supersedes the same.

2. **Processing.** In the context of the Agreement, Liquid Web shall act as a Processor of Customer and only Process Personal Data for the specific and limited purposes set forth in the Agreement or otherwise listed in **Exhibit A** to this Addendum, on behalf of and in accordance with the instructions of Customer, unless required to do so by applicable Laws. Customer has the sole and exclusive authority to determine the purposes and means of the Processing of Personal Data by Liquid Web. Liquid Web shall Process Personal Data only as necessary to perform its obligations under the Agreement and in compliance with: (a) the express terms and conditions of the Agreement; and (b) all applicable Privacy Laws. When Processing Personal Data, Liquid Web shall provide at least the same level of privacy and security protection for Personal Data as is required by this Addendum and applicable Privacy Laws when required by Applicable Law.

3. **Restrictions on Use of Personal Data.** Liquid Web will not: (i) sell or share any Personal Data (including as such terms are defined under applicable Privacy Laws) or otherwise retain, use, or disclose Personal Data for any purpose other than the specific business purpose set forth in the Agreement, including a commercial purpose other than providing the services under the Agreement, or as otherwise permitted by Privacy Laws and the Agreement; (ii) retain, use, or disclose Personal Data outside of the direct business relationship between the Liquid Web and Customer specified in the Agreement and this Addendum for the purpose set forth therein, unless expressly permitted by Data Laws and the Agreement or this Addendum; or (iii) combine or update Personal Data with personal information Liquid Web receives from, or on behalf of, another person or entity, or that Liquid Web collects from its own interaction with a data subject; provided that, to the extent not prohibited by the Agreement or Addendum, Liquid Web may combine Personal Data with other personal information to perform any permissible business purpose under applicable Data Laws consistent with a data subject's expectations, except for cross-context behavioral advertising or where such combination is with Personal Data of opted-out data subject for advertising and marketing services.

4. **Relocation.**

a. Liquid Web shall not transfer or store Personal Data outside the country to which Customer or its Personnel originally delivered it to Liquid Web for Processing (or, if it was originally delivered to a location inside European Economic Area, Switzerland, or United Kingdom (collectively, "**Europe**"), outside of Europe) without Customer's prior written consent; provided that Customer consents to Liquid Web's transfer of Personal Data to the countries specified in **Exhibit A**, provided that a mechanism to achieve adequacy in respect of that Processing is in place such as: (a) the requirement for Liquid Web and any Subprocessor to execute with Customer or Liquid Web, as the case may be, Standard Contractual Clauses; or (b) the existence of any other specifically approved safeguard for data transfers (as recognized under GDPR) and/or the applicable Public Authority finding of adequacy. In the case of Standard Contractual Clauses, the parties execute the Standard Contractual Clauses in accordance with **Exhibit B (as amended by Exhibit D where applicable) and/or Exhibit C and/or D**, which are incorporated herein by reference, and the following shall apply:

- i. Customer shall be the Data Exporter and Liquid Web shall be the Data Importer under the Standard Contractual Clauses.
- ii. Exhibit A to this Addendum shall be considered as Annex I, Annex II and Annex III to the EU Standard Contractual Clauses and Table 4 to the UK IDTA;
- iii. the parties' signatures to this Addendum shall be considered as signatures to the Standard Contractual Clauses; and
- iv. if so required by the laws or regulatory procedures of any jurisdiction, the parties shall execute or re-execute the Standard Contractual Clauses as separate documents setting out the proposed transfers of Personal Data in such manner as may be required.

2. **Access.** Liquid Web shall limit access to Personal Data to its Personnel who have duties of confidentiality, and security that are substantially similar to those required by the Agreement and shall only Process Personal Data in accordance with Customer's instructions, unless required to do so by applicable Laws, in which case Liquid Web shall inform Customer of the legal requirement before Processing, unless the applicable Law prohibits Liquid Web from doing so.

