

## Data Processing Addendum

This Data Processing Addendum ("**DPA**") is incorporated by reference into Aqua's End User License Agreement SaaS or other agreement governing the use of Aqua's services ("**Agreement**"), entered by and between Aqua Security Software Ltd. or any of its Affiliates ("**Aqua**") and the Customer (both as defined in the Agreement) to reflect the parties' agreement with regard to the Processing of Controller Personal Data. Both parties shall be referred to as the "**Parties**" and each, a "**Party**". Capitalized terms not otherwise defined herein shall have the meaning given to them in the Agreement.

**Whereas**, in connection with the performance of its obligations under the Agreement, Aqua may Process Customer Personal Data (as defined below) on behalf of Customer; and

**Whereas**, the parties wish to set forth the mutual obligations with respect to the processing of Customer Personal Data by Aqua;

**Now therefore**, intending to be legally bound, the parties hereby agree as follows:

1. **Definitions.** In addition to capitalized terms defined elsewhere in this DPA, the following terms shall have the meanings set forth below:
  - 1.1. "**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 interest in the subject entity.
  - 1.2. "**Authorized Affiliate**" means any of Customer's Affiliate(s) which is explicitly permitted to use the Services pursuant to the Agreement between Customer and Aqua but has not signed its own agreement with Aqua and is not a "Customer" as defined under the Agreement.
  - 1.3. "**Applicable Law**" means all privacy and data protection laws and regulations applicable to the processing of Customer Personal Data hereunder and in effect at the time of Processor's performance hereunder, including (i) the Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation) ("**GDPR**"), laws implementing or supplementing the GDPR; (ii) the Data Protection Act 2018, as well as the GDPR as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018 and as amended by the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019 (SI 2019/419) (the "**UK GDPR**") (iii) Israel's Protection of Privacy Law, 1981 and regulations and orders promulgated thereunder, including without limitation Protection of Privacy Regulations (Information Security) 2017, and Directive 2-2011 for Use of Outsourcing for the processing of Personal Data (collectively, "**Privacy Law**"); (iv) the California Consumer Privacy Act of 2018, Cal. Civil Code Title 1.81.5 and the regulations thereunder, as may be amended from time to time, including the California Privacy Rights Act ("**CCPA**"); and/or (v) the Swiss Federal Act on Data Protection of 19 June 1992, as revised as of 25 September 2020 ("**FADP**").
  - 1.4. "**Customer Personal Data**" means any Personal Data (or equivalent term under Applicable Laws, including Personal Information under the CCPA) processed by Aqua solely on behalf of Customer under this DPA and the Agreement.
  - 1.5. "**Sensitive Data**" means Personal Data that is protected under a special legislation and requires unique treatment, such as "special categories of data", "sensitive data" or other materially similar terms under Applicable Laws, which may include any of the following: (a) social security number, tax file number, passport number, driver's license number, or similar identifier (or any portion thereof); (b) credit or debit card number; (c) financial,

credit, genetic, biometric or health information; (d) information 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; and/or (e) account passwords in unhashed form.

- 1.6. "**Sub-Processor**" means any person (excluding an employee of Aqua) or entity, including Aqua Affiliates, that Process Customer Personal Data under the instruction and supervision of Aqua in connection with the Agreement.
- 1.7. "**Standard Clauses**" means (i) where the GDPR applies, the standard clauses for the transfer of Personal Data under Commission implementing Decision (EU) 2021/914 of June 4, 2021 on the Standard Clauses pursuant to Regulation (EU) 2016/679 of the European Parliament and Council as applicable to the controller transferring personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council (available [here](#)); and (ii) where the UK GDPR applies, the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses issued by the Commissioner of 21 March 2022.
- 1.8. The terms "**Controller**", "**Data Subject**", "**Data Protection Officer**", "**Member State**", "**Personal Data**", "**Personal Data Breach**", "**Processor**", "**Processing**", and "**Supervisory Authority**" shall have the meanings ascribed to them in the GDPR.
- 1.9. The terms "**Business**", "**Consumer**", "**Personal Information**", "**Processing**", "**Sell**", "**Share**", "**Service Provider**", shall have the meanings ascribed to them in the CCPA (to the extent applicable).

