INTRAC Data Protection Policy

Version 2.3

TABLE OF CONTENTS

ABBREVIATIONS

FAD	Finance and Admin Director
GDPR	General Data Protection Regulation These come into force in May 2018 and replaces the 1995 EU Data Protection Directive and the subsequent UK 1998 Data Protection Act. They cover the rights of individuals in relation to data held about them and spell out various duties for organisations who hold and process personal data.
ICO	Information Commissioner's Office https://ico.org.uk/ The ICO is the regulatory body for the UK in relation to the GDPR and their website includes sections specifically around the GDPR https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/
SMT	The Senior Management Team currently consisting of: Chief Executive; Finance and Admin Director; Consultancies and Training Director; Research, Learning and Communications Director; Business Development Manager

1 DATA POLICY

1.1 Responsibilities

INTRAC's Board is responsible for setting and reviewing this policy.

INTRAC's Management and Employees are responsible for its implementation. As with Health and Safety all staff will play a part in ensuring compliance with this policy.

In respect of the GDPR and any breaches of data security the Finance and Admin Director will be responsible for informing the appropriate regulatory authorities – the ICO and/or Charity Commission.

1.2 Scope

This policy covers data that is stored as hard copy as well as data that is stored electronically.

1.3 Data will only be held for specific organisational purposes

We will only hold data that is needed for a specific organisation purpose. See section 2.1.

We will not retain data longer than is necessary to achieve that purpose.

1.4 Each type of data will be assigned a data owner

The data owner is the person responsible for defining the rules for holding, processing, retention and security of that type of data. They are also responsible for ensuring that those rules are documented, communicated to and followed by staff involved.

The data owner will be responsible for periodically reviewing these rules to ensure that they adequately reflect current risks of loss/misuse and changes in technology and our organisational infrastructure.

The data owner will be responsible for periodically reviewing the rules for holding processing, and retaining data and ensuring that privacy notices/policies are revised accordingly and communicated to data subjects.

1.5 We will keep our data assets secure and safe

Data will be subject to appropriate security measures. The level of security will depend on the consequences to INTRAC or a partner organisation or individual if the data is lost, stolen or misused.

All electronic data should be stored in a location where it is encrypted and requires passwords to access it.

All electronic data should be backed up at regular intervals to an organisational server, where it is encrypted.

Data should should only be stored on a device that is not an organisational service (eg c:\ or a memory stick, if that location is encrypted and access is controlled by password). Storing data in such a location should be by exception and only if there is a business justification for doing so (eg whilst travelling without access to the organisational server through VPN).

Access to hard copy data should also be subject to adequate controls, eg use of locked filing cabinets for HR data. Thought should also be given to other threats such as loss/damage through fire or flooding.

We will identify key data assets and ensure that all data assets are documented through the Data Resource Register (see section 1.7)

1.5.1 BREACHES OF SECURITY

See Annexe 2.5 for guidance on what constitutes a Breach

If there has been a suspected breach of security then the FAD, or in their absence another member of the SMT, should be notified immediately. Also see section 1.6.7.

If the breach represents a significant risk to INTRAC (as determined by the FAD or director receiving notification) the Chief Executive will liaise with the Chair of the Board and ensure that the incident is reported promptly to the Charity Commission if appropriate.

https://www.gov.uk/guidance/how-to-report-a-serious-incident-in-your-charity

1.6 In respect of Personal Data we will comply with the GDPR

The terminology used in this section comes from the GDPR.

A Data Controller is the legal person who decides how data is collected, held and processed

A Data Processor is engaged by a data controller to process data as instructed

A Data Subject is a living individual who can be identified from the data held about them. This could be through their name or another unique identifier that has been given to them, or it

1.6.1 PRIVACY BY DESIGN AND DEFAULT

INTRAC will implement processes for the capture, storage and processing of personal data that respect the privacy of data subjects. This includes only collecting data that is required, retaining it only as long is necessary and putting appropriate physical, technological and operational security measures in place.

