Akvo Foundation
's-Gravenhekje 1A | 1011 TG Amsterdam | The Netherlands
+31 20 820 0175 | info@akvo.org | Akvo.org

The Akvo Foundation

Data Processing Agreement

March 2020

Akvo Foundation
's-Gravenhekje 1A | 1011 TG Amsterdam | The Netherlands
+31 20 820 0175 | info@akvo.org | Akvo.org

Document Control; Version History v.4

Version	Status	Reason for change	Changes done by
1	Draft, March 2018		Lynn Brannstrom
2	Draft, 26 April 2018	Discussion with Hans & Lars	Lynn Brannstrom
2.1	Draft, 17 May 2018	Updates made for final version prep	Lynn Brannstrom
3	Final, 22 May 2018	Liability updated	Lynn Brannstrom
3.1	Final, 12 June 2018	Adjustments made according to Deltares requests as well as fixing clause 4.2 to reference clause 5 instead of 6	Lynn Brannstrom
4.0	Draft, 26 February 2020	Setting up a Framework Agreement with Welthungerhilfe	Hans Merton
5.0	Final, 12 March 2020	Cleaned (last mark-ups and comments removed)	Hans Merton

This Agreement is entered into between the Akvo Foundation and

……

on the 1st of January 2020 (the "Commencement Date")

PARTIES

(1) **……**, incorporated and registered in ….. with **……. registration number …….** and having its registered office at **……** ("**Controller**");

(2) **The Akvo Foundation**, incorporated and registered in The Netherlands, with **Chamber of Commerce registration number in The Hague (KvK): 27327087 and Value Added Tax number (VAT/BTW): NL819794727B01** and having its registered office at **'s-Gravenhekje 1A1011 TG, Amsterdam, ("Processor")**

Each individually referred to as the "**Party**" and jointly referred to as the "**Parties**".

RECITALS

A. **WHEREAS** the Parties have agreed that the Controller will act as the sole Controller of the Personal Data and the Processor renounces to any rights it may have to act as a data controller of the Personal Data held by the Controller;

B. **WHEREAS** the Parties have agreed that it may be necessary for the Processor to Process certain Personal Data on behalf of the Controller;

C. **WHEREAS** in light of this Processing, the Parties have agreed to enter into this Agreement to address the compliance obligations imposed upon the Controller pursuant to the Applicable Law;

D. **WHEREAS** the Parties agree that the provision of the services under the Akvo Foundation's (General Terms of Service and SaaS Terms of Service) qualify as commissioned data Processing as per Art. 28 of the General Data Protection Regulation 2016/679; and

E. **WHEREAS** the Parties agree that this Agreement shall render any and all other previous agreements entered into between the Controller and the Processor in relation to data protection, before the date of this Agreement null and void and replace such previous agreement.

1. DEFINITIONS AND INTERPRETATION

1.1. The following terms shall have the following meanings:

Agreement:	means this Agreement, including all schedules, notifications and all notices to this Agreement;
Applicable Law:	means the relevant data protection and privacy laws to which the Parties are subject, including the General Data Protection Regulation 2016/679
Data Subject:	means the identified or identifiable person to whom Personal Data relates;
Personal Data:	means "*any information relating to an identified or identifiable natural person (data subject); an identifiable person is one who can be identified, directly or indirectly, in particular by reference identifier such as a name, an identification number, location data, an online identifier or the one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person*", as defined under the General Data Protection Regulation 2016/679 and includes any equivalent definition in the Applicable Law;
Process, Processing or Processed:	means "*any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction*", as defined under the General Data Protection Regulation 2016/679 and includes any equivalent definition in the Applicable Law;
Service Objectives:	means the Services and the associated Processing of Personal Data as defined in Schedule 1 to this Agreement;

Services:	means the specific SaaS Services rendered by Akvo under the ……. Agreement.
Service Agreement:	means the Akvo – …….. agreement (dated ……..) between the Controller as the user and the Processor, that governs the Controller's limited, non-exclusive and terminable right to the use of Akvo Products and Services as defined in the Terms of Service.
Security Breach	means a personal data breach as defined in Art 4 (12) GDPR Definitions

2. APPOINTMENT

2.1. The Processor is appointed by the Controller to Process such Personal Data for and on behalf of the Controller as is necessary to provide the Processing. Any subsequent agreement on the Processing shall be subject to the provisions of this Agreement.

