SUSSEX INSHORE FISHERIES & CONSERVATION AUTHORITY
DATA PROTECTION POLICY

Context

Sussex Inshore Fisheries and Conservation Authority is required to process relevant personal data regarding members of staff, volunteers, board members and a range of marine users.

From 25 May 2018, the General Data Protection Regulations (GDPR) comes into force, building upon existing data protection legislation. The GDPR will apply regardless of the UK's exit from the European Union.

This policy sets out the Authority's commitment to protecting personal data. For clarity, personal information means any data or information, in paper or digital format, relating to a living individual.

Data Protection Principles

Sussex Inshore Fisheries and Conservation Authority complies with the General Data Protection principles and ensures that personal data is:

- Processed fairly and lawfully and in a transparent manner
- Obtained for one or more specified, explicit and lawful purposes
- Adequate, relevant and only limited to what is required
- Accurate and where necessary kept up to date
- Not kept in a form which permits identification of data subjects for longer than is necessary
- Processed in accordance with the rights of data subjects
- Processed in a manner that ensures appropriate security of the personal data.

Anyone who processes data on behalf of the Authority, including staff, volunteers, contractors or others who process or use any personal information must ensure that they follow these principles at all times.

General requirements

Significant requirements under the DPA and GDPR are:

- Personal data should only be accessed by those who need to for work purposes
- Personal data should not be divulged or discussed except when performing normal work duties
- Personal data must be kept safe and secure at all times, including at the office, public areas, home or in transit
- Personal data should be regularly reviewed and updated
- Queries about data protection, internal and external must be dealt with promptly.

Sensitive personal information

There are more stringent measures in place to protect sensitive personal data.

Sensitive personal data means personal data consisting of information as to

- the racial or ethnic origin of the data subject,
- political opinions, religious beliefs or other beliefs of a similar nature,
- membership of a trade union,
- physical or mental health or condition,
- sexual life
- the commission or alleged commission of any offence, or any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings.

Data of this nature is subject to additional protection because the presumption is that information about these matters could be used in a discriminatory way and is likely to be of a private nature.

The majority of the Authority's work should be carried out without the need to collect sensitive personal information. In the event that such information is required to perform a legitimate business function, the collection should be limited to only what is necessary and processed only for that function and be stored securely.

Information Sharing

Personal data may need to be shared with other organisations in order to deliver services or perform our duties. This can only be done where we have permission or there is legal obligation for us to share. The Authority has powers laid down in part 6 of the Marine and Coastal Access Act 2009. This includes provisions within section 156 that may require individuals and organisations to apply for and pay Byelaw permit fees. It is a condition of permit applications that the vessel and owner details are passed to the Authority.

For all other business functions, there should be an information-sharing agreement in place which sets out the reasons for the collection and processing of the data.

Personal data can be shared within the Authority or with other third parties where there is an established purpose

One of the key changes within the GDPR is data protection by default and design, Data Sharing Agreements should be completed when setting up 'on-going' or 'routine' information sharing arrangements with third parties.

However, they are not needed when information is shared on a 'one-off' basis in 'exceptional circumstances' (i.e. in conditions of real urgency). In these cases, a record of the decision and the reasons for sharing information should be kept.

All Data Sharing Agreements must be signed off by the Chief Officer and Data Protection Officer who will keep a register of all Data Sharing Agreements.

Privacy Impact Assessments (PIAs)

PIAs will be completed in these situations to help identify and minimise risks to individuals and must be completed in the following situations that involve personal data:

- At the beginning of a new project or when implementing a new system
- Before entering a data sharing agreement
- When major changes are introduced into a system or process

Subject Access Requests (SARs)

The Authority recognises that access to personal data held about an individual is a fundamental right provided in the GDPR and will ensure that all requests from individuals to access their personal data are dealt with as quickly as possible and within the timescales allowed in the legislation.

Individuals will be expected to submit SARs in writing and provide any necessary proof of identification as part of the request. No charge can be made to provide this data.

Of prime importance is that information is not given out recklessly. Anybody requiring data should be requested to write to the office detailing their request. We can offer to forward any correspondence, or information, should our records show that we have the necessary data.

Complaints

Anyone who feels that the Authority has broken the law in any way can complain. Examples of this are when they think their information has not been obtained fairly, it has not been handled securely or they have asked for a copy of their information and they are not happy with the Authority's response.

Individuals who consider that data is inaccurate or out of date may also request, in writing, that the information be corrected or erased. They will receive a written response indicating whether or not the Authority agrees and if so, the action to be taken.

Individuals can also ask the Authority to stop handling their personal information if they think this will cause them harm or distress. This is not always possible but in such circumstances the request will be reviewed on a case by case basis.

Data Protection Act complaints will be dealt with in accordance with the existing complaints procedure.

Non-Compliance

One of the major changes implemented through the GDPR is the level of fine which can be levied on an organisation in cases of non-compliance or data breaches. The administrative fines are discretionary rather than mandatory; they must be imposed on a case-by-case basis and must be "effective, proportionate and dissuasive". In the most serious of cases the fine can be up to 20,000,000 Euros or 4% of annual turnover, whichever is the greatest.

Serious breaches of this policy caused by deliberate, negligent or reckless behaviour could result in disciplinary action and may even lead to criminal prosecution.

Role of the Data Protection Officer

The Authority has designated Ms R Griffin (Committee Manager) to act as Data Protection Officer. Any query relating to the implementation within the Authority, of the Data Protection Act and Subject Access Requests under section 7 of the Act should be referred to the Senior Management Team.

The Data Protection Officer will be responsible for ensuring that the Authority's entry on to the ICO register is kept up to date and all fees to the ICO are paid in time.