Safeguarding policy – sensitive processing for law enforcement purposes

Date issued: 01/09/2020

This Policy covers the processing of special category data for law enforcement purposes.

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 safeguards to protect the rights of individuals in relation to processing special category data (i.e. sensitive processing[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.

Special Category data includes the following:

- the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership;
- the processing of genetic data, or of biometric data, for the purpose of uniquely identifying an individual;
- the processing of data concerning health;
- the processing of data concerning an individual's sex life or sexual orientation.

The following data sets include special category data and are processed for law enforcement purposes:

- Seaborne and shore-based compliance inspections;
- Intelligence;
- Data shared by the Marine Management Organisation (MMO) under the associated Data Sharing Agreement (DSA).

Conditions for processing special category data for law enforcement purposes

The Authority is a competent authority under s.30(b) if the DPA inasmuch as we have statutory functions for law enforcement purposes as set out in s.31 of the DPA which include the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties. The Authority has a law enforcement remit under the Marine and Coastal Access Act 2009 (MaCAA).

[1] As defined in s.35(8) DPA

The Authority will ordinarily rely on a Schedule 8 (of the DPA) condition for processing special category data for law enforcement purposes unless relying on consent of the data subject. The Authority will only carry out sensitive processing in these circumstances. This includes processing under the DSA (i.e. sharing with the MMO).

The relevant schedule 8 conditions are paragraph 1 (statutory purposes) and 2 (administration of justice).

For the purpose of fulfilling s.42 of the DPA, this document is the appropriate policy document.

Accountability principle

The authority has put in place appropriate measures to ensure accountability as follows:

- Appointing a Data Protection Officer who reports directly to the CEO;
- Documenting data processing procedures (and specifically a data sharing log in relation to data processed under the DSA);
- Undertaking a Data Security Risk Assessment and Data Protection Impact Assessment to inform our ways of working and a Data Security Policy;
- Implementing security measures including a robust IT security system, staff training and monitoring.

Compliance with data protection principles

In processing sensitive data for law enforcement purposes, The Authority will ensure compliance with the data protection principles as follows:

Principle 1 - requirement that processing be lawful and fair

The Authority will only collect special category data with the consent of the data subject or where it is necessary for law enforcement purposes.

Where collected for law enforcement purposes, this information is necessary to fulfil our statutory functions as a regulator (under MaCAA) and to enable the effective administration of justice with regards to the prevention and detection of crime.

When collected on the consent of the data subject, the consent will unambiguous, given as an affirmative action and be recorded as the condition for processing.

Principle 2 - requirement that purposes of processing be specified, explicit and legitimate (purpose limitation)

The Authority undertakes sensitive processing for the purposes of the prevention, investigation, detection or prosecution of criminal activities or the execution of criminal penalties (as per s.31 DPA). The Authority has powers in accordance with powers conferred by virtue of s.166(3) of the Marine and Coastal Access Act 2009 for the purpose of enforcing the legislation set out in the following:

- section 166(1) of the Marine and Coastal Access Act 2009 (c.23);
- the schedule to the Sea Fishing (Regulations) 2018 (SI/ 849/18)

The Authority will only use special category data collected for law enforcement purposes where we are permitted by law to do so.

Special category data will be shared with the MMO under the DSA. Sensitive data may also be shared with other law enforcement bodies (including the Police, Environment Agency and Border Force) only in relation law enforcement purposes.

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

The Authority only collects and processes special category data for law enforcement purposes where necessary and not systematically.

Collection of special category data is considered proportionate because it enables effective law enforcement, particularly in relation to identifying persons or the intentions of persons, undertaking criminal activities or suspected of undertaking criminal activities.

Where the Authority has collected or obtained any special category data which is not relevant for the stated purposes, it will be erased without delay.

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

The Authority will take every reasonable step to ensure that special category 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.

The Authority will also identify any special category where the accuracy is unknown or suspected to be false and its use will reflect this grading.

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

Where no proceedings are being taken against any person for whom sensitive data has been collected, the information will be retained for no more than two

years after it has been collected after which time the data will be anonymised such that it does not constitute personal data.

Where proceedings are taken, the information will be retained for a period of six years after any such proceedings have concluded, at which point it will be 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.