2.2. The Processor shall Process Personal Data in accordance with the requirements of the Applicable Laws. For the avoidance of doubt, the Controller's instructions for the Processing of Personal Data shall comply with the Applicable Law and the Processor reserves the right to refuse such instructions if not in compliance with the Applicable Law. The Controller shall have sole responsibility for the accuracy, quality, and legality of Personal Data and the means by which it acquires the Personal Data.

3. DURATION

3.1. This Agreement shall commence on the Commencement Date and shall continue in full force and effect until the completion of the Service Objectives as defined in Schedule 1 or termination of the Service Agreement.

3.2. Notwithstanding Clause 3.1 and in those instances where the Service Objectives consists of a number of Processing activities, the Parties may agree to terminate part of the Processing activities forming part of the Service Objectives, in which case such termination shall take effect on the date agreed by the Parties in writing and shall not affect the validity

of the remaining Processing activities forming part of the same Service Objectives.

4. DATA PROCESSING

4.1. The Processor shall process Personal Data for the Service Objectives as described in the Service Agreement, as entered into between the Parties, on behalf of and under the direction of the Controller and as summarized in Schedule 1 hereunder.

4.2. Personal Data will be, where possible, processed within a Member State of the European Union (EU) or within a Member State of the European Economic Area (EEA). When transferring Personal Data to countries outside the EU/EEA Processor (a) will not do so without the Controller's prior written consent, and (b) warrants that Processing takes place within the restrictions and in compliance with the technical and organizational measures set out in clause 5 and in compliance with Applicable Laws.

4.3. Depending on how the Controller chooses to use the Service, the subject matter of Processing of Personal Data may cover the following types/categories of data:

- *Internal*: knowledge & belief, authenticating, preference.
- *Historical*: Life history.
- *External:* Identifying (name, username, ID card), ethnicity, sexual, behavioural, demographic, medical & health, physical characteristics.
- *Financial*: Account, ownership, transactional, credit.
- *Social*: Professional (salary, job title), criminal, public life, family, social network, communication.
- *Tracking*: Computer device (mac address, ip address, android IMEI), contact (email address, telephone number), location (GPS coordinates, country)

4.4. Data Subjects affected by the Processing of their Personal Data under this Agreement includes end-users of the Controller's websites which make use of the Services provided by the Processor, as well as the Controller's beneficiaries whose data, including Personal Data, is collected with Services provided by the Processor.

5. TECHNICAL AND ORGANIZATIONAL MEASURES

5.1. The Processor will establish data security in accordance with the Applicable Laws. The measures to be taken must guarantee a

protection level appropriate to the risk concerning confidentiality, integrity, availability and resilience of the systems. The state of the art, implementation costs, the nature, scope and purposes of Processing, as well as the probability of occurrence and the severity of the risk to the rights and freedoms of natural persons, must be taken into account.

5.2. The Processor has laid down the technical and organizational measures in Schedule 2 of this Agreement.

5.3. The technical and organisational measures are subject to technical progress and further development. In this respect, it is permissible for the Processor to implement alternative adequate measures. In so doing, the security level of the defined measures must not be reduced. Whenever the Processor will adjust the technical and organisational measures the Processor will update Schedule 2 accordingly without undue delay and inform the Controller about the content and reason of such update.

6. RECTIFICATION, RESTRICTION AND ERASURE OF DATA

6.1. The Processor may not on its own authority rectify, erase or restrict the Processing of Personal Data that is being processed on behalf of the Controller (unless this is required by law or Akvo's General Terms of Service and SaaS Terms of Service in which case the Controller will be notified in writing upfront), but shall only do so on documented instructions from the Controller and in accordance to data retention rules associated to the Service Agreement between Controller and Processor .