3. **Disclosure.** Liquid Web shall not sell, disclose, or transfer Personal Data to any third party, including a subcontractor, without Customer's prior written consent, unless such disclosure or transfer is contemplated under this Personal Data Addendum or the Agreement, allowed or required under applicable Law, necessary to comply with a subpoena or other legal process or in cooperation with law enforcement agencies or other government authorities, in which case Liquid Web shall, wherever required and not prohibited by Law, notify Customer promptly in writing before any such disclosure or transfer and comply with all reasonable directions of Customer with respect to such disclosure or transfer.

4. **Subprocessors.**

a. Customer consents to Liquid Web's use of Subprocessors set forth in Section 12 of **Exhibit A**. Liquid Web may update the list with new and replacement Sub-processors before they Process Personal Data. Customer may reasonably object to Liquid Web's use of any new or replacement Sub-processor (e.g. if Sub-processor's Processing may violate Data Protection Laws) by notifying Liquid Web in writing within ten (10) days of the Liquid Web's notification, and the parties will seek to resolve the matter in good faith. Liquid Web will use commercially reasonable efforts to make a change in the Services to avoid Processing of Personal Data by the Subprocessor for which Customer objects without burdening the Customer. If a change is not possible within thirty (30) days of such notification, then either party may terminate the Agreement without penalty the applicable order solely with respect to the Service(s) that cannot be provided by Liquid Web or an approved Subprocessor. Customer will be deemed to have given consent for use of the Subprocessor if an objection is not given in accordance with this Section.

b. Liquid Web shall enter into a written agreement with each Subprocessor that Processes Personal Data containing terms with at least the same level of protection as those contained in this DPA. Liquid Web will be liable to Customer for its Subprocessors' failure to fulfill its Personal Data protection obligations to the same extent Liquid Web would be liable if performing the Services.

5. **Cooperation**. Taking into account the nature of the Processing and the information available to Liquid Web, Liquid Web shall reasonably cooperate with Customer to comply with Privacy Laws, this Addendum, and Customer's instructions, and to assist Customer in fulfilling its own obligations under Privacy Laws, including complying with Data Subjects' requests to exercise their rights, replying to complaints from Data Subjects, replying to investigations and inquiries from supervisory authorities, conducting data protection impact assessments and prior consultations with supervisory authorities.

#### 6. **Security Safeguards**.

a. Liquid Web shall, taking into account the nature of the Personal Data and the risks involved in the Processing, maintain reasonable and appropriate security measures, including technical and organizational safeguards, designed to (a) ensure the security and confidentiality of Personal Data; (b) protect Personal Data against any anticipated threats or hazards to the security and integrity of such information; and (c) protect Personal Data against any actual or suspected unauthorized Processing, loss, use, disclosure or acquisition of, or access to such information.

b. Liquid Web shall exercise all necessary and appropriate supervision over its relevant Personnel to maintain appropriate privacy, confidentiality, and security of Personal Data.

c. Reasonable and appropriate technical and organizational measures include at the minimum the security measures set forth in the Agreement and as set forth in Section 11 of **Exhibit A**.

#### 7. **Data Breach Notification**.

a. Without limiting any other obligation under the Agreement, Liquid Web shall immediately inform Customer after becoming aware of a Personal Data Breach. Taking into account the nature of Processing and the information available to Liquid Web, Liquid Web shall assist Customer in complying with its obligations under Privacy Laws to notify Data Subjects of a Personal Data Breach.

8. **Return or Destruction of Personal Data**. Promptly upon the expiration or termination of the Agreement, or upon request by Customer at any other time, Liquid Web shall securely destroy every original and copy in every media of all Personal Data in Liquid Web's possession, custody, or control. If applicable Law allows for the deletion or return of such information, this section serves as Customer's selection of deletion at the end of the Term. If applicable Law or Liquid Web's data retention policy requires retention of the Personal Data, Liquid Web will ensure the continued confidentiality of the Personal Data in accordance with applicable Privacy Laws.