## 2. **Roles of the Parties**

- 2.1. The Parties acknowledge and agree that with regard to the processing of Customer Personal Data (i) Customer serves as a Controller of Customer Personal Data and (ii) Aqua serves as a Processor of such Customer Personal Data on Customer's behalf. The terms "Controller" and "Processor" below hereby signify Customer and Aqua, respectively
- 2.2. When Customer collects Personal Information that include Customer Personal Data that is subject to the CCPA, Customer is the Business with respect to such Customer Personal Data for purposes of this DPA and Aqua serves as a Service Provider on its behalf.

## 3. **Processing of Customer Personal Data**

- 3.1. Customer, in its use of the Services, and Customer's instructions to the Aqua, shall comply with Applicable Laws. Customer shall establish and have any and all required legal bases in order to collect, process and transfer to Aqua the Customer Personal Data, and to authorize the processing by Aqua, and for Aqua's processing activities on Customer's behalf, including the pursuit of 'business purposes' as defined under the CCPA.
- 3.2. Aqua shall Process Customer Personal Data on Customer's behalf for the following purposes: (i) Processing for Customer as part of its provision of the services detailed in the Agreement ("**Services**"); (ii) Processing in accordance with the Agreement and this DPA; (iii) Processing to comply with Customer's reasonable and documented instructions as specified in the Agreement and/or in this DPA where such instructions are consistent with the terms of the Agreement, including without limitation with regard to transfers of Customer Personal Data to a third country or international organization; (iv) rendering Customer Personal Data fully anonymous, non-identifiable and non-personal in accordance with applicable standards recognized by Applicable Laws and guidance issued thereunder; (v) processing as required by any laws to which Aqua is subject and/or as required by a court of competent jurisdiction or other competent government or semi-governmental authority. In such event, Aqua shall, unless prohibited by such law on

important grounds of public interest, inform Customer of that requirement before engaging in such Processing.

- 3.3. In addition, and without derogating from the foregoing, with respect to Customer Personal Data subject to the CCPA, Aqua acknowledges and confirms that it does not receive or process any Customer Personal Data as consideration for any services or other items that Aqua provides to Customer under the Agreement. Aqua certifies that it understands the rules, requirements and definitions of the CCPA, to the extent it applies to Aqua's Processing of Customer Personal Data under the Agreement and this DPA, and agrees to refrain from Selling or Sharing any Customer Personal Data, without Customer's prior written consent or instruction, nor take any action that it expects to cause any transfer of Customer Personal Data to or from Aqua under the Agreement to qualify as Selling and/or Sharing such Customer Personal Data under the CCPA. Aqua shall not have, derive, or exercise any rights or benefits regarding Customer Personal Data, nor shall it combine the Customer Personal Data with any personal information it processes on behalf of other parties or use and disclose Customer Personal Data outside the direct business relationship between Aqua and Customer— except for the purposes for which such Customer Personal Data was provided to it as stipulated in this DPA or the Agreement or if expressly permitted under the CCPA, and subject to the Agreement between the Parties. Aqua further acknowledges that Customer disclosed such Customer Personal Data only for the specified purposes set out in this DPA and the Agreement or as otherwise permitted by the CCPA. Aqua shall comply with all applicable sections of the CCPA, including implementing reasonable security measures as appropriate under the CCPA. Aqua further acknowledges that Customer has the right, upon notice, to take reasonable and appropriate steps to stop and remediate any unauthorized use of Customer Personal Data by Aqua, subject to audit conditions previously determined by the Parties in this DPA. Aqua shall notify Customer if it makes a determination that it can no longer meet its obligations under this Section 3.3 or the CCPA.
- 3.4. Controller sets forth the details of the Processing of Customer Personal Data, as required by Article 28(3) of the GDPR in **Schedule A** (*Details of Processing of Customer Personal Data*), attached hereto.
- 3.5. The Parties agree that the Services are not intended for the processing of Sensitive Data, and that if Customer wishes to use the Services to process Sensitive Data, it must first obtain Aqua's explicit prior written consent and enter into any additional agreements as required by Aqua.