6.2. If a Data Subject should apply directly to the Processor to request the rectification, erasure, or restriction of his Personal Data, the Processor must forward this request to the Controller without delay.

7. QUALITY ASSURANCE AND OTHER OBLIGATIONS OF THE PROCESSOR

7.1. When performing the Services and this Agreement the Processor will always comply all Applicable Law. In particular, the Processor ensures compliance with the following requirements:

a. The Processor has appointed a Data Protection Officer according to Article 39 GDPR who shall perform duties in compliance with Applicable Laws. The Data Protection Officer can be contacted via e-mail on privacy@akvo.org.

b. The Processor shall keep Personal Data Processed on behalf of the Controller logically separate from Personal Data Processed on behalf of any other third party;

c. The Processor and any person acting under its authority shall process the Personal Data in accordance with the Processor's Term of Service and on documented instructions from the Controller, including with regard to transfers of Personal Data to a third country or international organisation, unless required to do so by Union or Member State law to which the Processor is subject; in such a case, the Processor shall inform the Controller of that legal requirement before Processing, unless that law prohibits such information on important grounds of public interest; in the latter case, Processor will inform Controller comprehensively, transparently and without undue delay about the legal reasons prohibiting earlier information;

d. The Processor entrusts only such persons (whether legal or natural) with the data Processing under this Agreement who have given an undertaking to maintain confidentiality and have been informed of any special data protection requirements relevant to their work;

   The processor shall at the request of the data controller demonstrate that the concerned persons under the data processor's authority are subject to the abovementioned confidentiality.

e. The Processor and the Controller shall cooperate, upon written request, with any competent supervisory authority in the performance of its legitimate tasks;

f. The Processor shall inform the Controller immediately of any inspections and measures conducted by any supervisory authority, insofar as they relate to the Processing of data on behalf of the Controller under this Agreement or the Service Agreement; this also applies if the Processor is under investigation or is party of an investigation by a competent authority in connection with the Processing of data on behalf of the Controller under this Agreement or the Service Agreement;

g. The Processor will undertake reasonable best efforts to support the Controller if the Controller is subject to an inspection by any supervisory authority, an administrative or summary offence or criminal procedure, a liability claim by a Data Subject or by a third party or any other claim in connection with this Agreement.

8. MONITORING RIGHTS OF THE CONTROLLER

8.1. The Controller has the right, after consultation with the Processor, to carry out inspections or to have them carried out by an auditor. The Controller has the right to convince itself of the compliance with this Agreement by the Processor in its business operations by means of random checks, which are to be announced in advance with good time. These rights of the Controller shall not extend to facilities which are operated by sub-processors, sub-contractors or any third parties which the Processor may use to attain the Service Objectives and provide its Services. The Processor shall ensure and proof to the reasonable satisfaction of the Controller that the processing activities carried out by any sub-processors, or sub-contractors which the Processor may use to attain the Service Objectives and to provide its Services meet the requirements laid down in this Agreement and in Applicable Law.

8.2. The Processor shall ensure that the Controller is able to verify compliance with the obligations of the Processor in accordance with the Applicable Laws. The Processor undertakes to provide to the Controller all necessary information on request and, in particular, to demonstrate the execution of the technical and organisational measures as mentioned in Schedule 2 within a reasonable timeframe.

8.3. Evidence of the implementation of any measures in this regard may also be presented in the form of up-to-date certificates, reports or extracts thereof from independent bodies (e.g. external auditors, internal audit, the data protection officer, the IT security or data protection audit or by measures provided by Applicable Law).

