D&S IFCA Data Protection Policy

Master Document

(Linked to Other Policy & Standards)

Revised for the introduction of GDPR regulations

April 2019

Contents

Edition	Date	Comments
NJT 01	May 2018	Revised for the introduction of GDPR
NJT 02	14th December 2018	Reviewed and refined
NJT 03	3rd April 2019	Reviewed and refined

1. Introduction and overview

General Data Protection Regulation (GDPR) came into effect on 25th May 2018. GDPR is a European Union piece of legislation and, regardless of Brexit, applies to both controllers and processors of personal data.

Key considerations:

- D&S IFCA must have a lawful basis in order to process personal data. The term "processing is necessary" is not sufficient if D&S IFCA can achieve the same purpose without the processing.
- Documenting and qualifying actions or process is a key requirement for Data Protection
- Privacy notices should include the lawful basis for processing as well as the purposes of processing

This overarching policy has been created to provide a broad understanding of D&S IFCA's responsibilities in regard to Data Protection. This policy is linked to others and this is detailed within this document.

Supplementary guidance notes on Data Protection standards have been provided to D&S IFCA and re-modelled so they are fit for purpose. These guidance documents provide detail on the D&S IFCA's standards in regard to each aspect of Data Protection. They are all available on the D&S IFCA shared server (staff access) and are also either posted on the D&S IFCA website or are available by contacting D&S IFCA.

2. What is Data Protection?

GDPR has built upon the principles established in the Data Protection Act 1998. Principles have been modified but largely address the same issues considered in the Data Protection Act.

GDPR applies to 'personal data' meaning any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier.

The GDPR applies to both automated personal data and to manual filing systems where personal data are accessible according to specific criteria. This could include chronologically ordered sets of manual records containing personal data.

Personal data that has been pseudonymised – e.g. key-coded – can fall within the scope of the GDPR depending on how difficult it is to attribute the pseudonym to a particular individual.

Data protection applies to personal information that is held by the Authority about living, identifiable individuals. It may be automatically processed, such as on a computer, recording device or closed-circuit TV system or on paper such as hand-written meeting notes stored in a folder.

Key GDPR Principles

1. Data processed lawfully, fairly and in a transparent manner ('lawfulness, fairness and transparency')

   (The inclusion of transparency is a new provision for GDPR – It is now a core principle)

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

   (GDPR permits further processing for public interest and/or scientific purposes)

3. Data is adequate, relevant and limited to what is necessary in relation to the purposes for which they were processed

   (D&S IFCA Document rationale and detail in the Data Protection Register)

4. Data is accurate and, where necessary, kept up to date ('accuracy')

   (DPA required accuracy and GDPR maintains these standards but includes "reasonableness". Inaccurate data should be corrected or erased without delay

5. Data not to be kept longer than is necessary for the purpose ('storage limitation')

   (Data can be held if it is being processed for archiving purposes in the public interest or scientific purposes)

6. Data to be 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."

   (Technical and organisational measures are required to be put into place to protect against the risks identified in relation to personal data – "integrity and confidentiality")

3. Key issues

- D&S IFCA must have a lawful basis in order to process personal data. The term "processing is necessary" is not sufficient if D&S IFCA can achieve the same purpose without the processing.
- D&S IFCA must Document and qualifying actions or process as this is a key requirement for Data Protection
- GDPR has introduced a high standard for consent. Positive consent is required and recording and managing consent is essential. Privacy notices should include the lawful basis for processing as well as the purposes of processing.

4. The Approach Taken by D&S IFCA

D&S IFCA has reviewed existing policy and standards to comply with GDPR. D&S IFCA has identified the range of data it collects and manages which does include personal data.

- Internal systems have been developed to store and process and document a range of information and assist with any audits that may take place
- The developed process has been used to identify personal data and separate it from other forms of data.

An overarching framework (The D&S IFCA Information Management System) has been implemented to enable this policy to be adhered to.

5. Data Protection Standards

This overarching Data Protection Policy introduced by D&S IFCA to manage, store, record and protect personal data is linked to other policies and standards which includes:

- **Privacy Policy**
- **Information Management System**
- **Data Protection Register**
- **D&S IFCA Technology Policy**
- **Standards obtaining personal information**
- **Standards on managing personal information**
- **Standards on disclosing and information sharing**
- **Standards on individuals' rights**
- **Standards on information security**
- **Standards on ensuring security in procurement**
- **Standards on the privacy and electronics regulations**

6. How does the Data Protection Act affect you?

GDPR applies to anyone in the Authority who has access to, uses or passes on personal information in their day-to-day work.

Breaches of principle may result in the Authority facing investigation, monetary penalties, being publicly named-and-shamed, and loss of trust from our stakeholders.