#### 4. **Cross-Border Transfers**

- 4.1. Transfers from the EEA, Switzerland and the United Kingdom to countries that offer adequate level or data protection. Customer Personal Data may be transferred from EU Member States, the three EEA member countries (Norway, Liechtenstein and Iceland) (collectively, "EEA"), Switzerland and the United Kingdom ("UK") to countries that offer an adequate level of data protection under or pursuant to the adequacy decisions published by the relevant data protection authorities of the EEA, the European Union, the Member States or the European Commission, Switzerland, and/or the UK as relevant ("**Adequacy Decisions**"), as applicable, without any further safeguard being necessary.
- 4.2. Transfers from the EEA, Switzerland and the United Kingdom to other countries. If the Processing of Customer Personal Data by Aqua includes a transfer (either directly or via onward transfer):
  - 4.2.1. from the EEA to other countries which have not been subject to a relevant Adequacy Decision, and such transfers are not performed through an alternative recognized compliance mechanism for the lawful transfer of personal data (as defined in the GDPR) outside the EEA ("**EEA Transfer**"), the terms set forth in Part 1 of **Schedule C** (EEA Cross Border Transfers) shall apply;

4.2.2. from the UK to other countries which have not been subject to a relevant Adequacy Decision, and such transfers are not performed through an alternative recognized compliance mechanism for the lawful transfer of personal data (as defined in the UK GDPR) outside the UK (“**UK Transfer**”), the terms set forth in Part 2 of **Schedule C** (UK Cross Border Transfers) shall apply;

4.2.3. from Switzerland to other countries which have not been subject to a relevant Adequacy Decision, and such transfers are not performed through an alternative recognized compliance mechanism for the lawful transfer of personal data (as defined in the FADP) outside Switzerland (“**Switzerland Transfer**”), the terms set forth in Part 3 of **Schedule C** (Switzerland Cross Border Transfers) shall apply;

4.2.4. the terms set forth in Part 4 of **Schedule C** (Additional Safeguards) shall apply to any of such Transfers.

## 5. **Processor Employees**

5.1. Aqua shall ensure that access to the Customer Personal Data is limited on a need to know and/or access basis, and that all Aqua employees receiving such access have committed themselves to confidentiality

5.2. Aqua shall implement appropriate organizational controls, security measures, and training programs to train those of its personnel authorized to access the Customer Personal Data in order to ensure compliance with the Agreement, this DPA, and Applicable Laws.

## 6. **Security**

6.1. Aqua shall implement and maintain appropriate technical and organizational measures to ensure an appropriate level of security of the Customer Personal Data, including, as appropriate and applicable, structural and corporate segregation of the Customer Personal Data and other security measures commensurate with the type of Customer Personal Data and the risk of a data security breach, including as may be set forth in the Binding Security Document attached hereto as **Schedule B** and any other measure referred to in Article 32(1) of the GDPR. The parties acknowledge that security requirements are constantly changing and that effective security requires frequent evaluation and regular improvements of outdated security measures. Aqua will therefore evaluate the measures implemented in accordance with this Section 6 on an ongoing basis and will, at its own cost, tighten, supplement and improve these measures in order to maintain compliance with the requirements set out herein. Upon the Customer’s reasonable request, Aqua will reasonably assist Customer, in ensuring compliance with the obligations pursuant to Articles 32 to 36 of the GDPR taking into account the nature of the processing and the information available to Aqua.

6.2. If required under Applicable Law, Aqua will appoint a Data Protection Officer.

## 7. **Personal Data Breach**

7.1. Aqua shall notify Customer without undue delay by written notice upon Aqua becoming aware of a Personal Data Breach.

