Data Protection Policy

Approved by Senior Management Team

May 2024

Policy references

Title:	Data Protection Policy – "LIVE"	Policy Number	2
Author:	Caroline McLoone		
Ownership:	Corporate Services		
Approval:	Senior Management Team		
Operational Date:	19th April 2024	Approval date:	23rd May 2024
Version No.	2.5	Supercedes:	Version 2.4
Key words:	GDPR, Personal Data, Data Subject, Processing, Structured Filing System, Supervisory Authority, Data Security, Breach		
Links to other policies:	Freedom of Information Code of Practice Records Management Policy Statement Retention and Disposal Schedule Information Technology Acceptable Usage Policy Hybrid Working Policy Recruitment and Selection Policy		

Version History

Date	Version	Author	Comments
1/5/2011	1.0	Sharon Roulston	Policy clarifications
1/8/2018	2.0	Caroline McCarroll	Reflects GDPR legislation and associated Data Protection Acts 2018 enacted in Ireland the United Kingdom
26/10/18	2.1	Caroline McCarroll	Amendment of Compliance Checklist (Appendix C) to reflect testing
05/02/20	2.2	Roisin MacRory	Policy References updated Para 1.5 location of policy amended Appendix C updated
29/01/21	2.3	Roisin MacRory	Legislation updated
10/03/23	2.4	Roisin MacRory	Policy Review, minor updates
19/04/24	2.5	Caroline McLoone	DPO name change throughout.

Contents

Appendices

1.0 Introduction

1.1. In order to deliver Waterways Ireland's operational functions as a cross border body, we collect, store, use and share certain types of personal information, both in relation to the public and our employees. For example,

- To provide a member of the public with the services, products or information they have asked for.
- To keep a record of the public's relationship with us (when and how they have contacted us).
- To ensure we know how our customers prefer to be contacted.
- To assist us in identifying and understanding how we can deliver and improve our services, products or information.
- To maintain the security of our properties and for preventing and investigating crime, through the installation and use of Closed-circuit television (CCTV).
- To fulfil our legal and regulatory obligations both to our employees and the public.

This Data Protection Policy sets out Waterways Ireland's operational standards in relation to the collection, storage, use and disclosure of personal information. The policy also regulates such activities to ensure we operate in compliance with the General Data Protection Regulations (GDPR) in Ireland and in the UK.

The use of all personal data by Waterways Ireland is governed by the following legislative provisions which take precedence in all circumstances:

- The General Data Protection Regulation (EU) 2016/679 [**EU-GDPR**] and the Irish Data Protection Act, 2018
- UK General Data Protection Regulation [**UK-GDPR**] and the UK Data Protection Act 2018, as amended by the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations, 2019
- The Electronic Privacy Regulations 2011
- Privacy and Electronic Communications Regulations (PECR)

1.2. Waterways Ireland is registered as a Data Controller with the Information Commissioner's Office. The registration number is Z9098664.

1.3. A Glossary of Policy Terms is set out in Appendix A.

1.4. This policy should be read in conjunction with Waterways Ireland's Privacy Notice, the latter detailing our published commitments regarding the use and security of personal information which the organisation collects and uses. The current version is posted on our website at https://www.waterwaysireland.org/privacy-notice

1.5. The policy will be subject to routine consideration and from time to time revisions will be made to reflect implementation requirements and clarifications. The most up to date version of the policy will be available on Waterways Ireland's INTRANET (*Corporate Services folder)* and notified to staff through line management and email communication.

1.6. The policy will be formally reviewed at 12 month intervals (commencing May 2019), to reflect changes to legislation or the structure of Waterways Ireland, and new or amended organisational policies that have relevance to data protection.

2.0 What is the General Data Protection Regulation (GDPR)

The General Data Protection Regulation (GDPR) provides a comprehensive modern framework for data protection in the EU and UK. The legislation regulates the processing of personal information relating to **'living individuals'.**

Technological advances have made pre-existing data protection legislation no longer fit for purpose. GDPR takes account of the vast number of new ways in which people obtain and provide personal information, for example through the internet, smart phones, tablets, on-line shopping, banking etc.

GDPR also gives individuals increased rights in relation to the collection, use and management of their personal information, regardless of how it is provided/obtained by organisations. The legislation places increased responsibilities on organisations that collect and use personal information to retain documentation/evidence that demonstrates they are operating in compliance with GDPR, and it imposes significant fines if organisations are found to not be compliant.

3.0 What is E-Privacy

E-privacy directives complement the general data protection regime and sets out more specific privacy rights on electronic communications.

E-Privacy regulations cover several areas:

- Marketing by electronic means, including marketing calls, texts and emails.
- The use of cookies or similar technologies that track information about people accessing a website or other electronic service.
- Security of public electronic communications services.
- Privacy of customers using communications networks or services as regards traffic and location data, itemised billing, line identification services (eg caller ID and call return), and directory listings.

4.0 Purpose of this Data Protection Policy

The lawful and correct handling of personal data by Waterways Ireland staff or contractors acting on its behalf is essential to operating successfully, and the maintenance of confidence between Waterways Ireland and those with whom it deals, both internally and externally.

The purpose of this Data Protection Policy is to detail the operational standards and obligations of staff to ensure Waterways Ireland is compliant with GDPR and associated legislation in the UK and Ireland. It also obligates service providers/suppliers acting on our behalf and others with whom we share personal data, to only collect and manage personal data in accordance with Waterways Ireland GDPR contract clauses or a signed Data Sharing Agreement.

This policy requires that GDPR compliance is central to the way in which we do business on a daily basis. We must integrate associated Data Protection obligations into all of our operational activities, processes and risk management planning – GDPR defines this as Data Protection by Design and Default. These responsibilities start from the point in which we plan to collect or use personal information, and they continue in relation to our ongoing responsibilities regarding storage and security of such information, decisions on sharing with third parties, archiving requirements, and disposal of certain types of personal information in accordance with our Retention and Disposal Schedule. Aligned to these responsibilities is our obligation to honour the data protection and transparency commitments detailed in the Waterways Ireland published Privacy Notice.

5.0 Scope of the policy

5.1. This policy applies to employees, agency workers, third party suppliers/service providers operating on Waterways Ireland's behalf and other authorised individuals – referred to as “users” within this policy.

5.2. Failure to comply with this policy may result in disciplinary action for Waterways Ireland employees, termination of a contract in the case of a third party supplier/service provider, or termination of a Data Sharing Agreement in relation to organisations with whom we lawfully share personal data.

5.3. Individuals who consider that their personal information has been processed incorrectly by Waterways Ireland or in any way breaches the Data Protection Principles may complain initially to the Data Protection Officer, on appeal to the Chief Executive and if not satisfied with the investigation findings, they may complain to the supervisory authority i.e. Information Commissioner’s Office UK or the Data Protection Commission in Ireland. GDPR provides for a range of sanctions which may be imposed by the supervisory authority, including financial penalties. See section 19.0 regarding 'How to make a Data Protection Complaint'.

6.0 Data Protection responsibilities in Waterways Ireland

6.1. **Chief Executive**
The Chief Executive has overall responsibility for Data Protection compliance requirements and the implementation of this policy.

6.2. **Waterways Ireland Data Protection Officer**
The Data Protection Officer will provide advice, guidance and monitoring of GDPR compliance and implementation of this Data Protection Policy. The Data Protection Officer will report to the Chief Executive regarding Data Protection matters and have the support of the Directors, Regional Managers and their staff regarding implementation of this policy and associated GDPR compliance requirements.

Specific responsibilities include:

- Informing and advising Waterways Ireland senior management and staff of their obligations in relation to GDPR and this policy.
- Training of staff, awareness-raising and assignment of GDPR responsibilities.
- Monitoring compliance with this policy through audits.
- Processing requests by Data Subjects to access their personal data or exercise of other rights.
- Investigating Data Protection complaints.
- Cooperating with and actioning the requirements of the Data Protection supervisory authorities; the Information Commissioner's Office UK and the Data Protection Commission in Ireland.
- Providing advice when requested regarding need for Data Protection Impact Assessments and monitoring associated compliance in accordance with Article 35 of the GDPR.
- Updating this policy to reflect future legislative changes and communication of these changes to staff and other relevant users of the policy.
- Submission of Regions/Section proposals to begin new personal data collection and processing requests to the Senior Management Team for approval.
- Amendment of Waterways Ireland's 'Audit of Personal Data' held and also Privacy Notice to reflect new data collection and processing activities approved by the Senior Management Team. This audit must be maintained in accordance with Article 30 of GDPR.

