The Sustainable *Eel* Group

Data Management System

© Sustainable Eel Group
www.sustainableeelgroup.org

Version 2.1
1 November 2024

Data Management System

Versions Issued

Version	Date	Description of Amendment	Approved by
1.0	3 July 2018	Initial: Data Security Policy	A. Kerr, Chair of Board
2.0	23 June 2023	Additions made to align with ISEAL Codes of Practice. Change of title to Data Management System	SEG Board
2.1	1 November 2024	Change to registered address	SEG Board

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

Copyright:

Version 2.1
1 November 2024

For further information please see: www.sustainableeelgroup.org

Or contact us at: info@sustainableeelgroup.org

Registered address: Sustainable Eel Group VZW
Trierstraat 59-61
1040 Bruxelles
Belgium

Contents

Page

1. Purpose

1.1 This document describes the Data Management System for the Sustainable Eel Group (SEG). It describes how:

- SEG manages responsibilities and actions related to data governance;
- data, including personal and confidential/commercial data, will be handled to ensure it is kept confidential and secure;
- SEG manages any personal or confidential/proprietary data collected via its website or otherwise; and
- data can be managed in order to ensure the greatest opportunity for future use in the SEG Monitoring, Evaluation and Learning program.

1.2 This document also aims to:

- to ensure compliance with legislation such as the General Data Protection Regulation (GDPR), 2018, and ISEAL Codes of Best Practice; and
- make external organisations aware of the SEG Data Management System.

2. Applicability and responsibility

2.1 It is SEG's responsibility to:

- ensure that this system is kept up to date to comply with latest legislation and ISEAL codes of practice;
- implement the policy and system and communicate its requirements to partners and stakeholders who are also responsible for data related to the SEG Standard System;
- ensure the requirements of this policy and system are implemented in contracts and agreements;
- develop and deliver training internally and externally to ensure all data holders in the SEG data chain are aware of the risks to data and are able to mitigate those risks as described;
- describe how stakeholders can use SEG data on the website; and
- explain how data collected in surveys etc. will be used.

2.2 Any person/business or client 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. Composition

3.1 The Data Management System consists of:

1. This document (011 Data Management System);
2. The Data Inventory (011a Data Inventory); and
3. 011b Data Management System training (module in preparation)

3.2 The Data Management System works closely with, but is separate from, the Document Management System.

4. Data governance

4.1 Data governance involves both data security and ensuring that data-related processes create value. Managing the risks to data enables SEG to minimise exposure to data loss. Documenting the approach to data governance in this system provides clarity on how and where value can be created with data.

4.2 Good data governance is also an innovation enabler, it enables data to be seen and its management as an opportunity, not just risk. SEG aims to use relevant data in innovative ways to assess impact through SEG's Monitoring, Evaluation and Learning programme, to support training and to communicate with stakeholders.

4.3 SEG data

4.3.1 SEG manages a wide range of documents and data as part of its day-to-day operations, the vast majority of which are electronic in nature. Data is held by a variety of individuals and organisations as described in 011a SEG Data Inventory.

4.3.2 **SEG is committed to ensuring that personal and confidential/proprietary data provided by individuals, clients, businesses, contacts and stakeholders is protected, secure, and remains private.**

4.3.3 Personal data is defined as: '*any information that relates to an identified or identifiable living individual. Different pieces of information, which collected together can lead to the identification of a particular person, also constitute personal data*.'[1]

4.3.4 Confidential/proprietary data is defined as: '*any information which is proprietary to the disclosing party and is not generally known to the public*.'[2] All data and information about individual clients shall, as a default, be treated as confidential/proprietary data ('commercial in confidence').

4.3.5 SEG will strive to ensure that all data are managed in a manner that supports our Monitoring, Evaluation and Learning system.

4.4 Data retention

4.4.1 SEG records shall, in general, be maintained on file for seven (7) years, unless otherwise required to be kept for a longer or shorter period by local legislation. Personal information is subject to the GDPR and will be kept only as long as it is needed.

---

[1] European Commission. https://commission.europa.eu/law/law-topic/data-protection/reform/what-personal-data_en#:~:text=Personal%20data%20is%20any%20information,person%2C%20also%20constitute%20personal%20data.

