Safeguards Policy: General Processing of Criminal Offence Data

Date issued: 01/09/2020

This Policy covers the processing of criminal offence data.

Scope of this document

The General Data Protection Regulations (GDPR) requires that data is used fairly and responsibly and the Data Protection Act 2018 (DPA) sets out additional conditions for the use of personal data relating to the alleged commission of offences or proceedings for an offence committed or alleged to have been committed, including sentencing (collectively known as 'criminal offence data')[1]. These safeguards include reference to conditions which must be met in order to undertake such processing including the production of an appropriate policy document.

The following data sets are processed in relation to criminal offence data:

- Compliance logs (including formal and informal sanctions);
- Data shared by the Marine Management Organisation (MMO) under the associated Data Sharing Agreement (DSA).

Conditions for processing criminal offence data

The Authority processes criminal offence data under Article 10 of the GDPR and for statutory purposes in relations our functions as a regulator as described in paragraph 6(2) or Schedule 1 of the DPA.

This document is, for the purposes of fulfilling the conditions of processing data relating to criminal offences in Schedule 1 of the DPA, the appropriate policy document.

The types of processing we do include compiling logs of formal and informal enforcement action and considering criminal offence data to determine access to services (including permits to fish).

Compliance with data protection principles

In processing criminal offence data, the Authority will ensure compliance with the data protection principles as follows:

Principle 1 - requirement that processing be lawful and fair

The lawful basis for processing criminal offence data is for **public task** in our capacity as a regulator.

Our processing for the purposes of substantial public interest is necessary for the exercise our statutory duties under the s.153 and s.154 of the Marine and Coastal Access Act 2009 (MaCAA). The Authority acts as regulator for the

[1] As defined in s.11(2) DPA

protection of inshore fishers and marine environment from the exploitation of fisheries resources.

Criminal offence data is shared with the Marine Management Organisation (MMO) under the Data Sharing Agreement in order to fulfil our obligation under s.174 of MaCAA and for the purposes of effective fisheries management. Data is shared with other law enforcement bodies (including the Police, Environment Agency and Boarder Force) only in relation law enforcement purposes[2].

Principle 2 - requirement that purposes of processing be specified, explicit and legitimate

The Authority processes criminal offence data for the purposes set out above when the processing is necessary to fulfil statutory duties. This relates to the protection of inshore fisheries and marine environment.

Sharing of the data is limited to law enforcement purposes and to the provisions of the Data Sharing Agreement with the MMO. All sharing of criminal offence data is logged, and we will documents that they are authorised by law to process the data.

The Authority will not use criminal offence data except for the purposes for which it is collected.

Principle 3 - requirement that personal data be adequate, relevant and not excessive (data minimisation)

Criminal offence data is collected only in relation to persons undertaking activities relevant or ancillary to fishing activity and which fall within the Authority's jurisdiction.

In the case of fisheries offences, this may include offences for which the Authority does not have powers to enforce but which are relevant with respect of being within the scope of our duties and / or the stated purpose of the processing.

Where criminal offence data is provided to the Authority, which is not relevant for the stated purpose, the Authority will erase the data.

Principle 4 - requirement that personal data be accurate and kept up to date

The Authority will take every reasonable step to ensure that criminal offence data is correct and up to date. Where we determine that information is inaccurate or out of date, we will seek to erase or rectify the data without delay. However, a request for erasure or rectification will be considered only in the context of the lawful basis for processing being public task and where such a request is refused, the reasons will be documented.

[2] Safeguards Policy – Sensitive processing for law enforcement purposes

Principle 5 - requirement that personal data be kept for no longer than is necessary

Our retention period for criminal activity data is 6 years after which time its retention is reviewed. This retention period is based on the Limitations Act 1980. A review will include consideration of any business needs to retain the information and data subjects will be notified in the event the data is not erased.

Principle 6 - 'appropriate security'

Electronic information is processed within our secure network. Hard copy information is processed within our secure premises.

Our electronic systems and physical storage have appropriate access controls and security measures as detailed in the Authority's Data Security Policy.

Policy Review

This policy will be reviewed annually and more frequently as required.

