Data Protection Policy

This policy applies to set the basic standards regarding the processing of Personal Data by Scottish Environment Protection Agency (SEPA). This policy will be updated and amended from time to time. Staff will be notified of changes and a copy will be made available on the intranet.

SEPA Data Protection Policy statement

Everyone has rights with regard to how their personal information is handled. During the course of our activities SEPA will collect, store and process personal information about our customers, staff and all other individuals who work with us or contact us. We recognise the fundamental importance of handling this information in an appropriate and lawful manner to maintain the confidence and trust of our customers and staff in our processing of their Personal Data. Protecting the confidentiality and integrity of Personal Data is a critical responsibility that we take seriously at all times. If SEPA fails to comply with Data Protection Law, then it may be subject to enforcement and sanctions from the Information Commissioner.

In this Policy, we set out the framework in which SEPA will ensure the appropriate use of Personal Data in line with the law.

1 Introduction

1.1 ***Who we are*** - This Policy sets out how the Scottish Environment Protection Agency ("**we**", "**our**", "**us**", the "**Organisation**", **SEPA**) handle the Personal Data of our customers, suppliers, employees, workers and other third parties.

1.2 ***Application of this Policy*** - This Policy applies to all staff and contractors working for or on behalf of SEPA.

1.3 ***Definitions*** - Capitalised terms have the meanings given to them in the Glossary contained in Appendix 1.

2. Status of the Policy

2.1 This Policy has been approved by SEPA's Agency Management Team and discussed with its recognised trade union, Unison.

3. Scope

3.1 ***Personal Data*** - This Policy applies to all Personal Data we Process (or that a third party Processes on our behalf) regardless of the media on which that data is stored or whether it relates to past or present employees, workers, customers, clients or supplier contacts, shareholders, website users, and even members of the public whose Personal Data we Process.

3.2 ***Data protection responsibilities*** - All individual business areas, functions, teams and individuals are responsible for ensuring all Personnel comply with this Policy and need to implement appropriate practices, processes, controls and training to ensure such compliance. Staff with have management responsibility for Personnel, are expected to regularly review all the systems, processes and procedures under their control to ensure

they comply with this Policy and check that adequate governance controls and resources are in place to ensure proper use and protection of Personal Data.

3.3 ***Data Protection Officer*** - The Data Protection Officer (DPO) is responsible for ensuring the Organisation's compliance with Data Protection Law and for overseeing (and updating) this Policy and, as applicable, Related Policies and Guidelines. That role is held by Alison M. Mackinnon, Tel: 01786 457700, email: dataprotection@sepa.org.uk.

3.4 ***DPO Directions*** – staff must comply with all directions on data protection matters issued by the DPO.

3.5 ***Queries about this Data Protection Law or this Policy*** - The DPO should be contacted with any questions about the operation of this Policy or Data Protection Law or if where there are any concerns that this Policy is not being or has not been followed.

3.6 ***Mandatory Consultation*** – Staff **must immediately** contact the DPO in the following circumstances:

- if they are unsure whether particular Processing will be within the terms of the relevant Privacy Notice (see Section 5.2 below) or are otherwise unsure of the lawful basis which they are relying on to process Personal Data;
- if they are unsure about the retention period for the Personal Data being Processed (see Section 8 below);
- if they are unsure about what security or other measures need to implemented to protect Personal Data (see Section 9 below);
- if there has been a Personal Data Breach (Section 9.2 below);
- if they are unsure whether they are permitted to transfer Personal Data outside the EEA (see Section 10 below);
- if they receive any communication from an individual which may seek to exercise any rights which he/she may have under Data Protection Law as a Data Subject (see Section 11);
- whenever they are engaging in a significant new, or change in, Processing activity or plan to use Personal Data for purposes others than for which it was collected (see Section 12.4 below);
- if they are considering entering into any contracts with third parties (including our vendors) (see Section 12.7 below) which shall involve the disclosure or sharing of Personal Data; or
- If they plan to undertake any activities involving Automated Processing including profiling or Automated Decision-Making (see Section 12.5 below);

4 Data Protection Principles

4.1 ***Compliance with data protection principles generally*** - We adhere to the principles relating to Processing of Personal Data set out in Data Protection Law and summarised in Appendix 2. We are responsible for and must be able to demonstrate compliance with these principles (Accountability).

4.2 ***Specific requirements*** – the remainder of this Policy explains what measures the Organisation has put in place to comply with the data protection principles and what staff and contractors are expected to do as part of those measures.