6.3. **Head of IT**

The Head of IT is responsible for ensuring compliance with Data Protection in relation to the capture and storage of personal data through the use of CCTV at Waterways Ireland property.

6.4. **Directors and Regional Managers**

Each Director and Regional Manager has delegated responsibility for the protection of personal data within their own areas of operation and for compliance in relation to this policy. Specific responsibilities include:

- Implementing Data Protection actions and providing input as requested by the Waterways Ireland Data Protection Officer.

- Prioritising Data Protection responsibilities and required actions among their staff and monitoring compliance on a regular basis.

- Ensuring that the Data Protection Officer is consulted in a timely manner on issues which relate to the protection of personal data.

- Submitting proposals to begin new personal data collection and processing activities to the Data Protection Officer for Senior Management Team consideration and inclusion in Waterways Ireland's 'Audit of Personal Data' held.

- Ensuring that the GDPR Contract Clauses and associated Schedule of Processing is in place with all third party processors acting on behalf of Waterways Ireland, and that the general GDPR Contract Clause is incorporated into all other service contracts (**see section 14 and Appendices G and H).**

- Ensuring that an approved Data Sharing Agreement is in place for the sharing of personal data with other agencies/bodies, where such sharing is not governed by a legislative requirement.

- Completing the Data Protection Compliance Checklist **(see Appendix C)**, regarding their respective work areas on a quarterly basis.

6.5. **All Staff**

All Waterways Ireland staff and others acting on Waterways Ireland's behalf have a duty to ensure compliance with data protection legislation and the provisions within this policy. They each have a responsibility to ensure that all personal data they access, manage and control (*either hard copy or electronic*) as part of their duties, is carried out in accordance with this policy and their line manager's instructions.

- Staff should not initiate the collection or processing of personal data without their line manager's prior approval. Personal information must not be collected or used unless there is justification, both legally and practically for doing so.

- Decision Makers referred to in this policy are senior staff members acting on behalf of the Chief Executive, with delegated responsibility to make recommendations/decisions regarding the 'Rights of Data Subjects' (**see Appendix F)**.

- All information held on Waterways Ireland's equipment (including PCs, laptops, mobile phones and tablets) may be subject to an information search in the course of processing a Subject Access request or in relation to assessing compliance with this policy.

- Non-compliance with this policy will be dealt with in accordance with Waterways Ireland's Code of Conduct policy and Disciplinary policy.

7.0 How we must demonstrate compliance with the 6 Data Protection Principles

As Data Controller, Waterways Ireland is responsible for ensuring compliance with 6 GDPR principles and must be able to demonstrate this to Data Subjects and the supervisory authorities (the Information Commissioner's Office, UK and the Data Protection Commission in Ireland). Accountability underpins each of the 6 principles and requires our staff and representatives to keep relevant and sufficient records of evidence to demonstrate that personal information is:

7.1. **Processed lawfully, fairly and in a transparent manner;**

7.2. **Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (Purpose Limitation Rule).**
Further processing for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes will, in accordance with Article 89(1) of the GDPR, not be considered to be incompatible with the initial purposes.

7.3. **Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (Data Minimisation rule);**

7.4. **Accurate and where necessary kept up to date (Accuracy Rule)**
Where personal data is considered to be inaccurate, whilst having regard to the purposes for which it is processed, every reasonable step must be taken to ensure that it is erased or rectified without delay once informed of any inaccuracy.

7.5. **Kept in a form which permits identification of Data Subjects for no longer than is necessary for the purposes for which those data are processed (Storage Limitation Rule).**
Sections must retain personal data for no longer than committed to the Data Subject and detailed in the published Waterways Ireland Personal Data Retention and Disposal Schedule.

Personal data may only be stored for longer periods where it is to be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) of the GDPR. Such longer storage is only permitted where appropriate technical and organisational measures are in place to safeguard the rights and freedoms of the Data Subject.

7.6. **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 (Integrity and Confidentiality Rule).**

8.0 How we must demonstrate the lawfulness of data processing activities

Directors and Regional Managers must identify the lawful basis for processing personal data and obtain SMT approval in association with the Data Protection Officer, prior to beginning any new personal data processing activity.

The lawful bases for processing are set out in Article 6 of the GDPR and at **least one** of these must apply before Waterways Ireland can process personal data:

8.1. **Consent**
The Data Subject has given clear written consent for Waterways Ireland to process their personal data for one or more specific purposes.

8.2. **Contract**
The processing is necessary for the performance of a contract Waterways Ireland has with a Data Subject or because the Data Subject has asked Waterways Ireland to take specific steps prior to entering into a contract. Personal data relating to Sole Traders or Partnerships without limited liability is afforded the same protections as personal data relating to a member of the public or staff.

8.3. **Legal obligation**
The processing is necessary for Waterways Ireland to comply with the law (not including contractual obligations).

8.4. **Vital interests**
The processing is necessary to protect a Data Subject's life, e.g. in the case of an emergency.

8.5. **Public task/function**
The processing is necessary for Waterways Ireland to perform a task in the public interest or a function in exercise of our official authority as a cross border body, and the task/function has a clear basis in law.

8.6. **Legitimate interests**
The processing is necessary for Waterways Ireland's legitimate interests or the legitimate interests of a third party, unless there is a good reason to protect the Data Subject's personal data which overrides those legitimate interests. Note: this lawful basis does not apply to Waterways Ireland where the processing of personal data relates to the performance of its public task(s)/functions in exercise of its official authority as a cross-border body.

9.0 Use of Personal Data for purposes other than originally advised to the Data Subject requires prior approval

The use of personal data for purposes other than that for which the personal data was originally collected is not permitted except with the prior authorisation of line management, and with advice from the Data Protection Officer. A decision will be taken based on the following:-

9.1. The need to inform the Data Subject and provide them with additional relevant information prior to carrying out any further processing.

9.2. Any link between the purposes for which the personal data was collected and the purposes of the intended additional processing, and the legal basis which applied when the personal data was initially collected.

9.3. Consideration of the context in which the personal data was collected and the relationship between Waterways Ireland and the Data Subject.

9.4. The nature of the personal data and whether special categories of personal data are processed in accordance with Article 9 of the GDPR, or whether personal data in relation to criminal convictions and offences are processed in accordance with Article 10 of the GDPR.

9.5. The possible consequences of any further processing for the Data Subjects.

9.6. The existence of appropriate safeguards, for example encryption or pseudonymisation.

10.0 Conditions necessary for Consent to be considered valid

10.1. Waterways Ireland must be able to demonstrate that the Data Subject has provided consent to the processing of his/her personal data. Therefore, consent must be provided in a written declaration which details the consent separate from other written matters in the declaration. Consent should be obtained by amending any existing forms or issuing the Data Subject with a new consent

form to complete. Each Region/Section must amend or develop individual consent forms relevant to their data collection activities.

10.2. The written consent should be specific and granular so that you get separate consent for separate things for example, sharing photographs with a third party who you must name in full in order for them to also rely on the Data Subject's consent.

10.3. The consent form should be in clear language, intelligible, concise and in an accessible form.

10.4. The consent form should provide a positive confirmation of agreement by the Data Subject that Waterways Ireland can process their personal data for one or more specific purposes as detailed on the form. It requires a positive opt-in – Do not use pre-ticked boxes or any other method of default consent.

10.5. Consent cannot be inferred through silence (not objecting) or inactivity by the Data Subject.

10.6. Data Subjects must be made aware on a Waterways Ireland consent form that they have the right to withdraw their consent and we must tell them how, for example by telephoning xxxxxxxx or emailing xxxxx@waterwaysireland.org. A Data Subject has the right to withdraw their consent at any time and Waterways Ireland must act on the withdrawal of consent as soon as it can. The withdrawal of consent does not affect the lawfulness of processing based on the consent before its withdrawal.

