Iascach Intíre Éireann
Inland Fisheries Ireland

Data Protection Policy

Name of Document:	IFI Data Protection Policy				
Author (s):	Fiona Mahon, Data Protection Officer				
Authorised Officer:	Dr Ciaran Byrne, Chief Executive Officer				
Description of Content:	This document outlines the policy in relation to the collection and management of personal data at IFI under the General Data Protection Regulation (GDPR).				
Approved by:	Dr Ciaran Byrne, CEO				
Date of Approval:					
Assigned review period:	2 years				
Date of next review:					
Document Code:					
This documents comprises:	TOC	Text	List of tables	Table of Figures	No. Appendices
	0	20 pages	0	0	1

Version Control Table

Version No.	Status	Authors(s)	Reviewed by	Approved by	Date of issue
V 0.1	Draft	BH Consulting/ F. Mahon (DPO)	A & R Comm	Recommended to Board	September 2018
V 1.0		BH Consulting/ F. Mahon (DPO)	A & R Comm	Feedback applied	November 2018
V 1.1	Approved	BH Consulting/ F. Mahon (DPO)	Board	Board	November 2018

TABLE OF CONTENTS

1 Introduction

This Policy sets out the obligations of Inland Fisheries Ireland ("**IFI**") an organisation whose registered office is at 3044 Lake Drive, Citywest Business Campus, Dublin D24 Y265 regarding data protection and the rights of any individual for whom IFI holds and processes personal data including staff, stakeholders, visitors, licence holders and funding scheme applicants ("**data subjects**") in respect of their personal data under EU Regulation 2016/679 General Data Protection Regulation ("**GDPR**").

GDPR is an EU regulation designed to safeguard the privacy rights of individuals in relation to the collection and processing of their personal data. It is supplementary to the Data Protection Acts of 1988 & 2003 and has been transposed into Irish law in the form of the Data Protection Act 2018. The regulation became enforceable from the 25th of May 2018.

Under GDPR "personal data" is defined as any information relating to an identified or identifiable natural person (a "data subject"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

1.1 Policy Scope

This Policy sets out IFI's obligations regarding the collection, processing, transfer, storage and disposal of personal data. The principles and procedures set out herein shall be followed at all times by IFI, its employees, agents, contractors or other parties working on behalf of IFI. Any employee found to have violated this policy may be subject to disciplinary procedures, up to and including termination of employment.

Enquiries about this Data Protection Policy should be made to:

Data Protection Officer, 3044 Lake Drive, Citywest Business Campus, Dublin D24 Y265

1.2 Definitions

Please see Appendix I for the definitions of terms used in this policy.

1.3 The Data Protection Principles

This Policy aims to ensure compliance with the GDPR. The GDPR sets out the following principles with which any party handling personal data must comply. All personal data shall be:

- Processed lawfully, fairly and in a transparent manner in relation to the data subject;
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. Further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
- Adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed;
- Accurate and, where necessary, kept up to date. Every reasonable step shall be taken to ensure that personal data that is inaccurate, having regard to the purposes for which it is processed, is erased or rectified without delay;
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed. Personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to implementation of the appropriate technical and organisational measures required by GDPR in order to safeguard the rights and freedoms of the data subject;
- Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

1.4 The Rights of Data Subjects

The GDPR sets out the following rights applicable to data subjects (please refer to the relevant sections of this policy for further details):

- The right to be informed (Section 1.11);
- The right of access (Section 1.12);
- The right to rectification (Section 1.14);
- The right to erasure (also known as the 'right to be forgotten') (Section 1.15);
- The right to restrict processing (Section 1.16);
- The right to data portability (Section 1.17);
- The right to object (Section 1.18);

1.5 Lawful, Fair and Transparent Data Processing

The GDPR seeks to ensure that personal data is processed lawfully, fairly and transparently without adversely affecting the rights of the data subject. The Regulation states that processing of personal data shall be lawful if at least one of the following applies:

- The data subject has given consent to the processing of their personal data for one or more specific purposes;

- The processing is necessary for the performance of a contract to which the data subject is a party or in order to take steps at the request of the data subject prior to entering into a contract with them;
- The processing is necessary for compliance with a legal obligation to which the data controller is subject;
- The processing is necessary to protect the vital interests of the data subject or of another natural person;
- The processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller; or
- The processing is necessary for the purposes of the legitimate interests pursued by the data controller[1] or by a third party, except where such interests are overridden by the fundamental rights and freedoms of the data subject which require protection of personal data in particular where the data subject is a child.