9. NOTIFICATION OF SECURITY BREACHES BY THE PROCESSOR

9.1. The Processor shall assist the Controller in complying with the statutory obligations regarding the security and protection of personal data and shall make appropriate documentation in this regard. This includes, in particular, the obligation:

a. To ensure an appropriate level of protection through technical and organisational measures that take into account the circumstances and purposes of the Processing as well as the projected probability and severity of a possible infringement of the Applicable Law as a result of security vulnerabilities and that enable an immediate detection of relevant infringement events;

b. To notify the Controller in the most expedient time possible under the circumstances and without unreasonable delay and, where feasible, not later than seventy-two (48) hours after having become aware of any

accidental, unauthorised, or unlawful destruction, loss, alteration, or disclosure of, or access to, Personal Data ("Security Breach"). In consultation with the Controller, the Processor shall take without undue delay all appropriate measures to secure the data and limit any possible detrimental effect on the Data Subjects;

c. To co-operate with the Controller and provide the Controller with any and all information which the Controller may reasonably request relating to the Security Breach. The Data Processor will assist the Data Controller in obtaining the information required for the Controller to notify the competent supervisory authority as listed below:

   - The nature of the personal data including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
   - The likely consequences of the personal data breach;
   - the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

d. The Processor shall investigate the Security Breach and shall identify, prevent and make reasonable efforts to mitigate the effects of any such Security Breach and, with the Controller's prior agreement, to carry out any recovery or other action necessary to remedy the Security Breach;

e. To assist the Controller by appropriate measures with regard to the Controller's obligation to inform Data Subjects and competent authorities in case of a Security Breach; and

f. To assist the Controller with regard to the Controller's obligation to provide information to the Data Subject concerned and to immediately provide the Controller with all relevant information in this regard.

10. AUTHORITY OF THE CONTROLLER TO ISSUE INSTRUCTIONS

10.1. The Personal Data may only be handled under the terms of this Agreement, in alignment with the Processor's General Terms of Service and SaaS Terms of Service, and under the instructions issued by the Controller. Under the terms of this Agreement, the Controller retains a general right of instruction as to the nature, scope and method of data Processing, which may be supplemented with individual instructions. Any changes to the subject-matter (legitimate purpose" pursuant to Art. 5 Sect. 1 lit (b) GDPR) of the Processing and any

changes to procedure must be agreed and documented together. The Processor may only pass on information to third parties or to the Data Subject with the prior written consent of the Controller.

10.2. The Processor will only accept instructions via electronically communicated text in writing or in text form. The Processor must not use the data for any other purpose and is particularly forbidden to disclose the data to third parties. No copies or duplicates may be produced without the prior written and informed consent of the Controller. This does not apply to backup copies or troubleshooting where these are required to assure proper data Processing as part of adequate technical and organisational measures, or to any data required to comply with statutory retention rules.

10.3. The Processor shall inform the Controller without delay, if it believes that the Controller's instruction infringes Applicable Law or might cause the Processing to infringe Applicable Law. The Processor may then postpone the execution of the relevant instruction until its compliance with Applicable Law is confirmed or the relevant instruction is changed by the Controller's representative in compliance with Applicable Law.

11. DELETION AND RETURN OF DOCUMENTS, INFORMATION, AND PERSONAL DATA

11.1. Upon completion of the contractual work as laid down in the Service Agreement or when requested by the Controller, and within a reasonable time which shall not exceed 30 calendar days, the Processor must return to the Controller all Personal Data and documents in its possession and all work products and data produced, or – if requested by the Controller - delete them in compliance with the Applicable Law. The same applies to any test data. The deletion log must be presented upon request.

11.2. Electronic documentation intended as proof of proper Processing of Personal Data must be kept by the Processor beyond the termination of this Agreement, in accordance with relevant retention periods relevant to the Service Agreement and timeframes corresponding therein. The Processor shall hand such documentation over to the Controller after expiry of the Agreement, upon request by the Controller.

11.3. The Processor shall promptly notify the Controller in line with Section 6.2 of this Agreement if the Processor receives a request from a Data Subject to exercise the Data Subject's right of access, right to rectification, restriction of Processing, erasure ("right to be forgotten"), data portability, object to the Processing, or its right not to be subject to an automated individual decision making. The

Processor must assist the Controller in allowing Data Subjects to exercise their rights under the Applicable Law.