10.7. In assessing whether consent has been freely given by a Data Subject, it is necessary to consider whether the performance of a contract, including the provision of a service, is conditional on receiving consent for the processing of personal data necessary for the performance of the contract.

10.8. Evidence of consents received must be retained/filed and a record kept for reporting purposes (who, when, how and what you told people the consent was for).

10.9. Regions/sections must keep consent under review to ensure that the circumstances of consent use are the same as when the Data Subject originally provided the consent. Regular review of consent is necessary to ensure that the relationship between the Data Subject and Waterways Ireland, the purpose of the consent and the processing has not changed.

11.0 Processing of special categories of Personal Data (Sensitive Data)

Where Waterways Ireland intends to process any special categories of personal data, it is required to identify one or more legal bases from Article 9 of the GDPR to demonstrate the lawfulness of such data processing. This is in addition to the legal basis already identified in Article 6 of the GDPR. There are 8 legal bases within Article 9 to be considered of potential relevance:

11.1. The Data Subject has given their consent to the processing for one or more specified purposes.

11.2. Processing is necessary for the purposes of carrying out Waterways Ireland's obligations and exercising its specific rights or those of the Data Subject in relation to employment, social security or social protection law.

11.3. Processing is necessary to protect the vital interests of the Data Subject where they are physically or legally incapable of giving consent.

11.4. Processing relates to personal data which have been made public by the Data Subject.

11.5. Processing is necessary for the establishment, exercise or defence of legal claims.

11.6. processing is necessary for reasons of substantial public interest based on EU or member state law.

11.7. Processing is necessary for the assessment of the working capacity of the employee.

11.8. Processing is necessary for archiving purposes in the public interest or historical purposes or statistical purposes.

Criminal offence Data

Criminal offence data includes data about criminal convictions, criminal offences or related security measures. Whilst criminal offence data is not considered as a Special Category of personal data under GDPR, there are separate conditions which must be satisfied prior to collecting such data.

Firstly, it is necessary that a lawful basis for processing is identified, as per section 8.0 above. Secondly, in compliance with Article 10 of GDPR, it is necessary that an authorised Waterways Ireland manager documents that the processing of identified criminal offence data is being carried out in an official capacity for a specified purpose, and that he/she ensures that the processing

undertaken provides appropriate safeguards for the rights and freedoms of the Data Subject.

12.0 Our obligations in relation to the Rights of the Data Subject

The Data Protection Officer is responsible for receiving and processing requests from Data Subjects who wish to exercise their Data Protection rights as follows:

- The Right to be Informed
- The Right of Access
- The Right to Rectification
- The Right to Erasure
- The Right to Restrict Processing
- The Right to Data Portability
- The Right to Object
- Rights in relation to automated decision making and profiling

Requests from Data Subjects to exercise their rights under this policy should be submitted in writing to the Data Protection Officer (**see contact details in Appendix D).**

The Data Protection Officer will, on receiving such a request, acknowledge within 5 working days. Proof of identity may be requested in relation to all of the above GDPR rights in accordance with Waterways Ireland's commitment to secure personal data and to also enable the accurate retrieval of requested CCTV footage or other photographic records.

Proof of identify must be in the form of a photocopy of either:

(a) The pages which identify the Data Subject in their passport

(b) Their Driver's Licence, or

If the Data Subject does not hold either of the above documents, they should provide:

(c) A copy of an alternative official form of photographic ID or other official identification.

On receipt of the Requester's Proof of Identity, the Data Protection Officer will request the relevant Waterways Ireland Decision Maker to process the request by a required date. Where the Data Protection Officer or Decision Maker has reasonable doubts about the identity of the Requester, they may request additional information necessary to confirm the identity of the Data Subject. Waterways Ireland will not refuse to act on the request of a Data Subject to exercise their rights unless it is not possible to identify the Data Subject.

Timescales

Information provided or actions taken by Waterways Ireland's Decision Makers at the request of the Data Subject will be provided without undue delay and no

later than 1 calendar month from the date of receiving the request. This time period can be extended by 2 further months where necessary due to the complexity and number of requests. In such circumstances, the Data Protection Officer will inform the Data Subject of the time extension within 1 month of receiving the request, together with the reasons for the delay.

Manifestly unfounded or excessive requests

Where requests from a Data Subject are considered to be manifestly unfounded or likely to cause an excessive administrative burden, the Waterways Ireland Decision Maker may conclude a decision to charge an administration fee, or 'Refuse to act on the request' with prior demonstration of the case decision in writing to the Data Protection Officer. The Data Protection Officer has the right to consider the appropriateness of the Decision Maker's decision and advise as required.

12.1. **The Right to be Informed**

Where personal information is obtained directly from a Data Subject, **at the time in which it is collected**, the following information should be provided to the Data Subject, in the form of a Privacy Notice and other direct written communication as may be relevant:-

(a) The identity of Waterways Ireland as the Data Controller;

(b) Contact details of the Data Protection Officer;

(c) The purposes of any personal data processing and associated legal basis with evidence of the latter;

(d) The recipients of the personal data;

(e) State if the data is likely to be a third country or international organisation, and the safeguards that exist;

(f) The period for which the data will be stored;

(g) The existence of the Data Subject's right to request from Waterways Ireland access to, rectification or erasure of personal data, or restriction of processing concerning the Data Subject, or to object to processing as well as the right to portability (as explained in sections 12.2-12.7 below);

(h) Right to withdraw consent at any time, where relevant;

(i) Right to lodge a complaint with the Information Commissioner's Office UK or the Data Protection Commission in Ireland;

(j) Whether the Data Subject is required to provide any personal data as part of a legal or contractual requirement and the consequences of not doing so; and

(k) The existence of any automated decision-making including profiling and associated explanatory information about how decisions will be made and the significance of these.

Note (i): Waterways Ireland's overall GDPR Privacy Notice is available for download from our website at https://www.waterwaysireland.org/privacy-notice.
It will be updated periodically by the Data Protection Officer to reflect new Personal Data processing activities undertaken by the organisation and any changes to the ways in which personal data is collected, processed and shared.

Note (ii): In addition to the Privacy Notice, Waterways Ireland Decision Makers **(see Appendix F)** may authorise the provision of additional information to Data Subjects when collecting their personal information. This can be either through application forms, leaflets or other forms of direct written communication which provide specific context for individual data collection activities taking place, as required under section 12.1 (a) to (k) above.

Personal Data indirectly obtained

It is recognised that Waterways Ireland may obtain personal data indirectly from other organisations. Where obtained indirectly, the responsible Waterways Ireland staff member (Decision Maker) must contact the Data Subject and advise him/her that Waterways Ireland is holding their personal details, and at that time include the information specified in (a) to (k) above and additionally detail:-

(l) The categories of personal data Waterways Ireland is holding regarding the Data Subject; and

(m) Where the personal data originated from and whether it came from publicly accessible sources.

All of the above information requirements i.e. (a) to (m) should be issued to the Data Subject as soon as possible, or at the latest,

- within 1 month of first receiving the personal data indirectly;
- if the personal data is to be used for communication with the Data Subject, no later than at the time of first communication to the Data Subject; or
- if it is intended to disclose the personal data to another recipient, no later than the time when the personal data are first disclosed.

Note: Should Waterways Ireland intend to use the personal data for purposes other than those for which the data was originally obtained, it is necessary to inform the Data Subject and provide them with additional relevant information prior to carrying out any further processing.

12.2. **The Right to Access**

Data Subjects have the right to know if Waterways Ireland is processing their personal information and if this is the case, the right to access it, as well as the information requirements set out in section 12.1 (a) to (m) above. Requests to access an individual's own personal data should be submitted in writing to the Data Protection Officer using the Subject Access Request Form provided in **Appendix E**, enclosing proof of identity as explained in **section 12.0**. The Waterways Ireland Decision Maker may issue a response in writing or orally if requested by the Data Subject.

- Waterways Ireland will where possible and proportionate provide the data requested in the preferred format of the applicant.

- The information provided to the Data Subject should be concise, transparent, intelligent and easily accessible.