7.2. In such event, Aqua shall provide Customer with all information then known and available to Customer, relating to (i) the nature of the Personal Data Breach including, where possible, the categories and approximate number of Data Subjects concerned; (ii) the likely consequences of the Personal Data Breach; (iii) the name and contact details of Aqua's Data Protection Officer or another contact point where more information can be obtained; and (iv) a description of the measures taken or proposed to be taken by Aqua to address the incident including, where appropriate, measures to mitigate its possible adverse effects. The obligations herein shall not apply to incidents that are caused by Customer or anyone who uses the Services on Customer’s behalf.

- 7.3. Aqua shall reasonably cooperate with Customer in connection with the investigation, mitigation, and remediation of any Personal Data Breach and shall take all necessary and reasonable corrective action.
- 7.4. Customer will not make, disclose, release or publish any finding, admission of liability, communication, notice, press release or report concerning any Personal Data Breach which directly or indirectly identifies Aqua (including in any legal proceeding or in any notification to regulatory or supervisory authorities or affected individuals) without Aqua's prior written approval, unless, and solely to the extent that, Customer is compelled to do so pursuant to Applicable Laws. In the latter case, unless prohibited by such laws, Customer shall provide Aqua with reasonable prior written notice to provide Aqua with the opportunity to object to such disclosure and in any case Customer will limit the disclosure to the minimum scope required.

## 8. **Sub Processing**

- 8.1. Aqua's current Sub-Processors are listed in **Schedule A** of this DPA ("**Sub-Processor List**"). The Sub-Processor List as of the date of first use of the Services by Controller is hereby deemed authorized upon first use of the Services. Aqua shall provide notification of any new Sub-Processor(s) before authorizing such new Sub-Processor(s) to process Customer Personal Data in connection with the provision of the Services.
- 8.2. With respect to each new Sub-Processor, Aqua shall ensure that the arrangement between Aqua and such Sub-Processor is governed by a written contract, including terms which offer the same or materially similar level of data protection for Customer Personal Data as those set out in this DPA and that meet the requirements of Applicable Law.
- 8.3. Where a Sub-processor fails to fulfil its data protection obligations concerning its Processing of Customer Personal Data, Aqua shall remain responsible for the performance of any Sub-Processor's obligations.

## 9. **Data Subject Rights**

- 9.1. When a Data Subject whose Personal Data is being Processed by Aqua on Customer's behalf under this DPA submits a written request to Aqua regarding the Customer Personal Data, Aqua:
  - 9.1.1. Shall, to the extent permitted, provide Customer with written notice of the inquiry together with all relevant details ; and
  - 9.1.2. shall not respond to that request except on the written instructions of Customer or as required by Applicable Law to which the Aqua is subject, in which case Aqua shall, to the extent permitted by Applicable Law, inform Customer of that legal requirement prior to responding to the request.
- 9.2. Taking into account the nature of the Processing, Aqua shall assist Customer by implementing appropriate technical and organizational measures, insofar as this is possible and reasonable, for the fulfilment of Customer's obligation to respond to a Data Subject's request under Applicable Laws.

10. **Data Protection Impact Assessment and Prior Consultation.** At Customer's reasonable request, Aqua shall provide, at Customer's cost, with reasonable assistance needed to fulfill Customer's obligation under the GDPR or the UK GDPR (as applicable) to carry out a data protection impact assessment related to Customer's use of the Services or prior consultations with Supervisory Authorities or other competent data privacy authorities, as required under any Applicable Law, to the extent Customer does not otherwise have access to the relevant information, and to the extent such information is available to Aqua.

## 11. **Retention and Deletion of Customer Personal Data.**

- 11.1. Aqua will retain Customer Personal Data only for as long as necessary to satisfy the purposes for which it was provided to Aqua by Customer.