11.4. Taking into account the nature of the Processing, the Processor shall assist Controller by appropriate technical and organisational measures, insofar as the right to be forgotten is possible, for the fulfilment of the Controller's obligation to respond to a Data Subject's request under Applicable Law. The obligation to decide upon the deletion of the Data Subject's Personal Data shall, at all times, remain with the Controller. For the avoidance of doubt, the Processor will not undertake any efforts to delete Personal Data for and on behalf of the Controller without the Controller's prior written permission.

12. INDEMNIFICATION

12.1. The Controller will indemnify and keep indemnified the Processor in respect of all liabilities, costs and expenses suffered or incurred by the Processor in its capacity as Processor of the Personal Data of the Controller arising from any Security Breach as a result of any grossly negligent act or omission by the Controller in the exercise of its obligations under the Applicable Law provided that:

a. The Processor, within reasonable time, notifies the Controller of any actions, claims or demands brought or made against it concerning any alleged Security Breach;

b. The Processor will not compound, settle or admit to any actions, claims or demands without the consent of the Controller except by order of a court of competent jurisdiction;

c. The Controller shall be entitled at its own cost to defend or settle any proceedings;

d. The Processor shall not have acted of its own accord and independently of the instructions given to it by the Controller in its role as data Processor in accordance with the provisions of this Agreement, except in specific situations as laid down in the Processor's General Terms of Service and SaaS Terms of Service;

e. This indemnity shall be capped at a level of ……euros per year with a maximum of …….euros per individual claim and shall exclude any loss that has arisen out of negligence or wilful act, default or omission of the Processor, its employees, contractors, sub-contractors or any other person outside the Controller's control. The financial indemnity cap shall

not apply in the event of death or personal injury, where there shall be no limit.

f. Nothing in this Agreement shall restrict or interfere with the Controller's rights against the Processor or any other person in respect of contributory negligence.

The Processor's right to claim damages shall be forfeited if the Processor fails to give written notice of any damages that may be sustained as aforesaid within ten (10) days from the occurrence thereof or commences to make good such damages before written notice is given as aforesaid.

12.2. The Processor shall indemnify and keep indemnified the Controller in respect of all and any claims, legal proceedings or actions brought against the Controller exclusively arising as a result of the negligence or wilful default of the Processor in Processing Personal Data in terms of this Agreement. The indemnity referred to shall apply subject to the following:

a. The Controller, within reasonable time, notifies the Processor of any actions, claims or demands brought or made against it concerning any alleged Security Breach;

b. The Processor shall be entitled at its own cost to defend or settle any proceedings;

c. This indemnity shall be capped at a level of ….. euros per year with a maximum of ……euros per individual claim whether in a single claim or a series of claims arising from the same event and shall exclude any loss that has arisen out of negligence or wilful act, default or omission of the Processor, its employees, contractors, sub-contractors or any other person outside the Controller's control. The financial indemnity cap shall not apply in the event of death or personal injury, where there shall be no limit;

d. Nothing in this Agreement shall restrict or interfere with the Controller's rights against the Processor or any other person in respect of contributory negligence.

13. SUB-PROCESSING

13.1. "**Sub-Processing**", in the meaning of this Agreement, means cloud services provided by various third-party processors, for software execution, data storage, data retention and processing. Sub-processing does not include

ancillary services, such as telecommunication services, postal / transport services, maintenance and user support services or the disposal of data carriers, as well as other measures to ensure the confidentiality, availability, integrity and resilience of the hardware and software of that Processing equipment. The Processor shall, however, be obliged to make appropriate and legally binding contractual arrangements and take appropriate inspection measures to ensure the data protection and the data security of the Controller's data in the case of any outsourced ancillary services, including, if outsourced to Sub-Processors. The Akvo Foundation's sub-processors are listed here: https://akvo.org/help/third-parties/

13.2. The Controller agrees to the commissioning of sub-processors on the condition of a contractual agreement in accordance with Applicable Laws. For a list of current Sub-Processors go to: https://akvo.org/help/third-parties/
Processor will always inform Controller in writing prior to contracting a new or deleting an existing Sub-Processor as far as relevant for the services delivered under the Services Agreement.