- Whilst Data Subjects have the general right of access to any of their own personal information which is held, Waterways Ireland will be mindful of those circumstances where an exemption may apply and, in particular, the data protection rights of third parties who may also be identifiable from the data being requested.

No Charge

Data Subjects will not be charged for obtaining their personal information, unless a request is considered likely to cause an excessive administrative burden to Waterways Ireland.

12.3. **The Right to Rectification**

Waterways Ireland will rectify personal data where it is reported to be inaccurate or incomplete without undue delay, including enabling the Data Subject provide a supplementary statement.

Where Waterways Ireland has already disclosed the personal data in question to others, they will contact each recipient and inform them of the rectification - unless this proves impossible or involves disproportionate effort. If Waterways Ireland cannot take action to rectify for the reasons above, an explanation will be provided to the individual and they will be informed of their right to complain to the Waterways Ireland Data Protection Officer, and thereafter to the Information Commissioner UK or the Data Protection Commission in Ireland.

12.4. **The Right to Erasure – also known as "the Right to be Forgotten"**

Where there is no compelling reason for the continued processing of an individual's personal data, Waterways Ireland will delete or remove the personal data at the request of the individual. Data may be erased to prevent processing in the following circumstances:

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed;

- When the individual withdraws consent for the processing and there is no other legal basis for processing;

- When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing;

- The personal data was unlawfully processed;

- The personal data has to be erased in order to comply with a legal obligation.

There are some specific circumstances where the right to erasure does not apply. A request for erasure may be refused where the personal data is processed for the following reasons:

- To exercise the right of freedom of expression and information;

- To comply with a legal obligation, for the performance of a Waterways Ireland public task or in exercise of its official authority;

- For public health purposes in the publi22c interest;

- Archiving purposes in the public interest, scientific research historical research or statistical purposes; or

- The exercise or defence of legal claims.

If Waterways Ireland has already disclosed the personal data in question to others, the Waterways Ireland Decision Maker will contact each recipient and inform them of the erasure of the personal data - unless this proves impossible due to available technology or involves a disproportionate cost to Waterways Ireland. The Decision Maker is obligated to inform a Data Subject of its actions in this regard if requested.

12.5. **The Right to Restrict Processing**

Waterways Ireland will restrict the processing of personal data in the following circumstances:

- Where a Data Subject contests the accuracy of the personal data, we will restrict the processing until the accuracy of the personal data has been verified;

- When processing is considered to be unlawful and the Data Subject opposes erasure and requests restriction instead;

- Waterways Ireland no longer require the personal data for the purpose of the processing but the Data Subject requires the data to establish, exercise or defend a legal claim;

- The Data Subject has objected to the processing (where it was necessary for the performance of a public interest task or in the legitimate interests of Waterways Ireland), and the Decision Maker is considering whether Waterways Ireland's legitimate grounds override those of the Data Subject.

Where the personal data in question has already been disclosed to others, the Waterways Ireland Decision Maker must contact each recipient and inform them of the restriction on the processing of the personal data - unless this proves impossible or involves disproportionate effort. The Decision Maker is obligated to inform a Data Subject of its actions in this regard if requested.

Where a Data Subject has obtained a restriction to the processing of their personal data, such restriction will not be lifted by the Decision Maker without first informing the Data Subject.

12.6. **The Right to Data Portability**

The Right to Data Portability allows individuals to obtain and transmit their personal data from Waterways Ireland to another service provider, from one IT environment to another in a safe and secure way, without hindrance to usability.

This Right to Data Portability only applies:-

(a) To personal data an individual has provided to Waterways Ireland;

(b) Where the processing is based on the individual's consent or for the performance of a contract; and

(c) When processing is carried out by automated means.

Where the Data Portability request meets the requirements (a) to (c), the Waterways Ireland Decision Maker will provide the personal data in a structured, commonly used and machine readable form and free of charge. If the Data Subject requests, Waterways Ireland will transmit the data directly to another organisation, where this is technically feasible.

The Right to Data Portability will not apply where Waterways Ireland needs to continue processing of the requested data in order to fulfil its public task responsibilities or in exercise of its official authority as a cross-border body.

12.7. **The Right to Object**

Data Subjects have the right to object in relation to the following:

- Processing of their personal data based on Waterways Ireland's legitimate interests, the performance of a task in the public interest, or in exercise of its official authority (including profiling);
- Direct marketing (including profiling); and
- Processing of their personal data for purposes of scientific/historical research and statistics.

Waterways Ireland will stop processing the personal data unless:

(a) There is compelling legitimate grounds for the processing which override the interests, rights and freedoms of the individual; or

(b) The processing is for the establishment, exercise or defence of legal claims.

Waterways Ireland will inform individuals of their Right to Object '**at the point of first communication'** and through our Privacy Notice. The Right to Object will be 'explicitly brought to the attention of the Data Subject and shall be presented clearly and separately from any other information'.

Waterways Ireland must stop processing personal data for direct marketing purposes as soon as it receives an objection, and the relevant Decision Maker will confirm that such action has been taken to the Data Subject.

Where a Data Subject objects to Waterways Ireland processing their personal data for scientific, historical research or statistical purposes, Waterways Ireland will consider any objection however, may take the decision to continue with such processing where it is necessary for the performance of a task carried out in the public interest.

12.8. **Rights related to automated decision making including profiling**

Waterways Ireland does not currently use automated decision-making in relation to any personal data it collects and processes. Should Waterways Ireland decide to use automated decision-making in the future, it will not be used without human intervention to enable the expression and consideration of individual views. This will ensure that no decision is taken regarding personal data based solely on an automated process.

13.0 Our obligations to secure Personal Data

Employees must not hold personal information on Waterways Ireland's equipment without firstly ensuring the need to hold the information, legal basis for doing so, and putting in place appropriate security measures to prevent unauthorised access, disclosure or loss. All information held on Waterways Ireland equipment (including PCs, smart phones, mobile phones, tablets and laptops) may be subject to search, for example, in the course of processing Data Protection Subject Access Requests or as part of a periodic assessment of Directorate and Regional GDPR compliance.

13.1. Waterways Ireland's delegated officers to include the Head of IT will ensure:

- Appropriate security measures are in place to protect personal data, both automated and manual systems;
- The ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
- A process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures ensuring the security of the processing;
- Personal data systems are accessible to authorised staff only;

- Authorised staff using these systems will be advised of appropriate security procedures and the importance of their role within these procedures.
- Authorised staff must only access personal data where this is relevant to their role responsibilities. They should never use their access in order to obtain or view either their own personal records or the personal records of others where not required as part of their role responsibilities. The submission of a Subject Access Request is the route to obtaining personal information as explained in **section 12.2.**
- Personal data no longer required is disposed of through shredding in accordance with Waterways Ireland's Records Management Policy Statement and associated Retention & Disposal Schedule.
- Staff implement Data Protection obligations set out in other policies issued by Waterways Ireland (**see policy references on page 2)**.

13.2. Care should be taken in the use of email for the transmission of sensitive personal information. Emails containing sensitive personal information should be encrypted or information sent in hard copy in a sealed envelope.

13.3. Laptops, PC's and terminals should be appropriately sited at work stations so that they are visible only to authorised staff. Particular care must be taken by staff working from home to ensure no unauthorised access.

13.4. Hard copy files that contain personal information must be stored in a secure location with controlled access. When a file is moved from storage the staff member doing so will be responsible for its safe keeping at all times, particularly when taken into a public location.

13.5. Do not leave manual personal records, printouts etc where they can be accessed by unauthorised staff.

13.6. Use of removable electronic media (USB sticks, portable hard drives etc) will be in accordance with Waterways Ireland's ICT policies.

13.7. Inappropriate or unauthorised access to personal data or failure to implement any other staff obligation in relation to this Data Protection Policy and associated policies may result in disciplinary action.

14.0 Service contractors must be GDPR compliant

14.1. **Declaration of Compliance with GDPR for Tendering Purposes**
Tender submissions for service contracts with Waterways Ireland generally include the CV's of staff to be engaged in such contracts. To ensure compliance with GDPR, tender invitations for all service contracts should include a Declaration of Compliance with GDPR (**see Appendix G).** This declaration should be completed, signed and included with the Contract Documents returned as part of the Tender submission.