- 11.2. Following termination of the Agreement, Aqua shall delete all Customer Personal Data or any copies or portion thereof, including without limitation, deletion from its systems, once such data is no longer necessary to be retained or upon the request of Customer, unless Applicable Laws or other laws require otherwise.
12. Notwithstanding the foregoing, Aqua may retain Customer Personal Data to the extent authorized or required by the laws applicable to the Aqua such as for evidence purposes and/or for the establishment, exercise or defense of legal claims and/or for compliance with legal obligations, subject to the confidentiality and security obligations outlined in this DPA.
13. **Inspection and Audit Rights**
  - 13.1. Aqua shall make available to Customer that is not a competitor of Aqua or to any auditor mandated by Customer that is not a competitor of Aqua and not in conflict with Aqua (subject to their confidentiality and non-compete undertakings), upon Customer's thirty (30) days prior written request (no more than once every twelve (12) months), and subject to strict confidentiality undertakings by Customer, all material and information necessary to enable Customer to confirm compliance with this DPA, and shall allow for audits, including inspections, by the Customer or an auditor on its behalf in relation to the Processing of the Customer Personal Data by Aqua provided, however, that such information, audits, inspections and the results therefrom, including the documents reflecting the outcome of the audit and/or the inspections, shall only be used by Customer to assess compliance with this DPA, and shall not be used for any other purpose or disclosed to any third party without Aqua's prior written approval.
  - 13.2. Customer and Aqua shall mutually agree in advance on the date, scope, duration, and security and confidentiality controls applicable to the audit.
  - 13.3. Customer shall ensure that it (and each of its mandated auditors) will not cause (or, if it cannot avoid, minimize) any damage, injury or disruption to Aqua's premises, equipment, personnel and business while conducting such audit or inspection.
  - 13.4. Upon Aqua's first request, Customer shall return all records or documentation in Customer's possession or control provided by Aqua in the context of the audit and/or the inspection
14. **Notice of Infringement**. Aqua shall inform Customer without undue delay if, in its opinion, an instruction received under this DPA infringes the Applicable Laws. In such an event, Aqua may temporarily cease all Processing of the affected Customer Personal Data (other than securely storing such data) and/or suspend Customer's access to the Services. If the Parties do not agree on a resolution to the issue in question and the costs thereof, Customer may, as its sole remedy, terminate the Agreement and this DPA with respect to the affected Processing, and Customer shall pay to Aqua all the amounts owed to Aqua or due before the date of termination. Customer will have no further claims against Aqua (including, without limitation, requesting refunds for Services) pursuant to the termination of the Agreement and the DPA as described in this paragraph.
15. **Authorized Affiliates**
  - 14.1 The Parties acknowledge and agree that, by executing the DPA, Customer enters into the DPA on behalf of itself and, as applicable, in the name and on behalf of its Authorized Affiliates, in which case each Authorized Affiliate agrees to be bound by Customer's obligations under this DPA, if and to the extent that Aqua processes Customer Personal Data on the behalf of such Authorized Affiliates, thus qualifying them as the "Controller". All access to and use of the Services by Authorized Affiliates must comply with the terms and conditions of the Agreement and this DPA and any violation of the terms and conditions therein by an Authorized Affiliate shall be deemed a violation by Customer.
  - 14.2 Customer shall remain responsible for coordinating all communication with Aqua under the Agreement and this DPA and shall be entitled to make and receive any communication

in relation to this DPA on behalf of its Authorized Affiliates.

16. **Indemnity.** Aqua shall indemnify and hold Customer harmless against all claims, actions, third party claims, losses, damages and expenses incurred by the Customer and arising directly out of or in connection with a breach of this DPA and/or the Applicable Law by Aqua, all subject to and in accordance with the indemnity provisions set forth in the Services Agreement.

17. **General Terms**

17.1. **Termination.** This DPA shall terminate automatically upon the termination of the Agreement, provided however, that Aqua's obligations under this DPA will apply for as long as Aqua has access to Customer Personal Data.