9. **Further Agreements**. Liquid Web shall enter into any further privacy, confidentiality, or information security agreement reasonably requested by Customer to the extent necessary to comply with applicable Privacy Laws. In

case of any conflict between the Agreement and any such further privacy, confidentiality, or information security agreement, such further agreement shall prevail with regard to the Processing of Personal Data covered by it.

10. **Inability to Comply.** Liquid Web shall promptly notify Customer in writing if Liquid Web cannot comply with its obligations regarding Personal Data or under this Addendum.

11. **Audit.** During the term of the Agreement:

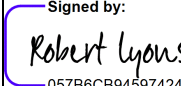
a. Upon Customer's request, Liquid Web shall make available to Customer all information as is necessary to enable Customer to verify Liquid Web's compliance with this Addendum.

b. To the extent required by applicable Law, Liquid Web shall allow Customer (or an inspection body composed of independent members selected by Customer, and which possess any professional qualifications required by Law and are mutually agreeable to Customer and Liquid Web) to audit and review Liquid Web's information security program, data processing facilities, and data protection compliance program to verify Liquid Web's compliance with this Addendum and applicable Privacy Laws.

12. **Order of Precedence.** This Addendum is incorporated into and forms part of the Agreement. For matters not addressed under this Addendum, the terms of the Agreement apply. In the event of a conflict between the terms of the Addendum and an Exhibit to this Addendum, the terms of the Exhibit shall prevail, and in the event of a conflict between the Exhibits, the Standard Contractual Clauses shall prevail. The liability of each party and its respective affiliates' arising out of or relating to this Addendum shall be subject to the section(s) of the Agreement governing limitations of liability, and this Addendum and any dispute or claim arising out of or in connection with it or its subject matter or formation shall be governed by and construed in accordance with the laws applicable to the Agreement.

13. **Standard Contractual Clauses.** The Standard Contractual Clauses apply to: (a) the legal entity that has executed the Standard Contractual Clauses as a data exporter and its affiliates; and (b) all affiliates of Customer established within Europe that are allowed to contract with Liquid Web as set forth in the Agreement. For the purposes of the Standard Contractual Clauses the aforementioned entities shall be deemed "data exporters."

WITNESS WHEREOF, the parties' authorized representatives have duly executed this DPA.

CUSTOMER:		LIQUID WEB, LLC	
By		By	<div>Signed by:</div>  <div>057B6CB94597424...</div>
Name		Name	Robert A. Lyons
Title		Title	Chief Executive Officer
Address		Address	2703 Ena Drive Lansing, MA 48917
Email		Email	dpa@liquidweb.com
Registration number (if any)			
Date		Date	December 4, 2025