14.2. **Data Processor service contracts**
Waterways Ireland employs Data Processors to process personal data on its behalf thereby enabling the organisation deliver its functions, to provide services

to the public and staff, IT support, and specialist advice. Data Processors must act in compliance with GDPR requirements and Waterways Ireland's contract instructions throughout the duration of the contract. To this end, GDPR contract clauses and the associated Schedule 1B of processing activities as issued by the Data Protection Officer must be completed and incorporated into the signed contract. **See Appendix H** (GDPR Standard Clauses of Contract for contractors engaged to process personal data on Waterways Ireland's behalf).

14.3. **Pre-procurement**

Managers must highlight in any pre-procurement dialogue with potential suppliers that the contract will be subject to the GDPR to make suppliers aware of the legislation and their obligations as the Processor.

14.4. **Specifications**

Managers must ensure that the contract specifications clearly set out the roles and responsibilities of Waterways Ireland as the Controller and the Contractor as Processor and any Sub-Processors, throughout the period of the contract. The specification must detail:

- Where appropriate, any technical requirements and organisational measures which the Processor needs to operate and maintain.

- The requirements and process in respect of audit of the Processor to check compliance with the GDPR; and

- Any security obligations equivalent to those imposed on Waterways Ireland as the Controller (implementing a level of security for the personal data appropriate to the risk), and

- The specification and contract clauses should refer to the Schedule 1B for processing. If the Processor does not follow these instructions, and determines the processing purpose or means of processing themselves, the Processor will be considered to be a Controller in respect of that processing.

14.5. **Contract Management/Supplier assurance**

Waterways Ireland managers must build into contract management sufficient checking activities to ensure contractors are meeting their obligations under the GDPR as the Processor. These supplier assurance activities may include audits undertaken by Waterways Ireland or a third party auditor. If obligations are not being met, Waterways Ireland is obligated to take urgent remedial action with the supplier to address issues and risks.

14.6. **Using Framework Agreements**

When awarding contracts from established Framework Agreements, managers must ensure that the terms of the Framework Agreement have been updated to incorporate GDPR clauses and requirements. The Office of Government Procurement (OGP) in Ireland has updated templates for tender documents to take account of GDPR. Templates for Northern Ireland will be made available

through the Central Procurement Directorate (CPD) within the Department of Finance.

14.7. **Contract Liabilities**

Managers must not accept liability clauses where Processors are indemnified against fines or claims under GDPR. The legal penalty regime has been extended directly to Processors to ensure better performance and enhanced protection for personal data, therefore entirely indemnifying Processors for any GDPR fines or court claims would undermine these principles. Similarly, Waterways Ireland must not indemnify itself against any fines or claims imposed on Waterways Ireland under GDPR through clauses aimed at transferring the cost of fines to suppliers.

14.8. **Contract Termination/ Expiry**

Upon termination or expiry of a contract the contractor must return all requested documents and personal data to Waterways Ireland as soon as reasonably practicable, or comply with the exit arrangements in the contract.

14.9. **Cost of Compliance**

Managers must not accept contract price increases from contractors as a result of work associated with GDPR compliance. Such costs are considered to be the cost of doing business in the EU.

14.10. **Contracts of service not requiring the processing of personal data**

Whilst recognising that a contract of service which does not include a responsibility to process personal data on Waterways Ireland's behalf, does not carry GDPR risks, it is important to safeguard against any unauthorised processing of personal data throughout the duration of such contracts. To mitigate against any potential risk, the following GDPR obligation clause must be incorporated into all such contracts:

General Data Protection Regulation (GDPR) Obligation Clause

"This contract does not include the processing of personal data on behalf of Waterways Ireland. Should it become necessary to process personal data on behalf of Waterways Ireland during the period of this contract, the Contractor may only do so with the prior written agreement and instructions of Waterways Ireland, this in the form of a signed General Data Protection Regulation (GDPR) Addendum to Contract, which in effect obligates the Contractor to act in compliance with the General Data Protection Regulation and associated Data Protection Act. Waterways Ireland does not accept liability for the actions, inactions or activities of the Contractor in relation to their compliance with the General Data Protection Regulation or associated legislative provisions".

15.0 Data Sharing

The disclosure of personal data by Waterways Ireland to a third party organisation or organisation(s) or the sharing of personal data between different divisions or sections of Waterways Ireland is called Data Sharing.

Regions or sections must not share personal data without the prior approval of a Director or the Chief Executive, having regard to the legal basis for sharing the data, the existence or need for a Data Sharing Agreement, guidance from the supervisory authorities, and legal advice as may be required.

15.1. **Types of Data Sharing**

Data sharing can be either:

(i) Systematic, routine data sharing where the same data sets are shared between the same organisations for an established purpose;

(ii) Exceptional, one-off decisions to share data for any of a range of purposes.

15.2. **Data Sharing Agreements**

Where the need and justification for data sharing has been demonstrated and approved by either a Director or the Chief Executive, and there is no legal obligation to share the data, a Data Sharing Agreement must be drawn up and signed by all organisations involved in the data sharing, prior to disclosing the personal data. The Agreement must clearly set out the purpose of the data sharing and the rules to be adopted by the various organisations to which it relates. It should be reviewed regularly where the information to be shared is on a large scale or on a regular basis. A Data Sharing Agreement pro forma will be made available by the Data Protection Officer (**see Appendix D).**

16.0 Our obligations to carry out Data Protection Impact Assessments (DPIA)

A Data Protection Impact Assessment is a legal requirement for certain listed types of processing, or any other processing that is likely to result in high risk to individuals' interests. A DPIA should always be carried out with prior advice from the Data Protection Officer.

An effective DPIA enables Waterways Ireland to appropriately assess the risks associated with particular data processing activities and put in place measures to effectively mitigate risks. DPIAs form part of Waterways Ireland's accountability obligations and demonstration of GDPR compliance. A failure to carry out a DPIA may result in a Data Protection breach, damage to individual Data Subjects and resulting fines imposed by the supervisory authorities.

A DPIA is not a one off exercise for file reference. It is a living process through the risk mitigation measures put in place and therefore the DPIA must be kept under review to consider if anything changes. For example, if a Region/Section makes any significant changes to how or why they process personal data, or to the amount of data collected, the DPIA will need to be reviewed to assess any new risks. Or if a new security issue is raised, new technology is made available, or concerns are raised regarding Waterways Ireland's processing of personal data then this requires a reconsideration of the DPIA.

If a DPIA reveals that the risk of processing is high and cannot be mitigated, Waterways Ireland is required to consult the relevant supervisory authority before starting the data processing. Advice from the supervisory authority may include a formal warning not to process the data or ban the processing altogether.

16.1. **Assessing if you need to do a Data Protection Impact Assessment**

Where managers plan to store or process personal data in new ways, it is necessary to consider the risks and decide whether or not a Data Protection Impact Assessment (DPIA) is required. The supervisory authorities also advise that a DPIA should be carried out for any major project which requires the processing of personal data.

Under Article 35 of GDPR, it is mandatory to carry out a DPIA in the following circumstances:

- Use of systematic and extensive profiling with significant effects
- Large scale use of sensitive data
- Systematically monitoring of public accessible places on a large scale

Additionally, the supervisory authorities require a DPIA to be carried out if we plan to:

- Use new technologies
- Use profiling or special category data to decide on access to services
- Profile individuals on a large scale
- Process biometric data
- Match data or combine datasets from different sources
- Collect personal data from a source other than the individual without providing them with a Privacy Notice (Invisible Processing)
- Track individuals' location or behaviour
- Profile children or target marketing or online services at them, or
- Process data that might endanger the individual's physical health or safety in the event of a security breach.

16.2. **Exceptions to the need to carry out a Data Protection Impact Assessment**

Waterways Ireland is not required to carry out a DPIA if:

- The planned data processing does not identify individuals. However, it is important to be aware that what may appear to be 'anonymised' data could become identifiable data if used with other information. It is therefore necessary that anonymised data is given careful consideration to ensure that it will not identify individuals.