13.3. Outsourcing to further Sub-Processors or changing any existing Sub-Processors is permissible if the Processor ensures compliance of such Sub-Processor, to Applicable Laws. In addition, the following provisions apply:

a. The transfer of Personal Data to the Sub-Processor and the Sub-Processor's commencement of the data Processing shall only be undertaken after compliance with all requirements has been achieved;

b. If the Sub-Processor provides the agreed service outside the EU/EEA, the Processor shall ensure compliance with Applicable Laws; and

c. The Processor shall impose on the Sub-Processor at least the same data protection obligations as set out in this Agreement, in particular with regard to the provision of sufficient guarantees to implement appropriate technical and organisational measures in such manner that the Processing will meet the requirements of the Applicable Law.

13.4. With respect to each Sub-Processor, the Processor will before the Sub-Processor first Processes any data of the Controller, carry out adequate due diligence to ensure that the Sub-Processor is capable of providing the level of protection for the Personal Data required by this Agreement and shall ensure that the agreement between the Processor and the relevant Sub-Processor, is governed by a written contract including terms which offer at least the same level of protection for the Controller as those set out in this Agreement and meets the requirements of article 28(3) of the GDPR.

14. MISCELLANEOUS

14.1. The Processor shall provide the Controller with reasonable cooperation and assistance needed to fulfil the Controller's obligation under the General Data Protection Regulation to carry out a data protection impact assessment related to the Controller's use of the Processor Services, to the extent that the Controller does not otherwise have access to the relevant information, and to the extent such information is available to the Processor.

14.2. If any variation is required to this Agreement as a result of a change in the Applicable Law, the Parties promptly inform each other and will discuss and negotiate in good faith any necessary variations to this Agreement with a view to agreeing and implementing those or alternative variations designed to address the relevant requirements.

14.3. Headings used in this Agreement are for convenience of reference only and shall not affect the meaning or interpretation of this Agreement. Schedules to this Agreement shall be deemed to be set forth *verbatim* herein and are an integral and inseparable part of this Agreement.

14.4. This Agreement, including the Schedules attached hereto constitute the entire agreement between the Parties pertaining to the subject matter hereof and supersede all prior agreements (excluding the Service Agreement, understandings, negotiations and discussions of the Parties.

14.5. The provisions of this Agreement are severable. Should a provision of this Agreement or a provision later on included in this Agreement be or become null and void as a whole or in part, or should a gap in this Agreement become evident, this does not affect the validity of the remaining provisions. It is the express intention of the Parties to maintain the validity of the remaining provisions at all events as a whole. Instead of the null and void provision, or in order to fill the gap, such valid and practicable regulation is deemed to be agreed with effect from the beginning that in legal and economic terms comes closest to what the Parties intended or would have intended in accordance with the purpose of this Agreement if they had considered the point at the time of conclusion of this Agreement.

14.6. Any notice, letter or other communication contemplated by this Agreement shall be communicated in writing via registered mail to the registered addresses of the Parties or, unless for informing the other Party about a default, claim, or similar, also via electronic mail.

14.7. The provisions of this Agreement shall endure to the benefit of and shall be binding upon the Parties and their respective successors and assigns.

14.8. This Agreement may be executed in counterparts, each of which shall be deemed an original, but all of which together shall constitute one and the same instrument.

AS WITNESS the hands of the duly authorised representatives of the Parties the day month and year first above written:

SIGNED on behalf of	Signature:……..……
…….	Name: …….
	Position: ……..
SIGNED on behalf of	Signature:……..……
The Akvo Foundation	Name:……..……
	Position:……..……

SCHEDULE 1

General Description of Processing Operations

The Akvo Foundation offers various tools as SaaS (Software as a Service) to partners. The tools include, but are not limited to, mobile survey data collection, project reporting, data visualisation, sensor hardware and website creation. The Akvo Foundation gives its partners the big picture by connecting all phases of their projects from collection of data, understanding their data, making informed decisions and sharing their data with the world.