If the personal data in question is "special category data" (also known as "sensitive personal data") for example, data concerning the data subject's race, ethnicity, politics, religion, trade union membership, genetics, biometrics (if used for ID purposes), health, sex life or sexual orientation at least one of the following conditions must be met:

a. The data subject has given their explicit consent to the processing of such data for one or more specified purposes (unless EU or EU Member State law prohibits them from doing so);
b. The processing is necessary for the purpose of carrying out the obligations and exercising specific rights of the data controller or of the data subject in the field of employment, social security and social protection law (insofar as it is authorised by EU or EU Member State law or a collective agreement pursuant to EU Member State law which provides for appropriate safeguards for the fundamental rights and interests of the data subject);
c. The processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;
d. The data controller is a foundation, association or other non-profit body with a political, philosophical, religious or trade union aim and the processing is carried out in the course of its legitimate activities, provided that the processing relates solely to the members or former members of that body or to persons who have regular contact with it in connection with its purposes and that the personal data is not disclosed outside the body without the consent of the data subjects;
e. The processing relates to personal data which is clearly made public by the data subject;
f. The processing is necessary for the conduct of legal claims or whenever courts are acting in their judicial capacity;

[1] GDPR includes a restriction in Recital 47 which states that public authorities such as IFI cannot rely on the legitimate interests of the controller as a legal basis for the processing of personal data. However, Recital 49 provides for processing by public authorities such as IFI for the limited purpose of network and information security which constitutes a legitimate interest of the data controller

g. The processing is necessary for substantial public interest reasons on the basis of EU or EU Member State law which shall be proportionate to the aim pursued, shall respect the essence of the right to data protection and shall provide for suitable and specific measures to safeguard the fundamental rights and interests of the data subject;

h. The processing is necessary for the purposes of preventative or occupational medicine, for the assessment of the working capacity of an employee, for medical diagnosis, for the provision of health or social care or treatment or the management of health or social care systems or services on the basis of EU or EU Member State law or pursuant to a contract with a health professional, subject to the conditions and safeguards referred to in Art. 9.3[2] of the GDPR;

i. The processing is necessary for public interest reasons in the area of public health for example, protecting against serious cross-border threats to health or ensuring high standards of quality and safety of healthcare and of medicinal products or medical devices on the basis of EU or EU Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject (in particular, professional secrecy); or

j. The processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Art. 89.1[3] of the GDPR based on EU or EU Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

1.6 Specified, Explicit and Legitimate Purposes

IFI collects and processes the personal data set out in Section 1.19 of this Policy. This includes:

- Personal data collected directly from data subjects;
- IFI only collects, processes and holds personal data for the specific purposes set out in Section 1.19 of this Policy (or for other purposes expressly permitted by the GDPR);
- Data subjects are kept informed at all times of the purpose or purposes for which IFI uses their personal data;
- Adequate, relevant and limited Data Processing

[2] Article 9.3 states that special category data 'may be processed for the purposes referred to in point (h) above when those data are processed by or under the responsibility of a professional subject to the obligation of professional secrecy under Union or Member State law or rules established by national competent bodies or by another person also subject to an obligation of secrecy under Union or Member State law or rules established by national competent bodies.'

[3] Article 89.1 'Safeguards and derogations relating to processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes'

IFI shall only collect and process personal data for and to the extent necessary for the specific purpose or purposes of which data subjects have been informed (or will be informed) as under Section 1.6 above and as set out in the organisation's Records of Processing Activities as required by Art. 30 of the GDPR.

1.7 Accuracy of Data and Keeping Data Up-to-Date

IFI shall ensure that all personal data collected, processed and held by it is kept accurate and up-to-date. This includes, but is not limited to, the rectification of personal data at the request of a data subject as set out in Section 1.14

The accuracy of personal data shall be checked when it is collected and at regular intervals thereafter. If any personal data is found to be inaccurate or out-of-date all reasonable steps shall be taken without delay to amend or erase that data, as appropriate.

1.8 Data Retention

IFI shall not keep personal data for any longer than is necessary in light of the purpose or purposes for which that personal data was originally collected, held and processed.

When personal data is no longer required all reasonable steps will be taken to erase or otherwise dispose of it without delay. For full details of IFI's approach to data retention including retention periods for specific personal data types held by IFI, please refer to the IFI Personal Data Retention Policy

1.9 Secure Processing

IFI shall ensure that all personal data collected, held and processed is kept secure and protected against unauthorised or unlawful processing and against accidental loss, destruction or damage. Further details of the technical and organisational measures which shall be taken are provided in Sections 1.20 to 1.25 of this Policy.