- Waterways Ireland is carrying out the processing of personal data on the basis of a legal obligation or public task/function in exercise of its official authority. This exception only applies if:

(i) We have a clear statutory basis for the processing
(ii) The legal provision or statutory code specifically provides and regulates the processing operation in question
(iii) We are not subject to other government obligations to complete DPIAs
(iv) A DPIA was carried out as part of the impact assessment when the legislation was introduced

- We have already carried out a DPIA and can demonstrate that the nature, scope, context and purposes of the processing are all similar.

- A DPIA is not required as a result of further guidance from the supervisory authorities.

16.3. **When and how to carry out a Data Protection Impact Assessment**

A DPIA must be carried out before Waterways Ireland begins collecting personal data and should be carried out with prior advice from the Data Protection Officer. The DPIA should be carried out using the pro forma provided in Appendix I or otherwise issued by the Waterways Ireland Data Protection Officer**.** The completed DPIA should be signed off by your Director, Regional Manager or equivalent and copied to the Data Protection Officer.

17.0 Training

17.1. Waterways Ireland will ensure that all employees are appropriately trained on Data Protection requirements and their obligations under GDPR, associated Acts and this policy. Data Protection training will be provided to all new staff and to existing staff on a regular basis.

17.2. Training will initially be provided by the Data Protection Officer or an appointed contractor, and thereafter reinforced by each Region or Section Manager to achieve ongoing compliance with this policy.

17.3. Varying training interventions will be used to reflect different levels of responsibility in relation to the collection and processing of personal data. Such training will include seminars, one-to-one guidance and instructions, on-line learning modules, and the issue of information circulars.

17.4. Requests for training and/or advice in relation to the implementation of Data Protection legislative requirements should be obtained through the Data Protection Officer (**see Appendix D)**.

18.0 Incident Reporting

18.1. Waterways Ireland has a responsibility to monitor all incidents that may breach security/confidentiality of information. All such incidents should be reported to the Data Protection Officer (see Appendix D).

18.2. Where incidents of breach or potential breach occur, the Data Breach and Incident Handling Guidelines should be followed, these requiring that any incident or suspected incident of data breach be immediately reported to the Data Protection Officer (**see Appendix D**). The Data Protection Officer will, following an initial investigation of the incident, make a determination as to whether it is necessary to notify the Information Commissioner's Office or the Data Protection Commission within 72 hours of the incident taking place. The Data Subject will also be notified unless the breach is considered not likely to be a risk to the Data subject.

19.0 How to make a Data Protection Complaint

If you wish to make a complaint regarding the way we have collected or processed your personal information, or the exercise of your rights under GDPR, please contact our Data Protection Officer by telephone, written or email correspondence as detailed below.

Caroline McLoone
Data Protection Officer
Waterways Ireland
2 Sligo Road
Enniskillen
Co Fermanagh
BT74 7JY

Email: data.protection@waterwaysireland.org
Tel: +44 (0)28 66346239

Please be assured that all complaints received will be fully investigated. To enable us address your complaint quickly and effectively resolve it, we ask that you provide us with as much information as possible.

19.1. **Role of the Information Commissioner's Office UK and the Data Protection Commission in Ireland**

If you are dissatisfied with the Data Protection Officer's findings in relation to your complaint, you have the right to complain to either the Information Commissioner's Office in the UK or the Data Protection Commission in Ireland. These are the supervisory authorities who enforce Data Protection legislation on behalf of the UK and Irish governments.

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
England, SK9 5AF

Email: casework@ico.org.uk
Tel: 0044 (0)303 123 1113
www.ico.org.uk

Data Protection Commission
Canal House
Station Road
Portarlington
Co Laois, R32 AP23

Email: info@dataprotection.ie
Tel: 00353 (0761) 104 800
www.dataprotection.ie

Dublin office:- **Data Protection Commission**
21 Fitzwilliam Square
Dublin 2
D02 RD28

In your communication to either the Information Commissioner's Office UK or the Data Protection Commission in Ireland, you should clearly identify the organisation or individual you are complaining about. You should also outline the steps you have taken to have your concerns dealt with by the organisation and the response you have received. You should provide copies of any letters between you and the organisation as well as supporting evidence/material. They will then address the matter on your behalf.

Appendix A

Glossary of Policy Terms

General Data Protection Regulation (GDPR)

Term	Meaning
Personal Data	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. **NOTE:-** **Personal data is information which:-** 1. Is processed by means of equipment operated automatically in response to instructions given for that purpose; or 2. Is recorded with the intention that it should be so processed; or 3. Is recorded as part of a relevant structured filing system or with the intention that it will form part of such a system. **Personal Data includes:-** **Automated data:** • Computer records; • Audio/video; • CCTV and digitised images; **Manual data:** • Paper files; • Card index systems;
Special Categories of Personal Data	GDPR refers to sensitive personal data as '**Special Categories of Personal Data**'. This relates to an identifiable living person but reveals any of the following:- ▪ Race or ethnicity ▪ Political opinions ▪ Religious or similar beliefs or other beliefs ▪ Physical or mental health ▪ Genetic data ▪ Sexual orientation ▪ Trade union membership ▪ Biometrics (where used for ID purposes) While the following are not listed as special categories of personal data, they are awarded additional protections: (i) Children's Data (ii) Criminal Data

Term	Meaning
Data Subject	An individual who is the subject of the data held
Processing	Any operation or set of operations which is performed on personal data or on sets of personal data, whether or not 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.
Restriction of Processing	The marking of stored personal data with the aim of limiting their processing in the future.
Profiling	Any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular analyse or predict aspects concerning the natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.
Pseudonymisation	The processing of personal data in such a manner that the personal data can no longer be attributed to a specific Data Subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.
Structured Filing System	Any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis. The personal data is structured either by reference to individuals or by reference to criteria relating to a particular individual.
Controller	The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by union or member state law, the Controller or the specific criteria for its nomination may be provided for by union or member state law. Waterways Ireland is the Data Controller for most data processing activities it undertakes.
Processor	A natural or legal person, public authority, agency or other body which processes personal data on behalf of the Controller. Waterways Ireland is the Data Processor in some circumstances e.g. Her Majesty's Revenue and Customs (HMRC) and the Office of the Revenue Commissioners in Ireland. We also engage Data Processors to provide certain services on our behalf e.g. our Information Technology (IT) department.
Recipient	A natural or legal person, public authority, agency or

Term	Meaning
	another body, to which the personal data are disclosed, whether a third party or not. Public authorities which may receive personal data in the framework of a particular inquiry in accordance with legislation shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing.
Third Party	A natural or legal, public authority, agency or body other than the Data Subject, Controller, Processor and person who, under the direct authority of the Controller or Processor, are authorised to process personal data.
Data Protection Officer	The contact person within Waterways Ireland who is responsible for the effective compliance with Data Protection legislation and providing advice and guidance.
Consent of the Data Subject	Any freely given, specific, informed and unambiguous indication of the Data Subjects 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.
Personal Data Breach	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.
Genetic Data	Personal data relating to the inherited or acquired genetic characteristics of a natural person which gives unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question.
Biometric Data	Personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or fingerprints.
Data Concerning Health	Personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status.
Representative	A natural or legal person who is designated by the Controller or Processor in writing represents the Controller or Processor with regard to their respective data protection obligations.
Supervisory Authority	An independent public authority which is established by governments to monitor the implementation of Data Protection legislation. This is the Information Commissioner's Office in the UK and the Data Protection Commission in Ireland.

Appendix B

Data Breach and Incident Handling Guidelines

1.0 Introduction

1.1 Waterways Ireland has responsibility to monitor all incidents that occur within the organisation that may breach security/confidentiality of information.

1.2 All incidents need to be identified, reported, investigated and monitored. It is only by adopting this approach that Waterways Ireland can prevent reoccurrence of such incidents.

NOTE
These guidelines do not apply to serious incidents where the principles of computer forensics should be applied to ensure that evidence gathered is admissible in court. In such cases the Data Protection Officer will seek professional advice/assistance, including from the Police Service of Northern Ireland (PSNI) or Garda Siochána where necessary.

2.0 Types of information security incidents

2.1 Breaches of information security/confidentiality could potentially compromise business operations and be damaging to Waterways Ireland as a whole. Such breaches could also pose a threat to the personal safety or privacy of an individual(s) and lead to disciplinary action and possibly legal sanctions.