5 Lawfulness, fairness, transparency

5.1 ***General requirements*** – The data protection principles require us to Process Personal Data lawfully, fairly and in a transparent manner. We must only collect, Process and share Personal Data for specified purposes.

5.2 ***Privacy Notices*** - In order to ensure compliance with these requirements, the Organisation has prepared two forms of Privacy Notice which explain how the Organisation Processes Personal Data that it collects. The Privacy Notice on our website – accessible at https://www.sepa.org.uk/help/privacy-policy/ – explains the purposes for which we Process Personal Data that we collect from Data Subjects who are external to the Organisation. The second Privacy Notice is accessible at https://www.sepa.org.uk/help/privacy-policy/privacy-notices/ and this explains the purposes for which we Process the Personal Data of our Personnel. It is essential that we Process all Personal Data in accordance with the terms of the relevant Privacy Notice and staff are responsible for ensuring that they are aware of the terms of each Privacy Notice in so far as it is relevant to the performance of your duties.

5.3 ***Processing must accord with Privacy Notices*** - The Privacy Notices have been prepared and approved by the DPO. Staff should not attempt to alter them or to Process Personal Data other than in accordance with their terms. If staff have any queries or concerns concerning any proposed Processing activity and whether it is within the scope of a Privacy Notice then they should consult the DPO before commencing any Processing.

5.5 ***Communication of Privacy Notices*** - The information contained within the Privacy Notices must be provided to the individual Data Subjects who's Personal Data we Process and we must ensure that the Privacy Notices are properly communicated to individuals at the point at which their Personal Data is collected. For advice on how to do this please consult the DPO.

5.6 ***Personal Data provided by third parties*** - When Personal Data is collected indirectly (for example, from a third party or publically available source), staff must provide the Data Subject with all the information required by the Privacy Notice as soon as possible after collecting/receiving the data. Where we receive Personal Data from a third party with whom we have a contractual relationship, we may require that third party to provide the Data Subject with the information contained in our Privacy Notice on our behalf. More generally, staff must also check that the Personal Data was collected by the third party in accordance with Data Protection Law and on a basis which contemplates our proposed Processing of that Personal Data.

6 Data minimisation

6.1 ***General requirements*** - Under the data protection principles, we must ensure that Personal Data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed.

6.2 ***Use for job duties only*** - Staff may only Process Personal Data when performing their job duties requires it. Staff cannot Process Personal Data for any reason unrelated to their job duties.

6.3 ***No excessive data*** - Do not collect excessive Personal Data. Staff should ensure that any Personal Data they collect is actually required for the intended purpose for which they will Process it.

6.4 ***Data retention and destruction*** - Staff must ensure that when Personal Data is no longer needed for specified purposes, it is deleted or anonymised in accordance with the Organisation's data retention and destruction policy –See also Section 8 of this Policy.

7 Accuracy

7.1 ***General requirements*** - The data protection principles require that Personal Data must be accurate and, where necessary, kept up to date. It must be corrected or deleted without delay when inaccurate.

7.2 ***Ongoing checking*** – Staff will ensure that the Personal Data we use and hold is accurate, complete, kept up to date and relevant to the purpose for which we collected it. Staff must check the accuracy of any Personal Data at the point of collection and at regular intervals afterwards.

8 Storage and retention

8.1 ***General requirements*** - The data protection principles require that Personal Data must not be kept in an identifiable form for longer than is necessary for the purposes for which the data is processed.

8.2 ***Data retention*** - We must not keep Personal Data in a form which permits the identification of the Data Subject for longer than needed for the legitimate business purpose or purposes for which we originally collected it including for the purpose of satisfying any legal, accounting or reporting requirements.

8.3 ***Storage on Organisation systems etc.*** - Staff must ensure that all Personal Data that they Process as part of their work duties are stored in the Organisation's systems (or, for paper records, either on the Organisation's premises or formally transferred to SEPA's offsite storage) in accordance with Relevant Policies and Guidelines. No Personal Data should be held anywhere else.

8.4 ***Compliance with retention policies*** - The Organisation maintains retention policies and procedures (as part of the Relevant Policies and Procedures) to ensure Personal Data is deleted after a reasonable time following the end of the purposes for which it was being held, unless law requires such data to be kept for a minimum time. We also provide Data Subjects with information concerning data retention periods in our Privacy Notices, where applicable. - Staff must perform their work duties in accordance with requirements of the relevant retention policies and procedures in so far as relevant to the Personal Data they Process.