[2] GDPR. https://gdprlocal.com/nda/#:~:text=(a)%20For%20purposes%20of%20this,)%20any%20marketing%20strategies%2C%20plans%2C

4.4.2 When a decision is made to destroy documents or records local or physical copies shall also be destroyed. Any printed copy of personal or confidential/proprietary data shall be confidentially destroyed, for instance, by shredding the documents. If stored electronically, the personal or confidential/proprietary information shall be securely electronically deleted.

4.5 Collecting and handling data

4.5.1 Agreements with CABs and other partners shall require that client/audit data they hold will be held in a secure means. CABs shall have a contractual agreement with the client specifying:

a) what data collected from the client or business can be used under what circumstances;
b) that data identified as personal or confidential/proprietary will not be shared without permission;
c) that their data will be treated securely;
d) that data will be provided to SEG, who shall also treat it as personal or proprietary/confidentially as appropriate;
e) that data from clients may be anonymized through aggregation for the SEG Monitoring, Evaluation and Learning program 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 or client; and
f) SEG will publish client SEG standard audit reports, without personal or confidential/proprietary information unless permission has been granted to publish such data, and certificates.

4.5.2 **Where not already covered by agreement, permission shall be sought to publish any data or information that is specific to an individual, client, or business. Where permission is not granted, data will not be published.**

4.5.3 When seeking personal or proprietary information from clients and businesses, such as through surveys or audits they shall be advised in writing that it will be treated according to the SEG Data Management System. A website link will be provided to the system to ensure that it can be accessed. SEG shall ensure that agreements with parties who handle SEG data shall be in alignment with this system.

4.5.4 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.

4.5.5 SEG shall periodically review the manner in which data is collected and handled to ensure that the efficiency of analysing data for the Monitoring, Evaluation and Learning system is maximised.

4.6 Data ownership

4.6.1 Source data that are gathered through the assurance process is owned by the entity (client, business, contact or stakeholder) who provided that information.

4.6.2 CABs shall hold the intellectual property rights of audit reports. The CAB collects and creates this information on behalf of SEG and shall provide copies of audit reports and certificates to SEG in a format specified by SEG. The requirement to provide this shall be specified in SEG's contract with the CAB.

4.6.3 Published audit reports, with personal and confidential/proprietary information removed (unless permission to publish it has been granted by the owner), are published and become public documents, with no ownership. Certificates are published, so become public documents, with no ownership. Parties wishing to use SEG data published on the website may do so. Attribution to SEG is appreciated.

4.6.4 SEG extracts data from audit reports in 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.

4.7 Data integrity

4.7.1 CABs shall apply data quality control processes to ensure that audit reports are accurate (see Assurance System). This shall be a contractual requirement of CABs. SEG staff shall review data 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.

4.7.2 Audit reports will be reviewed by the client, the CAB and SEG to ensure personal and confidential/ proprietary information has been removed before publication.

4.7.3 When producing other reports, SEG staff will consult with a colleague and/or an independent party to review the data and information presented and the conclusions made.

4.8 Data Repositories and Access

4.8.1 SEG data are stored and accessed according to the SEG Document Management System. These are listed in our 011a Data Inventory.

5. Data breach

5.1 An IT security incident is when there is denying, disrupting, stealing or accidental disclosure of Data or Information from IT systems. It is imperative that IT security incidents are reported and resolved in an efficient and timely manner. The severity, scope, amount of damage and therefore cost of an IT security incident increases with every hour it remains unresolved.

5.2 If SEG staff or board members suspect a breach of data they shall immediately take actions to contain and mitigate the breach and notify the Chair or their delegate, who will appoint someone to oversee the mitigation.

5.3 In the event that personal or confidential/proprietary data is published inadvertently SEG shall remove it immediately from the website and notify the owner of data of the incident. Additional actions may be required and shall be determined in consultation with the data owner.

6. Training

6.1 Individuals who handle client data shall be trained on this system prior to handling SEG data and shall complete an annual refresher training. SEG shall provide training to:

a) SEG staff who handle data;
b) CAB staff who handle client data;
c) Others who handle SEG data.

6.2 SEG Board members shall also be made aware of the system but, unless they handle data, require an overview only and not an annual refresher.

6.3 Training shall, minimally consist of:
a) Types of data (personal and confidential/proprietary);
b) The procedures for handling data;
c) The significant risks to data;
d) Processes for maximizing the efficiency of using data for monitoring, evaluation and learning.

7. Contacting SEG

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