Schedule 1 –

Dataset	Lawful basis	General processing or law enforcement purposes?	Description of data collection and use	Consideration of GDPR and DPA conditions for processing
Seaborne and shore-based compliance inspections	**Public task** – The Authority processes compliance inspections data to fulfil statutory duties at s.153 and s.154 (main duties) of the Marine and coastal access act and s.174 (duty of co-operation) in relation to sharing with the Marine Management Organisation.	**Both**	Data is collected during seaborne and shore-based compliance inspections. Data includes personal data (personal and vessel name(s), contact details, location and activity data), special category data (race, nationality and ethnic origin) and Criminal Offence data (where an offence is detected). Personal data is used to inform compliance activities, to facilitate contact with persons so inspected and to inform effective investigations of criminal activity or suspected criminal, activity. Data is subject to sharing with MMO and other enforcement bodies for law enforcement purposes.	**SC general processing** meets GDPR Article 9 conditions – Article 9(2)(g) the processing is necessary to ensure compliance with Equality Act (2000) and in particular s.149(1)(a) and (2). The SC data will be used to have due regard of eliminating discrimination, harassment, victimisation and any other conduct that is prohibited by or under the Act. **SC general processing** meets DPA s.10 and Schedule 1 conditions **–** SC data meets the conditions of paragraph 8 to the extent that it relates to a specified category of personal data (being personal data revealing racial or ethnic origin) and is necessary to monitor and evidencing compliance with the Equality Act (2000) and in particular s.149(1)(a) and (2). **SC data processing for law enforcement purposes** meets the data protection principles set out in Part 3 of the DPA including the first data principle as follows: The data is strictly necessary for law enforcement purposes to enable to successful identification of suspects and secure successful prosecution. Paragraph 2 of Schedule 8 of the DPA is satisfied as the information is used in the administration of justice and an appropriate policy document is in place at the time of processing (this document). **CO data processing for law enforcement purposes** meets GDPR Article 10 conditions – data is used for law enforcement purposes and in an official capacity under investigative powers under the Marine and Coastal Access Act 2009. Paragraph 2 of Schedule 8 of the DPA is satisfied as the information is used in the administration of justice and an appropriate policy document is in place at the time of processing.

Dataset	Lawful basis	General processing or law enforcement purposes?	Description of data collection and use	Consideration of GDPR and DPA conditions for processing
Compliance logs	**Public task** – The Authority processes compliance inspections data and outcomes of enforcement activity to fulfil statutory duties at s.153 and s.154 (main duties) of the Marine and coastal access act and s.174 (duty of co-operation) in relation to sharing with the Marine Management Organisation.	**Law enforcement purposes**	Includes record of the outcomes of criminal investigations, including verbal warnings, written warnings, Financial Administrative Penalties and prosecutions at Court. Data includes personal details, details relating to the circumstances of the offence and criminal offence data (i.e. charges etc.). Data is used to inform compliance activities, to inform decisions relating to enforcement actions (i.e. in the context of previous offences) the issuing of permits[3] and to facilitate contact with persons so involved. Data is subject to sharing with MMO and other enforcement bodies for law enforcement purposes.	**CO data processing for law enforcement purposes** meets GDPR Article 10 conditions – data is used for law enforcement purposes and in an official capacity under investigative powers under the Marine and Coastal Access Act 2009. Paragraph 2 of Schedule 8 of the DPA is satisfied as the information is used in the administration of justice and an appropriate policy document is in place at the time of processing.
Intelligence	**Public task** – The Authority processes intelligence to fulfil statutory duties at s.153 and s.154 (main duties) of the Marine and coastal access act and s.174 (duty of co-operation) in relation to sharing	**Law Enforcement purposes**	Data is collected from sources and includes personal data of sources and the subject involved in suspected criminal activities, criminal offence data and special category data (including race and ethnic origin data).	**CO data processing for law enforcement purposes** meets GDPR Article 10 conditions – data is used for law enforcement purposes and in an official capacity under investigative powers under the Marine and Coastal Access Act 2009. Paragraph 2 of Schedule 8 of the DPA is satisfied as the information is used in the administration of justice and an appropriate policy document is in place at the time of processing.

[3] Eastern IFCA permits to fish within certain fisheries include eligibility criteria which includes reference to previous offences.

Dataset	Lawful basis	General processing or law enforcement purposes?	Description of data collection and use	Consideration of GDPR and DPA conditions for processing
	with the Marine Management Organisation.			
Operational Planning (in relation to Tactical Coordination Group data)	**Public task** – The Authority processes information from various sources to inform compliance activity to fulfil statutory duties at s.153 and s.154 (main duties) of the Marine and coastal access act and s.174 (duty of co-operation) in relation to sharing with the Marine Management Organisation.	**Law Enforcement purposes**	Data from various sources is compiled and information is graded to inform compliance activities on a risk-based approach. Includes personal data (personal and vessel name(s), contact details, location and activity data), special category data (race, nationality and ethnic origin) and Criminal Offence data.	**CO data processing for law enforcement purposes** meets GDPR Article 10 conditions – data is used for law enforcement purposes and in an official capacity under investigative powers under the Marine and Coastal Access Act 2009. Paragraph 2 of Schedule 8 of the DPA is satisfied as the information is used in the administration of justice and an appropriate policy document is in place at the time of processing.