DATA PROTECTION POLICY

June 2018, Version 1.0

CONTENTS

1. Policy statement

1.1 The Aquaculture Stewardship Council ('ASC', 'we', 'us', and 'our') is committed to fully complying with all the requirements of the General Data Protection Regulation (GDPR).

2. Scope

2.1 This data protection policy explains how we will comply with our responsibilities and obligations under the GDPR and applies to:

- All personal data whose use is controlled by us, whether kept on paper or electronically (i.e. Computers);
- All our staff and any of our data processors.

2.2 This policy should be read and used in conjunction with our other following policies

- Privacy
- Retention
- Staff Handbook or Governance Handbook for Trustees

3. Objective

3.1 The objective of this policy is to:

- Ensure we follow the principles of personal data;
- Ensure personal data is processed in a consistent manner throughout the organisation at all times;
- Clarify responsibilities for implementing, complying and monitoring this policy;
- Give guidance to staff and data processors about how to identify and minimise the risks of breaching the GDPR as well as the possible consequences of doing so.

4. Definitions

4.1 **Personal data** means any information relating to an identified or identifiable person ('data subject') such as a name, postal/email address or an identification number.

4.2 Examples of personal data typically processed by us are:

- First and last names
- Postal and email addresses
- Telephone numbers
- Identity documents (e.g. passports & driving licence)
- Identity numbers (e.g. National Insurance and Bank accounts or national identity card number)
- Career & educational documents (e.g. CVs & qualifications)
- Any contact information

4.3 **Special categories of personal data** means personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying

a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation and data concerning criminal convictions or offences.

Examples of special category personal data typically processed by us are:

- Health & medical information (including whether a person has a disability)
- Information about ethnic origin & race
- Staff sickness records

4.4 **Data subject** means any individual whose personal data is processed by us.

Examples of our data subjects are:

- Clients/customers
- Staff including part-time staff, contractors and interns
- Staff next of kin
- Job applicants
- Partners
- Donors
- Aquaculture producers
- Seafood processors
- Retailers and market partners
- Scientists
- Consumers
- Supporters
- Suppliers of goods/service
- Contacts

4.5 **Processing** means any use of personal data such as the collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure, dissemination, erasure and destruction. NB: This means that virtually anything we do with personal data will be processing.

4.6 **Data controller** means the organisation which decides the purposes and means of the processing of personal data. NB: ASC is the data controller for the purposes of this policy.

4.7 **Data processor** means an individual or organisation that processes personal data on behalf of a data controller

Examples of our data processors are:

- Morcan
- Insurance and pension agencies
- Payroll agencies

4.8 **Personal data breach** means a breach of security leading to the accidental, or unlawful, destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

4.9 **Consent** means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data.

4.10 **Staff** means anyone working at or for us including:

- Board members/Trustees
- Other advisors such as Technical Advisory Group members
- Directors
- Permanent, interim and temporary employees
- Trainees
- Interns

5. Principles of data protection

5.1 Personal data shall be:

1. Processed lawfully, fairly and in a transparent manner.

2. Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes ('purpose limitation').

3. Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation').

4. Accurate and, where necessary, kept up to date ('accuracy').

5. Kept for no longer than is necessary ('storage limitation').

6. Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

6. Roles and responsibilities

6.1 Our Supervisory Board Members have ultimate responsibility for ensuring compliance with the GDPR, the principles of data protection and this policy.

6.2 The Head of Governance and Corporate Services has day-to-day operational responsibility for ensuring we comply with the GDPR, the principles of data protection and this policy. The Head of Governance and Corporate Services can be contacted at: richard.ryan@asc-aqua.org

6.3 All staff have a responsibility to comply with the GDPR, the principles of data protection and this policy when carrying out their duties.

6.4 Line managers are responsible for supporting staff's adherence with this policy.

6.5 All data processors have a responsibility to comply with the GDPR, the principles of data protection and this policy when carrying out their contractual and statutory obligations to us.