## **Exhibit A**

### **Description of Processing Activities**

1. **Controller.** The Controller is: The Customer entity specified on Page 1 of the Addendum.
2. **Processor.** The Processor is: The Liquid Web entity specified on Page 1 of the Addendum.
3. **Description of Services.** Cloud-based services such as web hosting and/or WordPress software and tools, as further detailed in the Agreement.
4. **Data subjects.** The personal data transferred concern the following categories of data subjects: Natural persons who are (i) Customer's prospective customers, customers, resellers, referrers, business partners, and vendors; (ii) employees or contact persons of Customer's prospective customers, customers, resellers, referrers, business partners, and vendors; (iii) Customer's employees, agents, advisors, and freelancers; and (iv) authorized by Customer to use the services authorized by the Agreement.
5. **Categories of data.** The personal data transferred concern the following categories of data: Any personal data relating to individuals made available by Customer to Liquid Web's hosting environment, which is determined and controlled by the Customer in its sole discretion. Specifically, the categories of personal data transferred may include (i) in relation to visitors of Customer, online identification data, professional life data, personal life data, connection data, or localization data (including IP addresses); and (ii) content uploaded by Customer, its online visitors and/or other partners to Customer's online properties.
6. **Special categories of data .** The personal data transferred concern the following special categories of data: Customer, its online visitors, and others may, in Customer's sole discretion, upload to Customer's online properties, information revealing racial or ethnic origins, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning an individual's health or sex life. Applied restrictions and safeguards may be found at <https://www.liquidweb.com/about-us/policies/certifications/> .
7. **The frequency of the sharing of data and the transfer thereof (e.g., whether the data is transferred on a one-off or continuous basis):** The data is transferred on a continuous basis while the parties are under Agreement and Customer is utilizing Liquid Web's services.
8. **Processing operations.** The personal data transferred will be subject to the following basic processing activities: Any processing activity necessary to provide services in Liquid Web's hosting environment pursuant to the Agreement, including handling and storage of such information.
9. **The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period:** Once Liquid Web is no longer providing services to Customer, Liquid Web will generally delete Customer's data between 30-60 days after the expiration of services; provided, however, that Liquid Web may keep Customer's business contact information and other account information for a longer period based on Liquid Web's legitimate business purposes, and in all cases processor may retain personal data for a longer period as required by applicable law.
10. **The Countries where Processing will occur:** Australia, the Netherlands, United Kingdom, United States of America.
11. **Technical and Organizational Measures:** Technical and organizational measures implemented and relevant certifications are listed at <https://www.liquidweb.com/about-us/policies/certifications/>.
12. **Subprocessors:** Available at <https://www.liquidweb.com/policies/sub-processor-list/>.

**EXHIBIT B**  
**EU 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.
- b. These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

***Clause 3***

**Third-party beneficiaries**

- a. Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:
  - i. Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;
  - ii. Clause 8 - Module One: Clause 8.5 (e) and Clause 8.9(b); Module Two: Clause 8.1(b), 8.9(a), (c), (d) and (e); Module Three: Clause 8.1(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g); Module Four: Clause 8.1 (b) and Clause 8.3(b);
  - iii. Clause 9 - Module Two: Clause 9(a), (c), (d) and (e); Module Three: Clause 9(a), (c), (d) and (e);
  - iv. Clause 12 - Module One: Clause 12(a) and (d); Modules Two and Three: Clause 12(a), (d) and (f);

- v. Clause 13;
- vi. Clause 15.1(c), (d) and (e);
- vii. Clause 16(e);
- viii. Clause 18 - Modules One, Two and Three: Clause 18(a) and (b); Module Four: Clause 18.

- b. Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

***Clause 4***  
**Interpretation**

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

***Clause 5***  
**Hierarchy**

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

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

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

***Clause 7***  
**Docking clause**

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

**SECTION II – OBLIGATIONS OF THE PARTIES**

***Clause 8***  
**Data protection safeguards**

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

**8.1 Instructions**

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



## 8.2 Purpose limitation

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

## 8.3 Transparency

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

## 8.4 Accuracy

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

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

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

## 8.6 Security of processing

- a. The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter “personal data breach”). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.
- b. The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

- c. In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.
- d. The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

### **8.7 Sensitive data**

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

### **8.8 Onward transfers**

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union<sup>4</sup> (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 30 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.<sup>8</sup> 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 Sub-Processor) 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<sup>12</sup>;
  - iii. any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.
- c. The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.
- d. The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.
- e. The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).
- f. Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly

identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation.

The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

### **Clause 15**

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

##### **15.1 Notification**

- a. The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:
  - i. receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or
  - ii. becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.
- b. If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.
- c. Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).
- d. The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.
- e. Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

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

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

- b. The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.
- c. The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

#### **SECTION IV – FINAL PROVISIONS**

##### ***Clause 16***

##### **Non-compliance with the Clauses and termination**

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

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

- d. Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.
- e. Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

##### ***Clause 17***

##### **Governing law**

These Clauses shall be governed by the law of 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 the Netherlands.

**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 the Netherlands.
- c. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.
- d. The Parties agree to submit themselves to the jurisdiction of such courts.