17.2. **Governing Law and Jurisdiction**

17.2.1. The parties to this DPA hereby submit to the choice of jurisdiction stipulated in the Agreement with respect to any disputes or claims howsoever arising under this DPA, including disputes regarding its existence, validity or termination or the consequences of its nullity.

17.2.2. This DPA 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 Agreement.

17.3. **Order of Precedence**

17.3.1. Nothing in this DPA shall detract from Aqua's obligations under the Agreement in relation to the protection of Customer Personal Data or permit Aqua to process (or permit the processing of) Customer Personal Data in a manner that is prohibited by the Agreement.

17.3.2. Subject to this Section 16.3, in the event of inconsistency between the provisions of this DPA and any other agreements between the parties, including the Agreement and (except where explicitly agreed otherwise in writing) agreements entered into or purported to be entered into after the date of this DPA, with regard to the subject matter of this DPA, the provisions of this DPA shall prevail. In the event of inconsistencies between the provisions of this DPA and the Standard Clauses (to the extent they apply), the Standard Clauses shall prevail.

17.4. **Changes in Applicable Law**

17.4.1. Each Party may, by at least forty-five (45) days prior written notice to the other Party, request in writing any variations to this DPA if they are required as a result of any change in, or decision of a competent authority under any Applicable Law in order to allow Customer Personal Data to be processed (or continue to be processed) without breach of that Applicable Law.

17.4.2. If a Party gives notice with respect to its request to modify this DPA under Section 16.4.1, the Parties shall make commercially reasonable efforts to accommodate such modification request. 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 or Aqua's notice as soon as is reasonably practicable.

17.4.3. In the event that the Parties are unable to accommodate such request within 30 days, then the Customer or Aqua may, by written notice to the other Party, with immediate effect and without any penalty, terminate the Agreement to the extent that it relates to the Services that are affected by the proposed variations (or lack thereof). Customer will have no further claims against Aqua (including, without limitation, requesting refunds for the Services) pursuant to the termination of the

Agreement and the DPA as described in this Section.

- 17.5. **Severance.** Should any provision of this DPA be held invalid or unenforceable, the remainder of this DPA shall remain valid and in force. The invalid or unenforceable provision shall either be (i) amended as necessary to ensure its validity and enforceability, while preserving the parties' intentions as closely as possible or, if this is not possible, (ii) construed in a manner as if the invalid or unenforceable part had never been contained herein.

### **Schedule A: Details of Processing of Customer Personal Data**

This **Schedule A** includes certain details of the Processing of Customer Personal Data as required by Article 28(3) of the GDPR.

#### **Subject matter and duration of the Processing of Customer Personal Data.**

The subject matter and duration of the Processing of the Customer Personal Data are set out in the Agreement.

#### **The nature and purpose of the Processing of Customer Personal Data:**

1. Providing the Services to Customer;
2. Performing the Agreement, this DPA and/or other contracts executed by the Parties;
3. Acting upon Customer's instructions, where such instructions are consistent with the terms of the Agreement;
4. Complying with applicable laws and regulations;
5. All tasks related with any of the above.

#### **The types of Customer Personal Data to be Processed are as follows:**

Details of users of the Services, including email address, username and IP address.

#### **The categories of Data Subject to whom the Customer Personal Data relates to are as follows:**

Customer's employees or subcontractors authorized by Customer to use the Services as detailed in the Agreement.

#### **Sub-Processors List:**

<https://www.aquasec.com/trust/sub-processors/>

**Schedule B: Binding Security Document**

1. Physical security.
2. Logical security.
3. Separation of databases.
4. Policy regarding the removal of magnetic and optical data (including hard drives, portable storage media, backup platforms, etc.).
5. Procedures regarding database management.
6. Provisions regarding the collection, marking, verification, processing, and distribution of the data.
7. Management of access to personnel, including determination of the methodology for providing access to data, restrictions upon access, and keeping an updated list of persons with access rights.
8. Confidentiality undertakings for those persons with access rights.
9. Pseudonymisation and encryption of personal data.
10. Provisions regarding operations of the systems and maintaining ongoing data integrity, confidentiality, availability and resilience of processing systems and services.
11. Monitoring for the discovery of breaches of data integrity and methodology for reparation of such breaches.
12. Provisions regarding employee reliability and record of data misuse in accordance with the level of data sensitivity.
13. Restoration of access to personal data in a timely manner in the event of a physical or technical incident.
14. Process for regularly testing, assessing, and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing of Customer Personal Data.
15. Measures to identify vulnerabilities with regard to the processing of Customer Personal Data.