1.10 Accountability and Record Keeping

IFI's Data Protection Officer (DPO) is Fiona Mahon
3044 Lake Drive, Citywest Business Campus, Dublin D24 Y265
fiona.mahon@fisheriesireland.ie
Tel: 01 8842600

The DPO shall be responsible for overseeing the implementation of this policy, for monitoring compliance with this policy and IFI's other data protection-related policies, with the GDPR and other applicable data protection legislation. All employees must co-operate with the DPO when carrying out their duties. The DPO is also available to answer queries or deal with concerns about data protection.

IFI shall keep written internal records of all personal data collection, holding and processing which shall incorporate the following information:

- The name and details of the organisation, the DPO and any applicable third-party data processors;
- The purposes for which IFI collects, holds and processes personal data;
- Details of the categories of personal data collected, held, processed by IFI and the categories of data subject to which that personal data relates;
- Details of any transfers of personal data to non-EEA countries including all mechanisms and security safeguards;
- Details of how long personal data will be retained by IFI (please refer to the IFI Personal Data Retention Policy); and
- Detailed descriptions of all technical and organisational measures taken by IFI to ensure the security of personal data

1.11 Data Protection Impact Assessments (DPIA)

IFI shall carry out Data Protection Impact Assessments (DPIA's) for any and all new projects and/or new uses of personal data which involve the use of new technologies and the processing involved is likely to result in a high risk to the rights and freedoms of data subjects under the GDPR. For further information please see the IFI Privacy by Design Policy/Data Protection Impact Assessment Policy.

DPIA's shall be overseen by the DPO and shall address the following:

- The type(s) of personal data that will be collected, held and processed;

- The purpose(s) for which personal data is to be used;
- IFI's objectives;
- How personal data is to be used;
- The parties (internal and/or external) who are to be consulted;
- The necessity and proportionality of the data processing with respect to the purposes(s)for which it is being processed;
- Risks posed to data subjects;
- Risks posed both within and to IFI; and
- Proposed measures to minimise and handle identified risks

1.12 Keeping Data Subjects Informed

IFI shall provide the information set out in this section to every data subject.

Where personal data is collected directly from data subjects, those data subjects will be informed of its purpose at the time of collection; and

Where personal data is obtained from a third party, the relevant data subjects will be informed of its purpose:

a) If the personal data is used to communicate with the data subject, when the first communication is made; or

b) If the personal data is to be transferred to another party, before that transfer is made; or

c) as soon as reasonably possible and in any event not more than one month after the personal data is obtained

The following information shall be provided:

- Details of IFI including but not limited to the identity of its DPO;
- The purpose(s) for which the personal data is being collected and will be processed and the legal basis justifying that collection and processing;
- Where applicable, the legitimate interests upon which IFI is justifying its collection and processing of the personal data;
- Where the personal data is not obtained directly from the data subject, the categories of personal data collected and processed;

Where the personal data is to be transferred to one or more third parties, details of those parties shall be provided;

- Where the personal data is to be transferred to a third party that is located outside of the European Economic Area (the "EEA") details of that transfer including but not limited to the safeguards in place (see Section 1.27 of this Policy for further details);
- Details of data retention;
- Details of the data subject's rights under the GDPR;
- Details of the data subject's right to withdraw their consent to IFI's processing of their personal data at any time.[4] Please see the IFI Personal Data Processing & Consent Withdrawal Policy for further details.
- Details of the data subject's right to complain to the Data Protection Commission (DPC) (the "supervisory authority" under the GDPR);
- Where applicable, details of any legal or contractual requirement or obligation necessitating the collection and processing of the personal data and details of any consequences of failing to provide it.

1.13 Data Subject Access

Data subjects may make Subject Access Requests ("SARs") at any time to find out more about the personal data which IFI holds about them, what IFI is doing with that personal data and why.

Data subjects wishing to make a SAR may do so in writing using IFI's Subject Access Request Form. SARs should be addressed to: **Data Protection Officer, Inland Fisheries Ireland, 3044 Lake Drive, Citywest Business Campus, Dublin 24, D24 Y265** or emailed to dpo@fisheriesireland.ie

The GDPR prescribes a timeframe of 'one month' (Art. 12) for responding to SAR's however it does not distinguish between a 28 and 31 day month. In this regard IFI will process requests for personal data within 30 calendar days however, this may be extended by up to two months (60 calendar days) if the SAR is complex and/or numerous requests are made. Please see the IFI Subject Access Request Policy & Procedure for further details.