**APPENDIX**

**ANNEX I**

**A. LIST OF PARTIES**

See the parties listed on page 1 of the Addendum, with contact details on the signature page of the Addendum.

**B. DESCRIPTION OF TRANSFER**

See Exhibit A of the Addendum.

**C. COMPETENT SUPERVISORY AUTHORITY**

The Autoriteit Persoonsgegevens (AP) (Dutch Data Protection Authority)

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

See Section 11 of Exhibit A of the Addendum.

**ANNEX III – LIST OF SUB-PROCESSORS**

See Section 12 of Exhibit A of the Addendum.



**EXHIBIT C**  
**UK IDTA**

**Part 1: Tables**

**Table 1: Parties and signatures**

<b>Start date</b>	The date of the Addendum	
<b>The Parties</b>	<b>Exporter (who sends the Restricted Transfer)</b>	<b>Importer (who receives the Restricted Transfer)</b>
<b>Parties' details</b>	The Customer entity specified on Page 1 of the Addendum	The Liquid Web entity specified on Page 1 of the Addendum
<b>Key Contact</b>	See Signature Page to Addendum	See Signature Page to Addendum
<b>Importer Data Subject Contact</b>		See Signature Page to Addendum
<b>Signatures confirming each Party agrees to be bound by this IDTA</b>	Signed for and on behalf of the <b>Exporter</b> set out above See signature to Addendum	Signed for and on behalf of the <b>Importer</b> set out above See signature to Addendum

**Table 2: Transfer Details**

<b>UK country's law that governs the IDTA:</b>	<input checked="" type="checkbox"/> England and Wales <input checked="" type="checkbox"/> Northern Ireland <input checked="" type="checkbox"/> Scotland
<b>Primary place for legal claims to be made by the Parties</b>	<input checked="" type="checkbox"/> England and Wales <input checked="" type="checkbox"/> Northern Ireland <input checked="" type="checkbox"/> Scotland
<b>The status of the Exporter</b>	In relation to the Processing of the Transferred Data: <input checked="" type="checkbox"/> Exporter is a Controller <input type="checkbox"/> Exporter is a Processor or Sub-Processor
<b>The status of the Importer</b>	In relation to the Processing of the Transferred Data: <input type="checkbox"/> Importer is a Controller <input checked="" type="checkbox"/> Importer is the Exporter's Processor or Sub-Processor

	<input type="checkbox"/> Importer is <b>not</b> the Exporter's Processor or Sub-Processor (and the Importer has been instructed by a Third Party Controller)
<b>Whether UK GDPR applies to the Importer</b>	<input checked="" type="checkbox"/> UK GDPR applies to the Importer's Processing of the Transferred Data <input type="checkbox"/> UK GDPR does not apply to the Importer's Processing of the Transferred Data
<b>Linked Agreement</b>	<p><b>If the Importer is the Exporter's Processor or Sub-Processor</b> – the agreement(s) between the Parties which sets out the Processor's or Sub-Processor's instructions for Processing the Transferred Data:</p> <p>Name of agreement: As specified on Page 1 of the Addendum</p> <p>Date of agreement: As specified on Page 1 of the Addendum</p> <p>Parties to the agreement: The parties set forth above as Exporter and Importer</p> <p>Reference (if any): N/A</p> <p><b>Other agreements</b> – any agreement(s) between the Parties which set out additional obligations in relation to the Transferred Data, such as a data sharing agreement or service agreement:</p> <p>Name of agreement:</p> <p>Date of agreement:</p> <p>Parties to the agreement:</p> <p>Reference (if any):</p> <p><b>If the Exporter is a Processor or Sub-Processor</b> – the agreement(s) between the Exporter and the Party(s) which sets out the Exporter's instructions for Processing the Transferred Data:</p> <p>Name of agreement:</p> <p>Date of agreement:</p> <p>Parties to the agreement:</p> <p>Reference (if any):</p>
<b>Term</b>	<p>The Importer may Process the Transferred Data for the following time period:</p> <input checked="" type="checkbox"/> the period for which the Linked Agreement is in force <input type="checkbox"/> time period: <input type="checkbox"/> (only if the Importer is a Controller or not the Exporter's Processor or Sub-Processor) no longer than is necessary for the Purpose.
<b>Ending the IDTA before the end of the Term</b>	<input checked="" type="checkbox"/> the Parties cannot end the IDTA before the end of the Term unless there is a breach of the IDTA or the Parties agree in writing. <input type="checkbox"/> the Parties can end the IDTA before the end of the Term by serving:

	<input type="text"/> months' written notice, as set out in Section 29 of the Mandatory Clauses (How to end this IDTA without there being a breach).
<b>Ending the IDTA when the Approved IDTA changes</b>	Which Parties may end the IDTA as set out in Section 29.2 of the Mandatory Clauses: <input type="checkbox"/> Importer <input type="checkbox"/> Exporter <input checked="" type="checkbox"/> neither Party
<b>Can the Importer make further transfers of the Transferred Data?</b>	<input checked="" type="checkbox"/> The Importer MAY transfer on the Transferred Data to another organisation or person (who is a different legal entity) in accordance with Section 16.1 of the Mandatory Clauses (Transferring on the Transferred Data). <input type="checkbox"/> The Importer MAY NOT transfer on the Transferred Data to another organisation or person (who is a different legal entity) in accordance with Section 16.1 of the Mandatory Clauses (Transferring on the Transferred Data).
<b>Specific restrictions when the Importer may transfer on the Transferred Data</b>	The Importer MAY ONLY forward the Transferred Data in accordance with Section 16.1 of the Mandatory Clauses: <input type="checkbox"/> if the Exporter tells it in writing that it may do so. <input type="checkbox"/> to: <input type="text"/> <input type="checkbox"/> to the authorised receivers (or the categories of authorised receivers) set out in: <input checked="" type="checkbox"/> there are no specific restrictions.
<b>Review Dates</b>	<input type="checkbox"/> No review is needed as this is a one-off transfer and the Importer does not retain any Transferred Data First review date: <input type="text"/> The Parties must review the Security Requirements at least once: <input type="checkbox"/> each <input type="text"/> month(s) <input type="checkbox"/> each quarter <input type="checkbox"/> each 6 months <input type="checkbox"/> each year <input type="checkbox"/> each <input type="text"/> year(s) <input checked="" type="checkbox"/> each time there is a change to the Transferred Data, Purposes, Importer Information, TRA or risk assessment

**Table 3: Transferred Data**

<b>Transferred Data</b>	The personal data to be sent to the Importer under this IDTA consists of:
-------------------------	---

	<input checked="" type="checkbox"/> The categories of Transferred Data will update automatically if the information is updated in the Linked Agreement referred to. <input type="checkbox"/> The categories of Transferred Data will NOT update automatically if the information is updated in the Linked Agreement referred to. The Parties must agree a change under Section 5.3 of the Mandatory Clauses.
<b>Special Categories of Personal Data and criminal convictions and offences</b>	<p>The Transferred Data includes data relating to:</p> <input type="checkbox"/> racial or ethnic origin <input type="checkbox"/> political opinions <input type="checkbox"/> religious or philosophical beliefs <input type="checkbox"/> trade union membership <input type="checkbox"/> genetic data <input type="checkbox"/> biometric data for the purpose of uniquely identifying a natural person <input type="checkbox"/> physical or mental health <input type="checkbox"/> sex life or sexual orientation <input type="checkbox"/> criminal convictions and offences <input type="checkbox"/> none of the above <input checked="" type="checkbox"/> set out in: Exhibit A of the Addendum
	<p>And:</p> <input type="checkbox"/> The categories of special category and criminal records data will update automatically if the information is updated in the Linked Agreement referred to. <input type="checkbox"/> The categories of special category and criminal records data will NOT update automatically if the information is updated in the Linked Agreement referred to. The Parties must agree a change under Section 5.3 of the Mandatory Clauses.
<b>Relevant Data Subjects</b>	<p>The Data Subjects of the Transferred Data are:</p> <input checked="" type="checkbox"/> The categories of Data Subjects will update automatically if the information is updated in the Linked Agreement referred to. <input type="checkbox"/> The categories of Data Subjects will not update automatically if the information is updated in the Linked Agreement referred to. The Parties must agree a change under Section 5.3 of the Mandatory Clauses.
<b>Purpose</b>	<input type="checkbox"/> The Importer may Process the Transferred Data for the following purposes: <input type="checkbox"/> The Importer may Process the Transferred Data for the purposes set out in: <p>In both cases, any other purposes which are compatible with the purposes set out above.</p>

