Sustainable *Eel* Group

The Sustainable *Eel* Group

Data Security Policy

www.sustainableeelgroup.org

Version 1.0

July 2018

Data Security Policy

Versions Issued

Version No.	Date	Description of Amendment
1.0	3 July 2018	Initial

This document is the property of the Sustainable Eel Group. It is effective from the date above

Version 1.0
July 2018

For further information please see: www.sustainableeelgroup.org

Or contact us at: info@sustainableeelgroup.org

Registered address: c/o Wetlands International European Association
Rue de Trèves 59-61, B-1040, Brussels, Belgium

Contents **Page**

1. Purpose 3

2. Applicability and responsibility 3

3. Data security 4

3.1 Handling confidential and proprietary data and information 4

3.2 Data Ownership 5

3.3 Quality Control 5

3.4 Data Repositories and Access 5

3.5 Client Audit Data 6

1. Purpose

This document describes the Data Security and Privacy Policy for the Sustainable Eel Group (SEG). It explains how personal and commercial data will be handled, to ensure it is kept confidential and secure, and how SEG processes any personal data collected via its website.

It is to ensure compliance with legislation such as the General Data Protection Regulation (GDPR), 2018.

2. Applicability and responsibility

This policy is for SEG use and for publication on the SEG website, www.sustainableeelgroup.org, to inform our contacts and users of our website of our policy.

It is SEG's responsibility to ensure that this policy is kept up to date to comply with latest legislation and guidance. A web-page version of this policy will be produced and is linked here.

3. Data security

Data and information required for the management and continuous improvement of the SEG system will come directly from clients and businesses, or indirectly via the Certification Body. SEG personnel will therefore be in possession of commercially sensitive data and information from individual businesses. This information serves as the basis for the SEG Monitoring and Evaluation system.

SEG is committed to ensuring that sensitive and confidential data provided by clients, businesses, contacts and stakeholders is protected, secure, and remains private.

3.1 Handling sensitive, commercial, confidential and proprietary data and information

- When seeking information from clients and businesses, such as through surveys, they shall be advised in writing that it will be treated according to our Data Security Policy. A website link will be provided to the policy to ensure that it can be accessed.
- All data and information about individual clients and businesses shall, as a default, be treated as confidential ('commercial in confidence').
- Data and information shall be held in password protected folders on the computers of SEG personnel, with back-up on cloud-based folders, again password protected.
- Permission shall be sought to publish any data or information that is specific to the client or business. SEG will publish client SEG standard audit reports, without commercially sensitive information, SEG shall have a contractual agreement with the client about what data collected from the client or business can be used under what circumstances.
- Certification Bodies shall have similar agreements with clients to treat their information securely.

- Data from clients will also be anonymised through aggregatation to monitor and report trends across the sector, e.g. '*The number and % of businesses in each part of the sector achieving the SEG standard'.* Such data will not be traceable via the published report, to the individual.
- When emails are sent to an external mailing list, email addresses will be placed in the 'blind copy (BC or BCC) box so that they are not visible to other parties.
- SEG holds a stakeholder mailing list using the on-line service 'Mailchimp'. This service requires contacts to opt-in to the service and is GDPR compliant. Access to the SEG mailing list is by log-in and password and is restricted to SEG staff and a contracted supplier who manages the issuing of SEG newsletters and other communications.
- Any contact can request to see and review the data held about them at any time and can also rescind permission to hold their data. To do this contact: info@sustainableeelgroup.org.

3.2 Data Ownership

- Source data and information that is gathered through the assurance process is owned by the entity (client, business, contact or stakeholder) who provided that information.
- CBs shall specify in their contracts with clients that client data will be treated confidentially, securely, and will be provided to SEG, who shall also treat it confidentially and securely.
- CBs shall hold the intellectual property rights of audit reports.
- Contractually, SEG obtains permission to use this data in anonymised form for marketing, monitoring and evaluation and other non-commercial purposes. SEG can use and process the information to create reports, and SEG shall be the owner of the data and information in such reports.
- Publication of an individual entity's information, without further processing - such that it is not traceable to the entity, shall require the permission of the provider.
- The underlying assurance data belong to the client, but SEG owns aggregated, transformed data. Any data that are public, such as through public audit reports, is considered in the public domain with no claims to ownership.

3.3 Quality Control

- CBs shall apply data quality control processes to ensure that audit reports are accurate. This shall be a contractual requirement of CBs.
- SEG staff shall review data and information received for obvious errors.
- A sample 10% of submissions will be double-checked in detail by SEG staff and also returned to the provider for double-checking.
- When producing reports, SEG staff will consult with a colleague and/or an independent party to review the data and information presented and the conclusions made.

3.4 Data Repositories and Access

- SEG staff shall hold data and information that only they use individually, in a folder on their personal computer that is password protected and backed up to a password protected cloud-based folder. Only those staff shall have access to those files and passwords.

- Where information must be accessed by more than one member of SEG staff, it shall be filed in a password protected shared cloud-based folder. Access controls (password or link to the folder), shall be restricted to SEG staff only. In the instance of staff changes or suspicions of security breaches, passwords will be changed. For shared drives, the person with the role of Data Protection Officer, responsible for authorising, assigning passwords and revoking them, is the Director of Conservation Operations, currently David Bunt.

3.5 Client Audit Data

- Certification Bodies (CBs) audit clients against the SEG standard to assess compliance. They shall compile audit reports which contain commercially sensitive or proprietary information. They also issue SEG standard certificates on behalf of SEG.
- The CB collects and creates this information on behalf of SEG and shall provide copies of audit reports and certificates to SEG. The requirement to provide this shall be specified in SEG's contract with the CB.
- The underlying data in audit reports belongs to the client. The audit reports are owned by the CB and, on provision to SEG, on whose behalf they are created, they are jointly owned by SEG.
- Published audit reports, with confidential information removed, are published and become public documents, with no ownership.
- Certificates are published, so become public documents, with no ownership.
- The commercial or other proprietary information in audit reports is to be treated as confidential. It shall not be published or shared with any other party without the written permission of the client.

Contact SEG

Should you have any concerns or queries about SEG's use of your data and information, please contact SEG via info@sustainableeelgroup.org.

The Sustainable *Eel* Group

Data Security Policy

Version 1.0
July 2018

For further information please see: www.sustainableeelgroup.org

Or contact us at: info@sustainableeelgroup.org

Registered address: c/o Wetlands International European Association
Rue de Trèves 59-61, B-1040, Brussels, Belgium