9 Security integrity and confidentiality

9.1 ***Protecting Personal Data***

9.1.1 Personal Data must be secured by appropriate technical and organisational measures against unauthorised or unlawful Processing, and against accidental loss, destruction or damage.

9.1.2 Staff must

- perform their work duties in such a way as to protect the Personal Data that we hold;

- follow all procedures and technologies we put in place to maintain the security of all Personal Data from the point of collection to the point of destruction. Staff must also comply with the requirements of all Relevant Policies and Guidelines and any directions issued by the DPO; and

- not attempt to circumvent the administrative, physical and technical safeguards we implement and maintain to protect the Personal Data.

9.2 ***Reporting a Personal Data Breach***

9.2.1 Data Protection Law may require the Organisation to notify any Personal Data Breach to the Information Commissioner's Office and, in certain instances, the individual Data Subjects affected.

9.2.2 We have put in place procedures to deal with any suspected Personal Data Breach and will make appropriate notifications where we are legally required to do so.

9.2.3 If staff know or suspect that a Personal Data Breach has occurred, staff should **not** attempt to investigate the matter themselves. **Immediately** contact the designated email address databreach@sepa.org.uk in accordance with the Security Incident Procedure Staff should preserve all evidence relating to the potential Personal Data Breach.

9.2.4 The contact details for reporting Personal Data Breaches are:
email – databreach@sepa.org.uk
Telephone: 03000 669966

Note that Personal Data Breaches should be notified immediately staff become aware of them i.e. on a 24/7 basis. Any delay may be seriously prejudicial, both in terms of protecting the Personal Data concerned but also in terms of our obligations to notify the relevant Data Subjects of the occurrence of a Personal Data Breach.

10 Transfers

10.1 ***General requirements*** - Data Protection Law restricts data transfers to countries outside the EEA in order to ensure that the level of data protection afforded to individuals by Data Protection Law is not undermined. Staff transfer Personal Data originating in one country across borders when they transmit, send, view or access that data in or to a different country.

10.2 ***Restrictions on transfers outside the EEA*** - Staff may only transfer Personal Data outside the EEA if one of the following conditions applies:

10.2.1 The European Commission has issued a decision confirming that the country to which we transfer the Personal Data ensures an adequate level of protection for the Data Subjects' rights and freedoms;

10.2.2 appropriate safeguards are in place such as binding corporate rules (BCR), standard contractual clauses approved by the European Commission (sometimes called 'model form clauses'), an approved code of conduct or a certification mechanism, a copy of which can be obtained from the DPO;

10.2.3 The Data Subject has provided Explicit Consent to the proposed transfer after being informed of any potential risks; or

10.2.4 the transfer is necessary for one of the other reasons set out in Data Protection Law including the performance of a contract between us and the Data Subject, reasons of public interest, to establish, exercise or defend legal claims or to protect the vital interests of the Data Subject where the Data Subject is physically or legally incapable of giving Consent and, in some limited cases, for our legitimate interest.

10.3 ***Role of the DPO*** - Where staff wish to transfer outside the EEA, it is their responsibility to ensure that the transfer concerned satisfies these requirements. In practice, this means that they need to check with the DPO to confirm that the proposed transfer is permissible **before** they do it. Staff must follow any guidelines or directions they are given by the DPO.

11 Data subject's rights and requests

11.1 ***Individual Rights*** - Data Subjects have rights when it comes to how we handle their Personal Data. These include rights to:

- withdraw Consent to Processing at any time (where we Process Personal Data on the basis of consent);
- receive certain information about our Processing activities;
- request access to their Personal Data that we hold;
- prevent our use of their Personal Data for direct marketing purposes;
- ask us to erase Personal Data if it is no longer necessary in relation to the purposes for which it was collected or Processed or to rectify inaccurate data or to complete incomplete data;
- restrict Processing in specific circumstances;
- challenge Processing which has been justified on the basis of legitimate interests or in the public interest;
- request a copy of an agreement under which Personal Data is transferred outside of the EEA;
- object to decisions based solely on Automated Processing, including profiling (ADM);
- prevent Processing that is likely to cause damage or distress to the Data Subject or anyone else;
- be notified of a Personal Data Breach which is likely to result in high risk to their rights and freedoms;
- make a complaint to a regulator; and
- in limited circumstances, receive or ask for their Personal Data to be transferred to a third party in a structured, commonly used and machine readable format.