For more information on what data is collected and the security measure taken to protect this data refer to the Akvo Foundation's Terms of Service and Privacy Policy.

SCHEDULE 2

Technical and Organizational Measures

The Processor warrants and undertakes in respect of all Personal Data that it Processes on behalf of the Controller that, at all times, it maintains and shall continue to maintain appropriate and sufficient technical and organisational security measures to protect such Personal Data or information against accidental or unlawful destruction or accidental loss, damage, alteration, unauthorized disclosure or access, in particular where the Processing involves the transmission of data over a network, and against all other unlawful forms of Processing.

Such measures shall include, but are not limited to, physical access control, logical access control (i.e. non-physical access control measures such as passwords), data access control, data transfer control, input control, availability measures, and data separation; in particular at least the measures set out in the Akvo Foundation's Privacy Policy.

The Processor shall provide the Controller, upon request, with adequate proof of compliance (e.g. the relevant parts of the Processor's agreements with its subcontractors).

For more detailed information on the latest state of the art measures adopted by our hosting providers, please refer to the following links:

Google https://cloud.google.com/security/
Amazon https://aws.amazon.com/security/
Elephant SQL https://www.elephantsql.com/security_policy.html

The Processor refers to https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/security/ for an overview of what TOM's should include.

Processors system documentation regarding our data protection strategy

On akvo.org, one can find Akvo's policies, terms of service and Data Processing Agreement. All Flow and Lumen documentation is available on Akvo's support pages. For example you can find an article on how we ensure data security or another one on how we handle your personal data. Akvo's software code is fully open source and documented on our GitHub pages.

Overview implemented GDPR compliance measures regarding Akvo Flow

Besides a number of changes in Akvo's tools as described below, also in Akvo's support model a number of changes have been implemented. About Akvo Flow, only a limited number of Akvo support staff members have access to partner instances in order to be able to deliver support. In all cases: it is the Partner's responsibility to make any changes in user admin roles within Flow. Without prior authorisation by the partner, Akvo staff is not allowed to do so.

To ensure how Akvo handles personal user data in Flow and Lumen follows GDPR and to ensure we handle partners' data (personal and captured data) in compliance with GDPR, Akvo has implemented the following changes:

- Ensured data is safely stored for all Flow's databases and backups (including changes to data exports, how we store photos and videos) in EU locations
- Introduced a new data export page, making it possible to download data directly from Flow rather than via emails.
- Ensured data access always respects user roles and permissions in Flow, in all its functionality. Akvo fixed all known issues causing inconsistencies in respecting user roles and permissions, ensured Maps also follow the setup (by allowing to filter data out by folder, survey, form) and improved how you see who has user admin rights in the user list.
- Ensured data is not available via visualizations due to how Akvo does aggregations in Lumen. Akvo also added password protection to shared dashboards.
- Changed how data is stored in the Flow app by moving everything to a private folder. This change affected the bulk uploading of data offline functionality and introduced a 90 minutes publishing window to allow for bulk upload.
- Redesigned how we geotag photos on the Flow app. Before Flow app always tried to capture the device location when a photo was taken, regardless of the user's settings. From now on, the Flow app respects if a user did not allow geotagging of photos on her device and only read the geotag provided by the camera app.
- Stopped saving all the devices and only store those last connected to Flow in the last 12 months, in line with the 'only store what you need' principle.
- Moved away from restricting users to access Flow only with Google emails to being able to use any email. This is not affecting our GDPR compliance but will simplify user management and bring more control to organizations. This login change will mean that any organisation can change all their existing user accounts and move them to their organisational emails. If a user wants to continue using a Google account, this will still be supported and possible.

Akvo also published a blog informing about the changes Akvo made to ensure GDPR compliance https://akvo.org/blog/simplicity-security-akvo-flow/.

The Akvo Foundation's sub-processors are listed here: https://akvo.org/help/third-parties/