2.2 Examples of these types of incidents include:

- Damage to or theft/loss of personal information (either manual or electronic);
- Leaving personal information/records in a public area;
- Incorrect disposal of personal information where no longer required;
- Unauthorised access to personal information;
- Unauthorised disclosure of personal information in any format including verbally;
- Transfer of personal information to the wrong person (by email, post or phone);
- Sharing of computer IDs and passwords.

2.3 Every breach must be taken seriously and reported according to the process as follows. If there is any doubt about what constitutes a security incident, staff should contact the Data Protection Officer.

3.0 Reporting of incidents

3.1 Any incident or suspected incident must be reported immediately to a line manager as an information loss/breach, and thereafter the Data Protection

Officer (**see Appendix D).** If the member of staff prefers to remain anonymous, a name need not be supplied.

3.2 This may involve staff reporting observed or suspected incidents or actions of others where security is threatened (**refer to the Waterways Ireland Employee Code of Conduct Policy).**

4.0 Incident investigation, recording and outcomes

4.1 The Data Protection Officer will make an initial assessment of the significance of the loss and whether further action and/or investigation is warranted – to include an assessment of potential adverse consequences for individuals and how likely these are to happen.

4.2 The Data Protection Officer will establish who needs to be made aware of the breach and action for containment, including notification of affected individuals and relevant organisations.

4.3 If a large number of people are affected or there are potentially very serious consequences arising from the breach, the Data Protection supervisory authorities, the Information Commissioner's Office (ICO) or the Data Protection Commission will be informed within 72 hours of first becoming aware of the breach, and if appropriate the Police Service of Northern Ireland or An Garda Siochána.

4.4 Notification of individuals and organisations will be carried out in accordance with the ICO guidance on data security breach management.

4.5 Where appropriate, the Data Protection Officer or nominee will lead an investigation to establish the circumstances of the incident, the extent of any loss and the implications for the organisation.

4.6 Where the Data Protection Officer assesses that an independent investigation is required, for example in the event of a significant incident or where the circumstances are particularly complex, Internal Audit may be asked to lead a more thorough investigation, which may involve interviewing staff or third parties involved.

4.7 Where an incident has occurred through a staff member's failure to apply Waterways Ireland's policy with respect to information management the Head of Human Resources and Director of Finance & Personnel may be consulted. Negligent or malicious action by an employee resulting in a data breach may lead to disciplinary action.

4.8 A report will be produced by the Data Protection Officer or Internal Audit, setting out the circumstances, extent and implications of the incident together with recommendations for preventing any subsequent similar incident, where relevant.

4.9 The Data Protection Officer will take action to ensure that lessons learned from the incident are applied to existing policies and practices. This may include implementing changes to or introducing additional systems of control, increasing awareness of information risk, or disseminating lessons learnt.

4.10 The Data Protection Officer will ensure incidents are logged to enable a central register to be maintained of all incidents occurring within the organisation.

5.0 Theft/loss of IT Equipment

5.1 All incidents relating to breaches of security and confidentiality where there has been a theft/loss of IT equipment must be reported immediately to the Head of IT.

Appendix C

Data Protection Quarterly Compliance Checklist

SECTION / DIVISION / REGION	
PERIOD	
COMPLETED BY	
DATE	

1.	**Processing Personal Data**	**YES**	**NO**	**N/A**
1.1.	We have documented and reviewed the personal data (PD) processed, where it comes from, who it is shared with and how long it is held for on the GDPR Record of Processing Activities [ROPA]	☐	☐	☐ Don't process PD
1.2.	We have identified and documented our lawful basis for processing personal data on the GDPR ROPA (Column V).	☐	☐	☐
1.3.	If "Consent" [Article 6(1)(a)] is used as a lawful basis, we have a process in place to manage that consent. Ref Paras 7.0 & 9.0 in DP Policy. *If **NO**, please provide details in Annex A*	☐	☐	☐ Consent not used
1.4.	We have identified where "Special Category" data is being processed. Ref Para 10.0 in DP Policy. *If **NO**, please detail how Special Category data is processed and risks mitigated in Annex A*	☐	☐	☐ Don't process Special Category PD
2.	**Data Protection - Individual's Rights**	**YES**	**NO**	**N/A**
2.1.	We have provided privacy information to individuals, when we are collecting their personal data or have considered that Privacy Notice is adequate *If **NO**, please detail reasons why in Annex A*	☐	☐	☐
2.2.	We can recognise Subject Access Requests and are aware of the procedure for responding. *Appendix E in DP Policy.*	☐	☐	☐
2.3.	We are aware of the other rights available to individuals under the GDPR and the process for responding. Ref Para 11 DP Policy.	☐	☐	☐
3.	**Data Protection - Technical and Organisational Measures**	**YES**	**NO**	**N/A**
3.1.	We are aware of the policies and guidance on processing personal data, and have incorporated them into our procedures. *If **NO**, please detail measures in place in Annex A*	☐	☐	☐
3.2.	We are satisfied that staff at all levels have the appropriate level of awareness and training on GDPR and personal data If ***NO***, *please detail details in place in Annex A*	☐	☐	

	YES	NO	N/A
3.3. Have you invited NEW tenders since the last reporting period?	☐	☐	
3.4. When you invite Tenders for service contracts, have you issued the Declaration of Compliance with GDPR for Tendering Purposes? (see Appendix G of policy). *If **NO**, please detail reasons and mitigations in Annex A*	☐	☐	☐ Don't invite tenders
3.5. Where contractors are engaged to process personal data on Waterways Ireland's behalf, are signed GDPR compliant contract clauses or Addendums in place (see Appendix H of policy). *If **NO**, please detail reasons and mitigations in Annex A*	☐	☐	☐ None engaged
3.6. Is the general GDPR contract clause included in all signed contracts of service which do not involve the processing of personal data? (see section 14.10 of policy). *If **NO**, please detail reasons and mitigations in Annex A*	☐	☐	☐ No contracts in place
3.7. Have any NEW third-party data sharing/processing relationships been established since last reporting period? *If **YES**, please provide details in Annex A*	☐	☐	
3.8. We have a process for removing personal data when it is no longer needed, including where that data is processed by another body under contract *If **NO**, please detail reasons why in Annex A*	☐	☐	☐
3.9. Staff know the identity of the Data Protection Officer	☐	☐	
4. Privacy	**YES**	**NO**	**N/A**
4.1. We understand that a Data Protection Impact Assessment (DPIA) is required when considering any policy or process, and integrate Data Protection into our processing activities *Appendix I of DP Policy*	☐	☐	☐
4.2. Have you have completed or are working on a DPIA? ***If YES, please provide details at Annex A***	☐	☐	
4.3. Personal data is always stored securely and access controlled *If **NO**, please detail measures in place in Annex A*	☐	☐	
4.4. We are aware of the Data Breach and Incident Handling Guidelines and follow it when required *Appendix B of DP Policy*	☐	☐	
4.5. Have you had any Data Loss or Data Breach incidents since last reporting period? *If **YES**, please provide detail on Annex A*	☐	☐	
4.6. We know when personal data is processed outside the **EEA** and have ensured adequate protection for the data. Note: UK is now outside the EEA. *If **NO**, please detail measures in place in Annex A*	☐	☐	☐
4.7. We know when personal data is processed outside the **UK** and have ensured adequate protection for the data. *If **NO**, please detail measures in place in Annex A*	☐	☐	☐

5.	Records Management	YES	NO	N/A
5.1.	We are aware of the Record Management Policy and have incorporated this into our processes	☐	☐	
5.2.	We have applied the Retention & Disposal Schedule to all records	☐	☐	
*If **NO**, please detail measures in place in Annex A*				

Annex A

Data Protection Compliance Checklist
Further Details On Responses

No.	Further Details

Appendix D

Waterways Ireland Data Protection Officer Contact Details

Caroline McLoone
Data Protection Officer
Waterways Ireland
2 Sligo Road
Enniskillen
County Fermanagh
BT74 7JY

Telephone: +44 (0) 28 6634 6239

Email: data.protection@waterwaysireland.org

Appendix E

Waterways Ireland Subject Access Request Form

A request for disclosure of your Personal Data under
the UK or Ireland Data Protection Acts 2018
and Section 12 of our Data Protection Policy 2018

Your Rights

Subject to certain exemptions, you have a right to be told whether any personal information is held about you **(the Data Subject),** the reason(s) why it is being held and who uses that information. You also have a right to a copy of that information. This includes images captured by CCTV.