## **Schedule C: Cross Border Transfers**

### **PART 1 – EEA Transfers**

1. The parties agree that the terms of the Standard Clauses are hereby incorporated by reference and shall apply to an EEA Transfer.
2. Module Two (Controller to Processor) of the Standard Clauses shall apply where the EEA Transfer is effectuated by Customer as the data controller of the Client Personal Data and Aqua is the data processor of the Customer Personal Data.
3. Clause 7 of the Standard Clauses (Docking Clause) shall not apply.
4. Option 2: GENERAL WRITTEN AUTHORISATION in Clause 9 of the Standard Clauses shall apply, and the method for appointing and time period for prior notice of Sub Processor changes shall be as set forth in Section 8 of the DPA.
5. In Clause 11 of the Standard Clauses, the optional language will not apply.
6. In Clause 17 of the Standard Clauses, Option 1 shall apply, and the Parties agree that the Standard Clauses shall be governed by the laws of the Republic of Ireland.
7. In Clause 18(b) of the Standard Clauses, disputes will be resolved before the courts of the Republic of Ireland.
8. Annex I.A of the Standard Clauses shall be completed as follows:
  - Data Exporter: Customer.
  - Contact details: As detailed in the Agreement.
  - Data Exporter Role: The Data Exporter is a data controller.
  - Signature and Date: By entering into the Agreement and DPA, Data Exporter is deemed to have signed these Standard Clauses incorporated herein, including their Annexes, as of the Effective Date of the Agreement.
  - Data Importer: Aqua
  - Contact details: As detailed in the Agreement.
  - Data Importer Role: The Data Importer is a data processor.
  - Signature and Date: By entering into the Agreement and DPA, Data Importer is deemed to have signed these Standard Clauses, incorporated herein, including their Annexes, as of the Effective Date of the Agreement.
9. Annex I.B of the Standard Clauses shall be completed as follows:
  - The categories of data subjects are described in **Schedule A** (Details of Processing) of this DPA.
  - The categories of personal data are described in **Schedule A** (Details of Processing) of this DPA.
  - The frequency of the transfer is a continuous basis for the duration of the Agreement.
  - The nature of the processing is described in **Schedule A** (Details of Processing) of this DPA.
  - The purpose of the processing is described in **Schedule A** (Details of Processing) of this DPA.
  - The period for which the personal data will be retained is for the duration of the Agreement, unless agreed otherwise in the Agreement and/or the DPA.

In relation to transfers to Sub-processors, the subject matter, nature, and duration of the processing is set forth in **Schedule A** (Details of Processing) of this DPA.

10. Annex I.C of the Standard Clauses shall be completed as follows:

The competent supervisory authority in accordance with Clause 13 is the supervisory authority in the Member State stipulated in Section 7 above.

11. Schedule B referred to in the DPA serves as Annex II of the Standard Clauses.

12. To the extent there is any conflict between the Standard Clauses and any other terms in this DPA or the Agreement, the provisions of the Standard Clauses will prevail.

## **PART 2 – UK Transfers**

The Parties agree that the International Data Transfer Addendum to the EU Commission Standard Clauses is hereby incorporated by reference and shall apply to UK Transfers as set forth in this Part 2.

### 1. Part 1: Tables

**Table 1: The Parties:** as stipulated in Section 8 of Part 1 of this **Schedule C**.

**Table 2: Selected SCCs, Modules and Selected Clauses:** as stipulated in Part 1 of this **Schedule C**.

**Table 3: Appendix Information:** means the information which must be provided for the selected modules as set out in the Appendix of the Standard Clauses (other than the Parties), and which for this Part 2 is set out in Part 1 to this **Schedule C**.