Note: if the data is being held for contractual or legal purposes then INTRAC will need to take legal factors into consideration when determining how long data should be retained. In general, a legal requirement would mean retaining the data for at least 6 years.

1.6.2 WE WILL BE TRANSPARENT ABOUT THE DATA WE HOLD

If INTRAC is the data controller:

- We will ensure data subjects receive a clear statement covering the data we hold and what we will be using it for.
- We will ensure that we do not collect data from minors without the agreement of a guardian/parent.
- If there is a contractual/legal requirement to hold the data we will ensure that
    - we do not collect additional data above and beyond what is needed
- If there is no contractual/legal requirement to hold the data (eg marketing data)
    - we will ensure that we have freely given consent before collecting and using the data
    - we will make it clear how they can opt out in future.
    - we will not use the data for a purpose other than that for which consent has been given
    - we will comply with any requests from the data subject to restrict processing of data

If we are the data processor, INTRAC will ensure that contract with the client makes it clear that

- They are the data controller
- INTRAC will only process the data as instructed by them.
- The data controller is responsible for ensuring that the individuals concerned are aware of the data being collected and how it is being used.

1.6.3 SECURITY OF DATA

See 1.5 above.

Additional levels of security will be required when handling sensitive personal data (and details of criminal records). Sensitive personal data is defined in Annex 2.3

For physical records appropriate security measures could include keeping records under lock and key.

For electronic records appropriate levels of additional security could include encryption, or the use of further password controls for a specific data set. Thought should also be given, particularly with data sets being processed on behalf of a client, to measures to anonymise the data before processing, ie to remove any names or combinations of traits that could link the data back to a specific individual.

Thought should also be given to locking computers and laptops whilst away from desks – eg use of windows key+L.

Failing to keep personal data secure could lead to disciplinary action on the grounds of mis-conduct.

1.6.4 DATA SUBJECT ACCESS REQUESTS

INTRAC will comply with the GDPR.

Data subjects have the right to access data held about them. There are a few exceptions to this in the GDPR but these are unlikely to apply to INTRAC. There are strict time-scales for responding to these requests. No charge can be made for supplying this data.

Applications should be forwarded immediately to the Office Administrator who will record details of the request, liaise with the relevant data owners and co-ordinate responses.

See section 2.4 for further details

1.6.5 DATA CORRECTION

If data is incorrect it will be corrected as soon as technically feasible after the error comes to light.

1.6.6 RIGHT TO BE FORGOTTEN

Data subjects can also ask for their details to be removed. The right to be forgotten does not include breaking the law so would not apply if there are legal reasons for retaining the data.

Details must be removed if the grounds for holding and processing the data is not contractual/legal requirements.

If the reasons for holding and processing the data is contractual/legal the data subject should be informed

- That we are unable to remove the details immediately for legal reasons.
- Of the nature of the legal reason, eg contract, specific legal requirements,
- If/when that legal obligation will end.
    - For contracts this would normally be 7 years after the end of the contract.
    - If a contract is governed by the law in another Jurisdiction, then that period could be different.

1.6.7 DATA PORTABILITY

Where possible we will make a data subject's data available electronically should they wish to transfer their data to another organisation.

1.6.8 SECURITY BREACHES AND LOSS OF DATA

Incidents that have or may have resulted in a security breach must be reported to the FAD (copy to the Office Manager) immediately. See 2.5.

The FAD will review the breach and assess the likely impact on data subjects in consultation with the relevant data owners. The incident and measures taken will be recorded. Where required the FAD will report details of the breach to the ICO within 72 hours.

https://ico.org.uk/for-organisations/report-a-breach/

The FAD will also ensure that data subjects are informed of the breach (either individually as a group) as appropriate as soon as possible.

1.7 We will document the data we hold

INTRAC records the data we hold in our Data Resource Register.