6.6 Failure to comply with this policy may result in legal and/or disciplinary action.

7. Rights

7.1 Data subjects' have the right to:

1. **Be informed** about the collection and use of their personal data.
2. **Access** their personal data.
3. **Rectification** of inaccurate personal data.
4. **Erasure** (deletion) of their personal data (also known as the 'right to be forgotten).*
5. **Restrict processing** of their personal data.*
6. **Data portability -** to easily move, copy or transfer their personal data.
7. **Object** to:

    7.1. processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling);

    7.2. direct marketing (including profiling); and,

    7.3. processing for purposes of scientific/historical research and statistics.

8. **Appropriate decision-making** in relation to automated decision making and profiling.

*This is not an absolute right and only applies in certain circumstances

8. Subject Access Requests

8.1 Any data subject may make a Subject Access Request, ('SAR'). Anyone member of staff or data processor in receipt of a SAR must pass it on to the Head of Governance and Corporate Services (with their line manager in copy) as soon as possible as a matter of urgency.

9. Security

9.1 All staff and data processors are responsible for ensuring that any personal data which we are responsible for is kept securely.

9.2 Examples of keeping personal data secure are:

- Paper files/records should be kept in locked cabinets when not in use;
- Monitors/computer screens should be visible only to those who need to see them;
- Paper files/records should not be removed from our business premises without appropriate authorisation;
- Desks should be cleared when not in use;
- Personal data no longer required for day-to-day use should be sent to secure archiving.

10. Disclosure (sharing)

10.1 This includes the disclosure (sharing) of personal data by:

- Staff with other teams /departments; and,
- Staff with third parties/other organisations (including out data processors).
- Our data processors to third parties.

10.2 Personal data must not be disclosed unless the recipient is authorised to have access to that personal data and then only in accordance with the GDPR.

10.3 Examples of unauthorised recipients are:

- Family members
- Friends

10.4 Staff and data processors should exercise great caution when asked to disclose personal data and if in doubt should seek advice from the Head of Governance and Corporate Services before doing so.

10.5 All decisions to disclose personal data must be recorded [and all such disclosures must be specifically authorised by the Head of Governance and Corporate Services.

11. Retention

11.1 Personal data must not be kept for any longer than is necessary and only in accordance with our retention policy.

12. Disposal (deletion)

12.1 When it is no longer necessary to keep it, personal data must be disposed of securely. This means that:

- Paper will be shredded on site, or disposed of externally as confidential waste;
- Computer equipment will be disposed of securely by specialist contractors.

[A register will be maintained to record details of the media and computer equipment that has been disposed of, when it was disposed, how it was disposed and by whom].

13. Transfer outside the EEA

13.1 The GDPR generally prohibits the transfer (sending) of personal data outside the European Economic Area (EEA) unless:

- An ‘adequacy decision’ has been made for the destination country; or,
- The transfer is subject to appropriate safeguards; or,
- A ‘derogation’ can be relied upon, e.g.
-
    - Where it is necessary for the conclusion or performance of a contract that we have with the data subject or another person, or,

- It is in our legitimate interests (this will only be available to and used by us in very limited circumstances).
- With the data subject's explicit consent (this can only be available to and used by us in very limited circumstances).

13.2 These restrictions mean that personal data cannot be freely transferred outside the EEA and that it will be a breach of the GDPR to do so unless any such transfer can be made in accordance with the above.

13.3 All decisions to transfer personal data outside the EEA must be specifically authorised by the Head of Governance and Corporate Services.

14. Data protection Impact assessments

14.1 A data protection impact assessment (DPIA) is a process to help identify and minimise the data protection risks of a project.

14.2 The GDPR includes a new obligation to conduct a DPIA for types of processing likely to result in a high risk to individuals' interests and is good practice for any major new project which requires the processing of personal data.

14.3 Any circumstances where a DPIA may be required should not be undertaken without the approval of the Head of Governance and Corporate Services.

15. Marketing

15.1 The rules about sending marketing messages, (which are not the GDPR), mean, in summary, that we should not contact individuals without being satisfied that they do not object to hearing from us and that by contacting them we are not being a nuisance to them.