11.2 ***Notify DPO*** - Where staff receive a communication from any individual which seeks (or might be construed as seeking) to exercise any rights in relation to Personal Data, they must **immediately** notify the DPO and follow the DPO's instructions. Do not attempt to deal with the communication beforehand.

12 **Specific activity**

12.1 ***General Requirements*** - Under Data Protection Law, we must implement appropriate technical and organisational measures in an effective manner, to ensure compliance with data protection principles. We must also be able to demonstrate we comply with them. This Section sets out what we require staff to do so that we may discharge these responsibilities.

12.2 ***Record Keeping*** - Data Protection Law requires us to keep full and accurate records of all our data Processing activities. The Register of Processing will be maintained by the DPO. Relevant staff must ensure that they update the DPO regarding the processing of Personal Data carried out as part of their works duties, so that proper and accurate records of the work that they do are recorded.

12.3 ***Training and Audit***

12.3.1 Staff must undergo all mandatory data privacy related training.

12.3.2 Where a staff member has management responsibility for other Personnel,

- they must ensure your team undergo similar mandatory training as well.
- they must regularly review all the systems and processes under their control to ensure they comply with this Policy and check that adequate governance controls and resources are in place to ensure proper use and protection of Personal Data.

12.4 ***Data Protection Impact Assessment (DPIA)***

12.4.1 the DPO must be advised at the earliest opportunity in order that he/she can consider the proposed project or activity and determine whether a Data Protection Impact Assessment is required, in the following circumstances:.

12.4.2 When we are considering or planning

- projects to implement major system or business change programs involving the Processing of Personal Data including:
- use of new technologies (programs, systems or processes), or changing technologies (programs, systems or processes);
- Automated Processing including profiling and ADM;
- large scale Processing of Sensitive Data; and
- large-scale, systematic monitoring of a publicly accessible area.
- any other activity which will involve (or may potentially involve) the Processing of Personal Data which has not been collected before or the Processing of Personal Data in new ways or for new purposes;

12.4.3 The DPO may require staff to complete pre-DPIA screening questions in order to determine whether a full DPIA is required. No Processing of Personal Data pursuant to such a project or activity may be undertaken meantime without the approval of the DPO.

12.4.5 Staff must comply with any directions given by the DPO and the terms of the Data Protection Impact Assessment process, which forms part of the Relevant Policies and Guidance.

12.5 ***Automated Processing (including profiling) and Automated Decision-Making***

12.5.1 Specific restrictions apply under Data Protection Law in relation to Automated Decision Making.

12.5.2 A DPIA must be carried out before any Automated Processing (including profiling) or ADM activities are undertaken.

12.6 ***Direct Marketing***

12.6.1 Should SEPA undertake direct marketing to our customers, we would be subject to certain additional rules and privacy laws, particularly where the marketing activity is conducted electronically, e.g. by e-mail, telephone, fax or SMS.

12.7 ***Sharing Personal Data***

12.7.1 Generally we are not allowed to share Personal Data with third parties unless certain safeguards and contractual arrangements have been put in place.

12.7.2 Staff may only share the Personal Data we hold with another employee, agent or representative of our group (which includes our subsidiaries and our ultimate holding company along with its subsidiaries) if the recipient has a job-related need to know the information and the transfer complies with any applicable cross-border transfer restrictions.

12.7.3 Staff may only share the Personal Data we hold with third parties, such as our service providers if:

- they have a need to know the information for the purposes of providing the contracted services;
- sharing the Personal Data complies with the Privacy Notice provided to the Data Subject;
- the third party has agreed to comply with the required data security standards, policies and procedures and put adequate security measures in place;
- the transfer complies with any applicable cross border transfer restrictions; and
- a fully executed written contract that contains GDPR approved third party clauses has been obtained; and
- the DPO has authorised the data sharing. Do remember that the proposed sharing of Personal Data may require the conduct of a DPIA beforehand.
- The DPO may issue authorisations of a specific or general nature regarding the sharing of Personal Data with specific third parties and where these have been issued staff must ensure that they comply with their terms.

13 **Changes to this Policy**

13.1 This Policy may be changed from time to time. Where changes are made staff will be notified but it is staff's responsibility to check back regularly to obtain the latest copy of this Policy, which can be found *here*

13.2 This Policy does not override any applicable national data privacy laws and regulations in countries where the Organisation operates.