It is a criminal offence to:

- Obtain or disclose personal information without the Authority's authorisation or consent
- Alter, deface, block, erase, destroy or conceal any information that has been requested, when providing information in response to a subject access request.
- Force someone to make a subject access request to find out if they have a criminal record, for employment or service provision vetting purposes.

This Policy is supported by senior management and commits the Authority to providing the necessary resources to ensure that this Policy's goals can be achieved.

The Authority supports the objectives of GDPR and aims to make every effort to ensure:

- Personal information is well-managed, held securely and that the rights and freedoms of individuals are safeguarded.
- Data protection is integrated into the Authority's working practices and information systems from the moment information is collected or received through to its destruction.
- D&S IFCA have effective standards, procedures, employee reporting and training in place to ensure this Policy works in practice.
- We have in place the necessary staffing, management structure and mechanisms in place so that Data Protection compliance is well–managed.
- Compliance with the Principles is maintained.
- D&S IFCA are committed to maintaining the best possible security and confidentiality of all personal information held on our computers, information systems and on paper, and expect our employees and members to comply fully with this Policy and Standards.
- The requirement to comply with GDPR will be included in all contractual agreements, where personal information is disclosed to our service providers or anyone else acting as our agent (data processors).
- Procedures that describe the arrangements and processes for the implementation of this Policy will be available on the Authority's shared drive.

7. Responsibilities

The Data Protection Officer reports to the Chief Officer who will make any necessary recommendations to the Authority:

- Ensuring the objectives of GDPR and related legislation are achieved and assisting the Authority with its compliance and maintaining standards of good practice.
- Providing advice to the Authority for the resolution of queries and maintaining the accuracy of the Authority's register entry and keeping it up to date.
- Managing Data Protection procedures, policy, standards and documentation.
- Arranging training provision for relevant employees and members (including temporary employees and volunteers, where appropriate).
- Constructing and reviewing compliance monitoring programmes; ensuring their completion and reporting findings.

8. Responsibilities of employees and members of the Authority

Everyone who creates receives uses and discloses personal information has responsibilities under the GDPR regulations, this Policy, and the Authority's Standards. Confirmation will be provided that they have read and received them and agree to maintain the confidentiality and security of personal information.

It is the responsibility of managers to ensure that anyone who is sub-contracted or employed on a temporary or voluntary basis are made aware of this policy, standards, relevant supporting procedures, receive appropriate training, and sign up to confidentiality agreements.

Where personal data are disclosed to our service providers or anyone else acting on our behalf, we will ensure that there is a written contract in place that includes the requirement for them to comply with the GDPR regulations (in particular Principle 7 - Security).

Elected Members and Statutory Members are required to comply with the D&S IFCA Data Protection requirements

9. Contravention of the D&S IFCA Data Protection Policy

Disciplinary action, including dismissal, may be taken against any employee or member who contravenes this Data Protection Policy and supporting standards and procedures.

If it is suspected that this Policy is not being complied with or if an intentional breach of the GDPR Data Protection Principles, undertaking, or criminal offence has taken place under the Act, the Data Protection Officer shall have full authority to take such immediate steps as considered necessary, in conjunction with the Devon Audit Partnership.

Both individual employees and the Authority may be liable for prosecution under the GDPR regulations. There are a number of offences, which include:

- Unauthorised obtaining and disclosing information without the authority or consent of Devon & Severn Inshore Fisheries Authority.
- The procurement, sale, and offering for sale of personal information.
- Forcing someone to make a subject access request to find out their criminal or other background. The Disclosure Barring Service is the correct vehicle for criminal checks.
- Non-compliance with an Enforcement or Information Notice and obstructing a warrant from the Information Commissioner's Office (for example to search the premises).
- Failure to notify, not keeping a register entry or registered address up to date.
- As we are a public authority under the Freedom of Information Act it is a criminal offence, when providing subject access request information, to alter, deface, block, erase, destroy or conceal any information that the requester is entitled to.

Penalties include monetary penalties which must be paid by our organisation for a serious breach of principle to the Information Commissioner (which can be tens of thousands of pounds). Also, if found guilty of an offence (for example for unauthorised disclosure) employees can be sentenced to a fine of up to £5,000 or more, (if the case is taken to Crown Court).

The Authority (and employees) can also face civil action separately through the courts for compensation claims.

10. Monitoring, Review and Further Information

Compliance with the Data Protection Policy and Standards will be monitored by the Chief Officer (with assistance from outsourced services) and reviewed annually. Audits may take place to assess the effectiveness of policies, procedures and levels of employee awareness.

A Policy and Standards Receipt Form will be circulated to staff and Authority members to confirm that the information has been understood.

This Data Protection Policy has been authorised by the Acting Chief Officer of Devon and Severn Inshore Fisheries and Conservation Authority.

Name: Mat Mander

Signed …… Date ……

For enquiries relating to this Policy and standards, contact either the Data Protection Officer or the Chief Officer/Acting Chief Officer.