IFI does not charge a fee for the handling of normal SARs. IFI reserves the right to charge reasonable fees for additional copies of information that have already been supplied to a data subject and for requests that are manifestly unfounded or excessive, particularly where such requests are repetitive.

[4] The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Please see Article 29 WP 'Guidelines on consent under Regulation 2016/679' for further details.

1.14 Rectification of Personal Data

Data subjects have the right to require IFI to rectify any of their personal data that is inaccurate or incomplete.

IFI shall rectify the personal data in question and inform the data subject of that rectification within one month of the data subject informing IFI of the issue. The period can be extended by up to two months in the case of complex requests.

In the event that any affected personal data has been disclosed to third parties, those parties shall be informed of any rectification that must be made to that personal data.

1.15 Erasure of Personal Data

Data subjects have the right to request that IFI erases the personal data it holds about them in the following circumstances[5]:

- It is no longer necessary for IFI to hold that personal data with respect to the purpose(s) for which it was originally collected or processed;
- The data subject wishes to withdraw their consent to IFI holding and processing their personal data; please see the IFI Personal Data Processing & Consent Withdrawal Policy for further details.
- The data subject objects to IFI holding and processing their personal data (and there is no overriding legitimate interest to allow IFI to continue doing so) (see Section 1.18 of this Policy for further details concerning the right to object);
- The personal data has been processed unlawfully;
- The personal data needs to be erased in order for IFI to comply with a particular legal obligation

Unless IFI has reasonable grounds to refuse to erase personal data all requests for erasure shall be complied with and the data subject informed of the erasure within one month of receipt of the data subject's request. The period can be extended by up to two months in the case of complex requests.

In the event that any personal data that is to be erased in response to a data subject's request has been disclosed to third parties, those parties shall be informed of the erasure (unless it is impossible or would require disproportionate effort to do so).

[5] This right is not absolute and only applies in certain circumstances. Data Subjects can require data to be "erased" when there is a problem with the underlying legality of the processing or where they withdraw their consent.

Please see the IFI Policy on the right of erasure of personal data (Right to be forgotten) for further information.

1.16 Restriction of Personal Data Processing

Data subjects may request that IFI ceases processing the personal data it holds about them. If a data subject makes such a request, IFI shall retain only the amount of personal data concerning that data subject (if any) that is necessary to ensure that the personal data in question is not processed further.

In the event that any affected personal data has been disclosed to third parties, those parties shall be informed of the applicable restrictions on processing it (unless it is impossible or would require disproportionate effort to do so).

Please see the IFI Restriction of processing data policy for further details.

1.17 Data Portability

Where data subjects have given their consent to IFI to process their personal data in such a manner or the processing is otherwise required for the performance of a contract between IFI and the data subject, data subjects have the right, under the GDPR, to receive a copy of their personal data and to use it for other purposes (namely transmitting it to other data controllers).

To facilitate the right of data portability, IFI shall make available all applicable personal data to data subjects in the following format[s]:

- .CSV, .XML, .DOCX, .TXT, .XLSX, .PDF

Please see the IFI Data Portability Policy for further details. Where technically feasible, if requested by a data subject personal data shall be sent directly to the required data controller.

All requests for copies of personal data shall be complied with within one month of the data subject's request. The period can be extended by up to two months in the case of complex or numerous requests.

1.18 Objections to Personal Data Processing

Data subjects have the right to object to IFI processing their personal data based on legitimate interests, direct marketing (including profiling) and processing for scientific and/or historical research and statistical purposes.

Where a data subject objects to IFI processing their personal data based on its legitimate interests, IFI shall cease such processing immediately unless it can be demonstrated that IFI's legitimate grounds for such processing override the data subject's interests, rights and freedoms or that the processing is necessary for the conduct of legal claims.

Where a data subject objects to IFI processing their personal data for direct marketing purposes IFI shall cease such processing immediately.

Where a data subject objects to IFI processing their personal data for scientific and/or historical research and statistical purposes the data subjects must under the GDPR, 'demonstrate grounds relating to his or her particular situation.' IFI is not required to comply if the research is necessary for the performance of a task carried out for reasons of public interest.

