GENERAL DATA PROTECTION REGULATION - GDPR

COMPLIANCE FOR DISTRICT SALMON FISHERY BOARDS

INTRODUCTION

This document is a brief guide to assist District Salmon Fishery Boards with compliance with GDPR. GDPR is a new EU regulation that comes into force on 25 May 2018 and together with the Data Protection Act 2018 will replace the existing Data Protection Act 1998. It has come about as a result of the need for consistency across the EU in applying data protection law. The general aim is to strengthen the rules around the protection of personal data and to make organisations more accountable and transparent for their handling of data.

The Information Commissioner's Office (ICO) is responsible for the observance and implementation of the Regulation and the new Act and they have information and advice on their website https://ico.org.uk. There is a phone service available to assist small organisations prepare for GDPR (0303 123 1113). Further information may be found in the ICO's 'Guide to GDPR' and 'Preparing for GDPR 12 steps to take now'. We strongly recommend that Boards consult the ICO guidance as it is not possible to set out the full scope of the GDPR within this guide.

The regulation engages for those organisations that choose to collect and hold personal data. Personal data is data that allows a living individual to be identified. It requires those who hold personal data to comply with the following six principles for the handling of personal data: -

- fairly and lawfully processed
- processed for limited purposes
- adequate and relevant and limited to what is necessary
- accurate and where necessary up to date
- not kept in a way that people can be identified from it for longer than is necessary
- processed in a way that ensures appropriate security

Boards hold personal data including the names and addresses of proprietors but also other fishery related interests in their districts. Boards are responsible for determining the purposes and means of processing (in our case storing) personal data; they will therefore be Data Controllers for the purposes of GDPR.

ADVICE TO BOARDS TO ASSIST WITH COMPLIANCE

1. Appoint an officer responsible for compliance with the law.

2. Carry out an information audit to ensure that the data you hold is GDPR compliant (see annex 1).

3. Draft a Board Data Handling Policy and ensure it is implemented (see annex 2). This will provide evidence that you have the processes in place to ensure ongoing compliance with GDPR.

4. Ensure that the Board displays a Privacy Statement on its website and that attention is drawn to it in all communications, if possible. The statement should be updated as necessary from time to time and should be drafted to meet the needs of each Board individually. Because Boards will not be sharing data as a matter of course we would envisage that a Board Privacy Statement may simply state:-

"The [xxx] Board holds certain personal data for the purpose of fulfilling its statutory responsibilities under the Salmon and Freshwater Fisheries (Consolidation) (Scotland) Act 2003, which includes the protection of salmon fisheries within its district. We will only pass personal data to third parties without the consent of the data subject where it is necessary for us to do so in support of our statutory responsibilities. Data is held subject to our Data Handling Policy. The Board's responsible officer for data is [xx] and any queries regarding this Privacy Statement should be directed at him/her."

5. There is an obligation to provide individuals with privacy information at the time any personal data is collected from them. Certain key information needs to be provided to that person including:

- board contact details
- the purpose for which the information is being held and
- the lawful basis of processing and the period for which the information will be retained.

In practice we advise that the simplest way of doing this is by having a note on all communications referring to the Board's Privacy Statement.

Annex 1

Board Data Audit

1. Data processing

GDPR requires that any information processed must be under one of six legitimate bases. These are: consent, contract, legal obligation, vital interests, public task and legitimate interests. Please see ICO guidance[1] if you wish to find out more detail on these. The Board should determine which valid lawful bases it is relying on for each data processing purpose and ensure that this distinction is reflected in the maintenance and labelling of its databases. The key bases that Boards are likely to rely on are set out below:

1.1 Public Task. The Board may process the following data necessary for it to perform its public task with respect to the protection of salmon within its district and the functioning of the Board, which duties are set out within the Salmon Act 2003. This may comprise keeping and maintaining an up to date database which includes names and addresses of: -

- fishing proprietors within the district
- mandatories of fishing proprietors
- persons associated with bailiffing activities
- other persons or groups with an interest in fisheries in the district that are relevant to the work of the Board
- other persons or businesses with an interest in fisheries out-with the district that are relevant to the work of the Board

1.2 Legitimate Interests. In practice Boards should be able to process most their data requirements on the basis of 'Public Task', however where a Board needs to process data which falls outside this, the data may be processed provided that the processor subjects it to an Legitimate Interests assessment. Such data subjects may include persons or businesses with an interest in the work of the Board in the district but not related directly to its public functions. This may include local fishery interests such as tackle shops or angling clubs, and local environmental groups with an interest in rivers. It may also include persons or businesses with an interest in fisheries outwith the district such as Fisheries Management Scotland, the Atlantic Salmon Trust, or the Angling Trust, or other environmental groups or organisations.