This resource is wider than just personal data that we hold and is an internal document. It details what data/information we hold, why we hold it, where it can be found, who is responsible for it, whether it contains personal data, access controls, how the data may be shared externally and how long it will be retained.

Data owners will review the details in the register

- Periodically (at least annually) to ensure that it is up-to-date
- Internal or external events that have a significant impact on risks of data loss/misuse. This includes any changes to systems, storage locations, major security threats, changes to relevant procedures, changes in outsourcing relations.

1.8 Linked Policies and other Documents

This policy should be read in conjunction with

- INTRAC Information Security Policy
- Privacy Notices
    - Employee Privacy Notice
    - Recruitment Privacy Notice
    - Website Privacy Notice
        - Training, additional privacy statement
        - Events, additional privacy statement

Staff can find details of the data we hold, why and how it is used, where it is stored etc in INTRAC's Data Resource Register

2 ANNEXES

2.1 Organisation Purposes for holding data

- Governance ie ensuring that we are well managed and comply with general legal requirements. This will include information about trustees and the records of meetings, but will also include details of leases, risk registers, insurances
- Personnel Management (employees, interns, volunteers).
- Job Management (clients, contracts, time, payments)
- Job Performance, ie data that we hold and process on behalf of a client in order to complete a contract, eg data about beneficiaries for impact analysis
- Training (trainees)
- Supplier Management (payment details, invoices, contracts, records of meetings)
- Marketing

2.2 Deciding who is the Data Owner

- Core: administrative and governance functions
- Consultancy
- Training
- Research

These roughly relate to the teams within INTRAC and will generally determine who is responsible for the data

2.3 Sensitive Personal Data

- racial or ethnic origin,
- political opinions,
- religious or philosophical beliefs, or trade union membership,
- genetic data,
- biometric data for the purpose of uniquely identifying a natural person,
- data concerning health
- data concerning a natural person's sex life or sexual orientation

2.4 Data Subject Requests

If a data subject asks for details of data we hold on them, or for correction or deletion of information we hold, the request should be forwarded to the Office Admin Manager as soon as possible.
Data Subjects also have the right to obtain copies of data we hold electronically in a structured and machine readable way so they can share it with other data controllers (eg to ease moving from one service supplier to another). This is unlikely to apply in the case of INTRAC but any requests should also be forwarded to the Office Admin Manager.

The Office Admin Manager will

- log the request,
- record measures taken to confirm identity of the data subject
- in the rare event that it is deemed inappropriate to respond to the request, ensure that the data subject is informed of the reasons and their right to lodge a complaint with the ICO
- act as liaison between different data controllers,
- ensure appropriate documentation of progress, response and any further steps (such as correction of data).

INTRAC will respond to the request within one month. In the exceptional event that this is not possible the data subject will be informed of the delay and the reasons for it. The maximum further delay allowed is 2 months.

INTRAC will not charge for providing the information requested.

2.5 Data Breaches

2.5.1 WHAT IS A DATA BREACH

A data breach is an unauthorised release of secure or private information.

This could be the result of an intentional act, such as a cybercrime involving someone hacking into our systems.

It could also be the result of an unintentional act, such as

- Losing a lap-top or a USB
- Leaving a lap-top or USB unattended in a public location
- Emailing the wrong person
- Losing or leaving paperwork unattended

Whilst breaches are a greater risk in a public location a breach could also occur in the office.

- If you are processing or connected to a drive that contains sensitive information you should ensure your computer is locked when you are not using it.

2.5.2 MINIMISING RISKS FROM A DATA BREACH

The risks from unintended release must be minimised by

- Use of secure passwords and encryption on lap-tops and USB
- Use of passwords to control access to locations containing personal data
- Use of secure facilities for sharing data, eg requiring passwords or tokens
- Keeping hard copies of sensitive data (including but not limited to personal data) under lock and key