Data Security Policy

Date issued: 15/09/2020

This document sets out the Authority's policy on data security

Introduction

The Authority was established under statute[1] to manage inshore fishing activity and the impact of such activity on the environment[2] within its district, including the development and implementation of management measures and the enforcement of compliance with such in addition to national and international fisheries legislation.

The Authority collects, processes and stores data to carry out its statuary functions. Use of data is crucial to making effective management and enforcement decisions and this is reflected in our related duty to collect such data as is required to meet our statutory functions[3] and in Defra guidance to Inshore Fisheries and Conservation Authorities (IFCAs) which sets out the use of 'evidence based marine management'[4].

The need for a data security policy

The Authority processes personal data including special category and criminal offence data. To ensure that the appropriate technological and organisations measures are in place to use this data securely, The Authority has assessed the risks of processing this data[5]. These assessments highlight the risks to data security and the mitigation required. Mitigation highlighted from the assessments is referred to in this document as policy to implement it across the organisations.

Principles

This policy is based on the following principles:

- The Authority will comply with all relevant legislation and in particular, the General Data Protection Regulations (GDPR) and the Data Protection Act 2018 (DPA).

- Ensuring compliance with data protection legislation is a corporate responsibility requiring the active involvement of all staff at all levels of the organisation.

- We will ensure data protection and data security by design by adhering to best practice with reference to HMG's Security Policy Framework.

[1] Section 149 and 150 Marine and Coastal Access Act 2009
[2] Sections 153 and 154 Marine and Coastal Access Act 2009
[3] Section175(1) Marine and Coastal Access Act 2009 (c.23)
[4] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/182346/2011-ifca-guide-marinemanage.pdf
[5] The Authority's Data Security Risk Assessment and the Data Protection Impact Assessment.

- The Authority will seek to improve practices by regularly reviewing the data security needs of the organisation and revise them as necessary.

- When reviewing our needs, we consider state of the art technology and cost implications of security measures in the context of the risk posed by processing.

- In determining the most effective data security measures, the Authority will ensure confidentiality, integrity and availability.

Data security
The following measures will ensure data security.

Governance

- A Data Protection Officer (DPO) is assigned, who has responsibility for ensuring the implementation of the Data Security Policy.

- Feedback and review, including as a result of any complaints or data breaches as well as through investigation of best practice is the responsibility of the DPO.

- Personal data will not be shared without the permission of the DPO.

- The DPO will be responsible for investigating, reporting of a data breach (where necessary) and implementing any remedial action.

Structure

- The Authority will have in place data holding systems which will ensure data security by design in the following ways:
    - Data minimisations – the Authority will only collect that data which is needed to fulfil a stated purpose;
    - Data anonymisation – the Authority will store personal data separately from related non-personal data.

- The Authority will maintain an audit trail of the use of personal data including how it was used.

Staff
The Authority will ensure that all employees are aware of data security and are able to practice safe processing to avoid data security issues. This will include:

- Appropriate induction process to ensure understanding of the organisations stated purpose of data and not using beyond that purpose

- Vetting (Baseline Personnel Security Standards) undertaken for all employees who have access to Official information
- Contractual obligation for confidentiality
- Relevant data security and data protection training
- Data being shared on a ‘need to know’ basis

Cyber security

The Authority has in place up to date and robust cyber security measures including the following:

- Intercepting proxies which block malicious websites;
- Internet security gateways;
- Use of safe browsing lists;
- Mail and spam filtering enabled;
- Maintenance of up to date protective software (anti-malware and anti-virus software);
- Regular software updates;
- Robust backup system;
- Double encryption on laptops;
- Encrypted, work issued smart phones with no remote access to IT system;
- Network firewalls;
- Regular software updates.

Data sharing

The Authority will only share data in accordance with associated privacy notices or where the law provides for such sharing. When the Authority shares information;

- It will be shared using a secure means;
- Only in accordance with stated purpose or the law

Data breaches

- Data breaches will be reported to the Information Commissioners Office, as required, within 72 hours of the breach being detected

- Where the data breach is likely to result in high risk of adversely affecting the rights and freedoms of the data subject, the data subject will be notified without undue delay.

- The Authority will log the use of all personal data so as to facilitate the detection of data breaches.

- Any data breaches, or suspected data breaches, must be reported to the DPO immediately.

Complaints

- Individuals concerned about any aspect of the Authority's data security or management may raise their concerns with the DPO in the first instance.

- If the concern cannot be resolved, a formal complaint may be submitted via the Authority's complaint procedure.

- An individual may wish to raise a complaint with the Information Commissioners Office at any time. To contact the Information Commissioners Office, visit their website at the following link: https://ico.org.uk/make-a-complaint/

Review

The Data security policy will be reviewed continually and as a result of any significant changes to the Authority's practices, the Data Security Risk Assessment or Data Protection Impact Assessments.

This policy will be reviewed no later than two years after the last issue date.