Data processed under this heading should be subject to a 'Legitimate Interests Assessment' (LIA). This can be broken down into three elements:

- purpose test: are we pursuing a legitimate interest?
- Necessity test: is processing necessary for that purpose?
- Balancing test: do the individual's interests override the legitimate interest?

[1] ICO Guide to GDPR p10-45

It should be considered good practice for the data officer to note compliance with the Board's accountability obligations. A tick box on the data entry may indicate that that the LIA process has been carried out.

1.3 Contract

The Board may process data where it is necessary for a contract that the Board has with the individual. For example, the Board may have a number of ongoing contracts associated with the use and maintenance of its offices and 'Contract' will be the appropriate basis to hold this information. The processing is only legitimate in so far as it is necessary for the performance of the contract. For example, if the Board uses a local electrician to rewire the office then it will be necessary to hold his details on file for so long as it has an interest under that contract. In most cases that will be no longer that the limitation period for breach of contract, which is 5 years.

1.4 Consent

In any other situation the Board is required to obtain the consent of a person whose data it wishes to hold. For example, if the Board sends a newsletter to interested members of the public then it is recommended that the Board seeks consent for holding the contact details for each recipient on the circulation list. If consent is obtained then it must set out the purpose for which the information will be processed. If the purpose changes then fresh consent must be sought. A record should be kept for that consent in every case. Beyond this scenario we doubt if Boards will need to rely on consent very much, if at all, as its data processing operations should be covered by Public Task, Legitimate Interests and Contract.

2. Security

The Board should carry out an audit of the security of its data storage facilities. Security measures should be 'appropriate' to the size of the Board's network and information systems. This will encompass reviewing both physical security and cybersecurity

2.1 Physical Security

The audit should consider, the security of the premises in general, security of devices used and disposal of paper.

2.2 Cyber-security

You should consider whether your networks and information system are secure. For more information please see the ICO practical guide to cybersecurity.

Annex 2

Draft Board Data Handling Policy

Boards should consider developing a Data Handling Policy. This will provide evidence that there are procedures in place to ensure compliance with GDPR. The following may be used as a starting point for the development of such a policy:

[XXX] District Salmon Fishery Board Data Handling Policy

1. The Board has rights and duties under the Salmon and Freshwater Fisheries (Consolidation) (Scotland) Act 2003 which necessitate the processing of data. The Board accepts that it is a data controller for the purposes of the General Data Protection Regulation and that it must comply with the following six principles for the handling of personal data: -

- *fairly and lawfully processed*
- *processed for limited purposes*
- *adequate and relevant and limited to what is necessary*
- *accurate and where necessary up to date*
- *not kept in a way that people can be identified from it for longer than is necessary*
- *processed in a way that ensures appropriate security*

3. The Board's officer responsible for compliance with GDPR is [xxxx]. He/she will maintain the Board's databases in compliance with GDPR. The Board will hold [four] separate databases:

- *A Public Task database of data held necessary to uphold the Board's statutory duties*
- *A Contract database with information required in fulfilment of those contracts*
- *A Legitimate Interests database held subject to satisfaction of a 'legitimate interests' assessment[2]' (LIA assessment);*
- *Consent database, all data held under consent of the data subjects.*

4. The Board will audit its information annually to ensure that its data bases are compliant with the six principles of GDPR. In particular, the audit will ensure:

- *that data is held in compliance with the act*
- *data held is accurate*
- *that no more data is held that is necessary*
- *that data will be held only for so long as it is needed.*

[2] The LIA assessment requires that the information officer before entering the data on the Legitimate Interests database satisfies him/herself that the Board is pursuing a legitimate interest in so doing, that processing the data is necessary for that purpose and that he/she has considered whether there are any balancing personal issues that override the right of the Board to process that data (for example where that individual has particular vulnerabilities).

After each annual audit the responsible officer will note that the audit has taken place and that he/she certifies the Board's databases as being compliant with GDPR.

5. The Board will ensure that all the data held is securely stored. This will apply to physical copies of data as well as computer-based data.

6. The Board will respond within 28 days to any written request (including by e-mail) by a data subject for details of information held by the Board on them.

7. The Board will publish a Privacy notice on its website