1.19 Personal Data Collected, Held and Processed

All personal data collected, held and processed by IFI is recorded in a Register/Records of Processing Activities as per GDPR Art. 30.

1.20 Data Security – Transferring Personal Data

IFI ensures that that the following measures are taken with respect to all communications and other transfers involving personal data:

- All emails sent from IFI are transported over an encrypted session;
- IFI staff have been advised that all emails containing personal data shall be marked 'confidential.' This setting can be enabled by the user before sending the email. An email disclaimer is also included on all outgoing email from IFI which outlines the confidentiality of the content;
- Personal data shall be transmitted over secure networks only; transmission over unsecured networks is not permitted in any circumstances;
- Where personal data is to be sent by facsimile transmission the recipient shall be informed in advance of the transmission and should be waiting by the fax machine to receive the data;
- Where personal data is to be transferred in hardcopy form it shall be passed directly to the recipient, sent via registered post or collected in person;
- All personal data to be transferred physically, whether in hardcopy form or on removable electronic media shall be transferred in a suitable container marked "confidential"
  Please see the IFI ICT Policy and IFI ICT Procedures Manual for further details.

1.21 Data Security – Storage

IFI shall ensure that the following measures are taken with respect to the storage of personal data:

- All hard copies of personal data along with any electronic copies stored on physical removable media shall be stored securely in a locked box, drawer, cabinet or similar; (Please see the IFI Clear Screen & Clean Desk Policy for further details)
- All personal data stored electronically shall be backed up. All IFI personal data is backed up each evening to IFI's Disaster Recovery (DR) site with backups stored both onsite and offsite backups sent out monthly
- No personal data shall be stored on any mobile device (including but not limited to, laptops, tablets and smartphones) whether such device belongs to IFI or otherwise without the formal written approval of the Head of each Department
- No personal data shall be transferred to any device personally belonging to an employee and personal data shall only be transferred to devices belonging to agents, contractors or other parties working on behalf of IFI where the party in question has agreed to comply fully with the letter and spirit of this Policy and of the GDPR (which may include demonstrating to IFI that all suitable technical and organisational measures have been taken).
- Only dedicated IFI email accounts shall be used in connection with an individual users work for IFI. The use of third party or web based email accounts for the transmission of IFI information is strictly prohibited.

1.22 Data Security - Disposal

When any personal data is to be erased or otherwise disposed of for any reason (including where copies have been made and are no longer needed) it shall be securely deleted and disposed of. Hard copy documents containing personal data (particularly special category data) shall be securely shredded on IFI premises. The IFI ICT Department has facilities to professionally delete and destroy information on hard drives, DVDs, CDs and other storage media. For further information on the secure deletion and disposal of personal data please refer to the IFI ICT Policy and the IFI Personal Data Retention Policy.

1.23 Data Security – Use of Personal Data

IFI shall ensure that the following measures are taken with respect to the use of personal data:

- No personal data shall be shared informally and if an employee, agent, sub-contractor or other party working on behalf of IFI requires access to any personal data that they do not already have access to; such access should be formally requested from the Head of Department;

- No personal data shall be transferred to any employees, agents, contractors or other parties, whether such parties are working on behalf of IFI or not, without the authorisation of the Head of Department;
- Personal data shall be handled with care at all times and shall not be left unattended or on view to unauthorised employees, agents, sub-contractors or other parties at any time;
- If personal data is being viewed on a computer screen and the computer in question is to be left unattended for any period of time, the user shall lock the computer and screen before leaving it; (Please see the IFI Clear Screen & Clean Desk Policy for further details) and
- Where personal data held by IFI is used for marketing purposes, it shall be the responsibility of the Communications manager to ensure that the appropriate consent is obtained and that no data subjects have opted out, whether directly or via a third-party service such as the Telephone Preference Service (TPS).

1.24 Data Security – IT Security

IFI shall ensure that the following measures are taken with respect to IT and information security:

- All passwords used to protect personal data should be changed regularly and should not use words or phrases that can be easily guessed or otherwise compromised. All passwords must contain a combination of uppercase and lowercase letters, numbers and symbols
- Under no circumstances should any passwords be written down or shared between any employees, agents, contractors or other parties working on behalf of IFI, irrespective of seniority or Department. If a password is forgotten it must be reset using the applicable method. IT staff do not have access to passwords. All software (including, but not limited to applications and operating systems) shall be kept up-to-date. IFI's IT staff shall be responsible for installing any and all security-related updates. The IFI ICT Department frequently update servers / desktops and laptops as updates become available for vendors. A WSUS server is currently deployed within the core infrastructure from which updates can be auto installed.
- No software may be installed on any IFI owned computer or device without the prior approval of the ICT support function or IT manager.