### 2. Part 2: Mandatory Clauses

Mandatory Clauses of the Approved Addendum, being the template Addendum B.1.0 issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18 of those Mandatory Clauses.

## **PART 3 - Swiss Cross Border Transfers**

The Parties agree that the Standard Clauses as detailed in Part 1 of this **Schedule C**, shall be adjusted as set out below where the FADP applies to Switzerland Transfers:

1. References to the Standard Clauses mean the Standard Clauses as amended by this Part 3;
2. The Swiss Federal Data Protection and Information Commissioner shall be the sole Supervisory Authority for Swiss Transfers exclusively subject to the FADP;
3. The terms “General Data Protection Regulation” or “Regulation (EU) 2016/679” as utilized in the Standard Clauses shall be interpreted to include the FADP with respect to Swiss Transfers;
4. References to Regulation (EU) 2018/1725 are removed;
5. Swiss Transfers subject to both the FADP and the GDPR, shall be dealt with by the EU Supervisory Authority named in Part 1 of this Schedule C;
6. References to the “Union”, “EU” and “EU Member State” shall not be interpreted in such a way as to exclude Data Subjects in Switzerland from the possibility of exercising their rights in their place of habitual residence (Switzerland) in accordance with Clause 18(c) of the Standard Clauses;
7. Where Swiss Transfers are exclusively subject to the FADP, all references to the GDPR in the Standard Clauses are to be understood to be references to the FADP;

8. Where Swiss Transfers are subject to both the FADP and the GDPR, all references to the GDPR in the Standard Clauses are to be understood to be references to the FADP insofar as the Swiss Transfers are subject to the FADP;

**PART 4 – Additional Safeguards**

1. In the event of an EEA Transfer, UK or Switzerland Transfer, the Parties agree to supplement these with the following safeguards and representations, where appropriate:
  - a. The Processor shall have in place and maintain in accordance with good industry practice measures to protect the Customer Personal Data from interception.
  - b. The Processor will make commercially reasonable efforts to resist, subject to applicable laws, any request for bulk surveillance relating to the Customer Personal Data protected under GDPR, the UK GDPR, or the FADP, including under section 702 of the United States Foreign Intelligence Surveillance Act (“FISA”);
  - c. If the Processor becomes aware that any government authority (including law enforcement) wishes to obtain access to or a copy of some or all of the Customer Personal Data, whether on a voluntary or a mandatory basis, then unless legally prohibited or under a mandatory legal compulsion that requires otherwise:
    - I. The Processor shall inform the relevant government authority that the Processor is a processor of the Customer Personal Data and that the Controller has not authorized the Controller Processor to disclose the Customer Personal Data to the government authority, and inform the relevant government authority that any and all requests or demands for access to the Customer Personal Data should therefore be notified to or served upon the Controller in writing;
    - II. The Processor will use commercially reasonable legal mechanisms to challenge any such demand for access to Customer Personal Data which is under the Processor’s control. Notwithstanding the above, (a) the Controller acknowledges that such challenge may not always be reasonable or possible in light of the nature, scope, context and purposes of the intended government authority access, and (b) if, taking into account the nature, scope, context and purposes of the intended government authority access to Customer Personal Data, the Processor has a reasonable and good-faith belief that urgent access is necessary to prevent an imminent risk of serious harm to any individual or entity, this subsection (c)(II) shall not apply. In such event, the Processor shall notify the Controller, as soon as possible, following the access by the government authority and provide the Controller with all relevant details of the same, unless and to the extent legally prohibited to do so.
2. Once in every 12-month period, the Processor will inform the Controller, at the Controller’s written request, of the types of binding legal demands for Customer Personal Data it has received and solely to the extent such demands have been received, including national security orders and directives, which shall encompass any process issued under section 702 of FISA.