	<input checked="" type="checkbox"/> The purposes will update automatically if the information is updated in the Linked Agreement referred to. <input type="checkbox"/> The purposes will NOT update automatically if the information is updated in the Linked Agreement referred to. The Parties must agree a change under Section 5.3 of the Mandatory Clauses.
--	---

**Table 4: Security Requirements**

<b>Security of Transmission</b>	Please see Section 11 of Exhibit A to the Addendum
<b>Security of Storage</b>	Please see Section 11 of Exhibit A to the Addendum
<b>Security of Processing</b>	Please see Section 11 of Exhibit A to the Addendum
<b>Organisational security measures</b>	Please see Section 11 of Exhibit A to the Addendum
<b>Technical security minimum requirements</b>	Please see Section 11 of Exhibit A to the Addendum
<b>Updates to the Security Requirements</b>	<input checked="" type="checkbox"/> The Security Requirements will update automatically if the information is updated in the Linked Agreement referred to. <input type="checkbox"/> The Security Requirements will NOT update automatically if the information is updated in the Linked Agreement referred to. The Parties must agree a change under Section 5.3 of the Mandatory Clauses.

**Part 2: Extra Protection Clauses**

<b>Extra Protection Clauses:</b>	
<b>(i) Extra technical security protections</b>	
<b>(ii) Extra organisational protections</b>	
<b>(iii) Extra contractual protections</b>	

Part 3: Commercial Clauses

Commercial Clauses	
--------------------	--

Part 4: Mandatory Clauses

Mandatory Clauses	Part 4: Mandatory Clauses of the Approved IDTA, being the template IDTA A.1.0 issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 5.4 of those Mandatory Clauses.
-------------------	--

**EXHIBIT D**  
**SWISS DATA ADDENDUM**

In relation to Personal Data subject to the FADP, the EU SCCs (Exhibit B) as completed above shall also apply, with the following amendments. Insofar as the Personal Data is subject to both the FADP and the EU GDPR or UK GDPR, these modifications shall only apply with respect to the Swiss Personal Data and shall not affect the application of the clauses of the EU SCCs for the purposes of the EU GDPR or UK GDPR.

- 1) References to the EU GDPR shall be interpreted as references to the FADP as applicable;
- 2) References to specific sections of the EU GDPR shall be replaced with the equivalent section of the FADP as applicable;
- 3) References to the EU, UK, member state, or member state law shall be interpreted as references to “Switzerland” or “Swiss law” as the case may be, and the term “member state” shall not be interpreted in such a way as to exclude data subjects in Switzerland from the possibility of suing for their rights in their place of habitual residence (i.e., Switzerland);
- 4) The competent supervisory authority relating to Swiss Personal Data is the Swiss Federal Data Protection and Information Commissioner; this also applies to Clause 13(a) and Annex III of the EU SCCs;
- 5) References to the “competent supervisory authority” and “competent courts” will be replaced with the “the Swiss Federal Data Protection and Information Commissioner” and the “relevant courts in Switzerland”; and
- 6) In Clause 17 of the EU SCCs, the governing law shall be the laws of Switzerland.