Please refer to the IFI ICT Policy for further details.

1.25 Organisational Measures

IFI shall ensure that the following measures are taken with respect to the collection, holding and processing of personal data:

- Methods of collecting, holding and processing personal data shall be regularly evaluated and reviewed;

- All personal data held by IFI shall be reviewed periodically, as set out in the IFI Personal Data Retention Policy;

All employees, agents, contractors or other parties working on behalf of IFI shall;

- Be made fully aware of both their individual responsibilities and IFI's responsibilities under the GDPR and under this Policy and shall be provided with a copy of this Policy;

- Ensure that any and all of their employees who are involved in the processing of personal data are held to the same conditions as those relevant employees of IFI arising out of this Policy and the GDPR;

- Only those persons that require access to and use of personal data in order to carry out their assigned duties correctly shall have access to personal data held by IFI;

- Persons handling personal data shall be appropriately trained to do so and shall be appropriately supervised;

- Persons handling personal data will be bound to do so in accordance with the principles of the GDPR and this Policy by contract;

- Shall be required and encouraged to exercise care, caution and discretion when discussing work-related matters that relate to personal data whether in the workplace or otherwise;

- The performance of those persons handling personal data shall be regularly evaluated and reviewed;

- Where any agent, contractor or other party working on behalf of IFI handling personal data fails in their obligations under this Policy that party shall indemnify and hold harmless IFI against any costs, liability, damages, loss, claims or proceedings which may arise out of that failure.

1.26 Subject Access Requests (SAR)

Data subjects may make Subject Access Requests (SAR's) to IFI to find out more about the personal data that IFI holds about them, what IFI is doing with that personal data and for what purpose(s). Please see the IFI Subject Access Request Policy & Procedure for further details.

1.27 Transferring Personal Data to a Country outside the EEA

Any transfers of personal data to countries outside of the EEA shall be managed through model clause contracts.

1.28 Data Breach Notification

All personal data breaches shall be reported immediately to IFI's Data Protection Officer. Please see the IFI policy on communication of a personal data breach to the data subject and the IFI policy on the notification of a personal data breach to the Supervisory Authority for further details.

Appendix I - Definitions

The following definitions which are used in this policy are taken from the General Data Protection Regulation (GDPR) and are provided to ensure clarity for the reader. Full copies of the GDPR are available at the following link: https://gdpr-info.eu/ Copies of the Data Protection Act 2018 are available on the Oireachtas website

A Data Subject is an identifiable natural person; an identifiable natural person is one who can be identified directly or indirectly.

A natural person is a living individual.

Personal Data is any information relating to an identified or identifiable natural person ('data subject'). An identifiable natural person is one who can be identified, directly or indirectly in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. Examples of personal data include:

- Name
- Address
- Date of Birth
- Phone number
- Email address
- IP Address
- Employee number
- PPS number

Special categories of personal data are subject to stricter processing requirements. This includes personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

Consent of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

Data Controller is the natural or legal person, public authority, agency or any other body which alone or jointly with others, determines the *purposes and means* of the processing of personal data.

A Personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to personal data transmitted, stored or otherwise processed. This includes breaches that are the result of both accidental and deliberate actions.

The Processor is a natural or legal person, public authority, agency or any other body which processes personal data on behalf of a Data Controller.

Processing - is defined as any operation or set of operations which is performed on personal data or on sets of personal data whether by automated means such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Processing Purpose - is the pre-defined reason for collecting and processing a specific set of data e.g. to provide a range of fisheries management and development services, to complete HR, payroll and pension administration functions, issuing of Fixed Charge offences. Each purpose should be paired with a description of data use. All pre-defined purposes should be listed in a privacy notice made available to data subjects before data is collected and a Data Protection Impact Assessment (DPIA) should include a check to ensure pre-defined purposes do not differ from current data uses.

Supervisory Authority – is the independent public authority with responsibility for monitoring the application of the GDPR in order to protect the fundamental rights and freedoms of natural persons in relation to processing and to facilitate the free flow of personal data within the European Union. In the context of the Irish Jurisdiction this authority is vested in the office of the Irish Data Protection Commission.

Accountability – The controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with the GDPR. The measures implemented shall be reviewed and updated where necessary. ("Accountability Principle")