Appendix 1 – Glossary of Terms

Automated Decision-Making (ADM): when a decision is made which is based solely on Automated Processing (including profiling) which produces legal effects or significantly affects an individual. Data Protection Law prohibits Automated Decision-Making (unless certain conditions are met) but not Automated Processing.

Automated Processing: any form of automated processing of Personal Data consisting of the use of Personal Data to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning that individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements. Profiling is an example of Automated Processing.

Consent: agreement which must be freely given, specific, informed and be an unambiguous indication of the Data Subject's wishes by which they, by a statement or by a clear positive action, signifies agreement to the Processing of Personal Data relating to them.

Controller: the person or organisation that determines when, why and how to process Personal Data. It is responsible for establishing practices and policies in line with Data Protection Law. We are the Data Controller of all Personal Data relating to our Personnel and Personal Data used in our business for our own purposes.

Criminal Offence Data: Personal Data relating to criminal offences and convictions, or related security measures.]

Data Subject: a living, identified or identifiable individual about whom we hold Personal Data. Data Subjects may be nationals or residents of any country and may have legal rights regarding their Personal Data.

Data Privacy Impact Assessment (DPIA): tools and assessments used to identify and reduce risks of a data processing activity. DPIA can be carried out as part of Privacy by Design and should be conducted for all major system or business change programs involving the Processing of Personal Data.

Data Protection Officer (DPO): the person required to be appointed in specific circumstances under Data Protection Law. Where a mandatory DPO has not been appointed, this term means a data protection manager or other voluntary appointment of a DPO or refers to the Organisation data privacy team with responsibility for data protection compliance.

Data Protection Law: all data protection laws applying to the Processing of Personal Data by the Organisation, including the GDPR and, in the United Kingdom, the new Data Protection Act 2018;

EEA: the 28 countries in the EU, and Iceland, Liechtenstein and Norway.

Explicit Consent: consent which requires a very clear and specific statement (that is, not just action).

General Data Protection Regulation (GDPR): the General Data Protection Regulation ((EU) 2016/679).

Personal Data: any information identifying a Data Subject or information relating to a Data Subject that we can identify (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably access. Personal Data

includes Sensitive Personal Data and Pseudonymised Personal Data but excludes anonymous data or data that has had the identity of an individual permanently removed. Personal Data can be factual (for example, a name, email address, location or date of birth) or an opinion about that person's actions or behaviour.

Personal Data Breach: any act or omission that compromises the security, confidentiality, integrity or availability of Personal Data or the physical, technical, administrative or organisational safeguards that we or our third-party service providers put in place to protect it. The loss, or unauthorised access, disclosure or acquisition, of Personal Data is a Personal Data Breach.

Personnel: all employees, workers contractors, agency workers, consultants, directors, members and others.

Privacy by Design: implementing appropriate technical and organisational measures in an effective manner to ensure compliance with Data Protection Law.

Privacy Notices: the privacy notices referred to in Section 5.2 as updated from time to time

Processing or Process: any activity that involves the use of Personal Data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transmitting or transferring Personal Data to third parties.

Pseudonymisation or Pseudonymised: replacing information that directly or indirectly identifies an individual with one or more artificial identifiers or pseudonyms so that the person, to whom the data relates, cannot be identified without the use of additional information which is meant to be kept separately and secure.

Related Policies and Guidelines: the Organisation's policies, operating procedures or processes related to this Policy and designed to protect Personal Data.

Special Category Data: information revealing racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health conditions, sexual life, sexual orientation, biometric or genetic data,

Appendix 2 – Data Protection Principles

Article 5 of the GDPR requires that Personal Data shall be:

(a) processed lawfully, fairly and in a transparent manner in relation to the data subject (**'lawfulness, fairness and transparency'**);

(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall…not be considered to be incompatible with the initial purposes (**'purpose limitation'**);

(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (**'data minimisation'**);

(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that Personal Data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay (**'accuracy'**);

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the Personal Data are processed; Personal Data may be stored for longer periods insofar as the Personal Data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes…subject to implementation of the appropriate technical and organisational…in order to safeguard the rights and freedoms of the data subject (**'storage limitation'**);

(f) 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'**).

In addition, the GDPR requires that the controller shall be responsible for, and be able to demonstrate compliance with the Principles. (**'accountability'**).