Please read our Privacy Notice at https://www.waterwaysireland.org/privacy-notice to learn more about your Data Protection Rights and how Waterways Ireland as a Data Controller collects and secures personal data.

You can also obtain a copy of this Privacy Notice by contacting the Data Protection Officer:

Telephone: +44 (0) 28 6632 3004
Email: data.protection@waterwaysireland.org

Waterways Ireland's Rights

Waterways Ireland is only required to give you the information you are seeking if it is satisfied as to your identity. We are not required to provide information if someone else can be identified from it, unless that person consents to the disclosure, and we may deny access to personal information where it is allowed by the Data Protection Acts. However, in any event, we will respond to your Subject Access Request within 1 calendar month of receipt, if you have supplied us with acceptable proof of identity and assist us in locating the required information, if any.

If it is necessary for us to extend the deadline for response to you by a further 2 months due to the complexity of your request or the number of requests we are dealing with, we will inform you of this time extension within 1 calendar month of receiving your request and give you the reasons for the delay.

If you wish to find out what information, if any, may be held about you then please complete **all relevant sections on** this Subject Access Request form.

Sections 1,2 and 3 require you to give sufficient information about yourself as the applicant (and the data subject if applicable) to help Waterways Ireland confirm your identity. We have a duty to ensure that the personal information which we hold is secure, and we must be satisfied that you are who you say you are. Section 4 requires you to enclose evidence of your identity with your application. Sections 5 and 6 will help us locate the information you have requested.

When completing this Subject Access Request form, please use block capitals and black ink.

Section 1: Applicant Details

Applicant Surname: …….. Title: Mr/Miss/Mrs ……

Forename(s): ……**Date of Birth**……

Address: ……

……

……

Post Code: ……**Country** ……

Day Time Telephone No……..
(A telephone number would be helpful in the event that we need to contact you about this Subject Access Request)

Email: ……

Section 2: Verification

Are you the Data Subject? **Yes/No**
(*If Yes, please proceed to Section 3, if No, please fill in the rest of section 2 below).*

Please attach a copy of the authority you have to act on the Data Subject's behalf.
Note: This request will not be processed unless accompanied by such evidence of authority.

For use by Agents of the Data Subject only:
Please provide the full name of the Data Subject, Date of Birth and address below:

Surname: …….. Title: Mr/Miss/Mrs ……..

Forename(s): …… **Date of Birth** …….

Address: ……..……

……

……

Post Code: ……**Country …**……..…

Day Time Telephone No……..

Email: ……..

Section 3: Data Subject – Additional Personal Details

If any data which may be held about you/Data Subject is likely to include a name or address which is different to that given in section 1 or 2, please give details below:

Pervious Surname/Maiden Name: ……..……

Address: ……..…

……

……

Post Code: ……**Country …**……

Section 4 : Data Subject – Proof of Identity

To help Waterways Ireland establish your identity as the Data Subject, please enclose with your application a copy of one of the following documents to confirm your name, address and date of birth:

(a) Passport
or,
(b) Drivers Licence

If you do not hold either of the above documents, please provide

(c) A copy of an alternative form of official photographic ID or other official identification

If requesting CCTV, the photographic ID must have a recent, full face photograph.

Section 5 : Nature of Subject Access Request

Data requested: (Please describe the data which you are seeking as precisely as you can. The more precise you can be the better able we will be able to assist you. Continue on a separate sheet if necessary):

Section 6: CCTV requests only

Please provide further information which will help to locate the images you are requesting (the date, time (2 hour period maximum) and location must be provided, a description of what you are wearing and any other person you are with would be helpful, and if the request involves a vehicle, property or any other useful information, please provide here) :

Approximate Height ……..

……

……

……

……

……

Section 7: Declaration

I declare that the information given in this Subject Access Request form is correct.

Name: ……..

Signed: ……..

Dated: ……

Please send the completed Subject Access Request form and proof of identity by post or email to the following address:-

Data Protection Officer
Waterways Ireland
2 Sligo Road
Enniskillen
County Fermanagh
BT74 7JY

By email to data.protection@waterwaysireland.org

Data Protection Act Declaration: The data gathered by this form will be used to process your request under the Data Protection Acts 2018. It will be held by the Data Protection Officer and may be transferred to other parts of Waterways Ireland for the purposes of verifying your identity or processing your request for data. The data will be held for 7 years from the date when we responded to your request, unless your request forms part of an ongoing case, in which case the data will be kept for as long as is necessary.

Office use only

Date Subject Access Request received: ……

Waterways Ireland File reference……..

Application form checked: ☐

Identification forms checked: ☐

Details of identification documents received:

……

……

Name of Waterways Ireland official who processed the Subject Access Request

……..……...

Position: …….

Location: ……

Date request completed: …….

Signature: ……..

Appendix F

Waterways Ireland Data Protection Decision Makers

Decision makers referred to in this policy are senior staff members acting on behalf of the Chief Executive with delegated responsibility to make recommendations/ decisions regarding the 'Rights of Data Subjects'. The following staffing grades will be considered as Decision Makers regarding the implementation of this Data Protection policy.

- Directors
- Regional Managers
- Heads of Function or equivalent
- Senior Engineers or equivalent

Appendix G

Declaration of Compliance with the General Data Protection Regulation (GDPR) for Tendering Purposes

1. Please read Waterways Ireland's GDPR Privacy Notice posted on our website at https://www.waterwaysireland.org/privacy-notice

2. We confirm that all Data Subjects whose Personal Data is provided in our Tender have consented to the processing of such Personal Data by us, the Contracting Authority, the Evaluation Team and the supplier of the etenders.gov.ie website, for the purposes of our participation in this Competition or that we otherwise have a legal basis for providing such Personal Data to the Contracting Authority for the purposes of our participation in this Competition and that we will provide evidence of such consent and/or legal basis to the Contracting Authority upon request if required.

3. The personal information provided in relation to this tender will be used for;
    - Tender Assessment
    - Audit Requirements, and
    - To demonstrate Health & Safety Competency

    This information will be retained for no longer than is necessary and in accordance with Waterways Ireland's Retention & Disposal Schedule.

4. We confirm that we have read and understood Waterways Ireland's published GDPR Privacy Notice.

Signed By:_____

Print Name:_____

For and on Behalf of:_____

Date:_____

Appendix H (**SCHEDULE 1A)**
(Version 22nd June 2018)

GDPR STANDARD CLAUSES OF CONTRACT
For contractors engaged to process Personal Data on Waterways Ireland's behalf

Waterways Ireland requires all contractors engaged in the processing of **Personal Data** to sign and implement this GDPR Addendum to contract, in compliance with the EU General Data Protection Regulation (EU-GDPR) which became effective from 25 May 2018 and the UK General Data Protection Regulation (UK-GDPR) which took effect on 31 January 2020.

GDPR DEFINITIONS FOR IMMEDIATE REFERENCE

EU-GDPR: the General Data Protection Regulation *(Regulation (EU) 2016/679)*

UK-GDPR: the UK General Protection Regulation

LED: Law Enforcement Directive *(Directive (EU) 2016/680)*

Data Protection Legislation: (i) the GDPR, the LED and any applicable UK and Ireland implementing Laws as amended from time to time (ii) Ireland Data Protection Act 2018 and the UK Data Protection Act, 2018 as amended by the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations, 2019 (UK) to the extent that they relate to processing of personal data and privacy; (iii) all applicable Law about the processing of personal data and privacy.

Data Controller: is a natural or legal person or organisation which determines the purposes and means of processing personal data. Waterways Ireland is the Data Controller in the case of contracts awarded by the body.

Data Processor: is a natural or legal person or organisation which processes personal data on behalf of a Controller. The Contractor awarded such a contract by Waterways Ireland is the Data Processor acting on our behalf.

Sub-processor: any third Party appointed to process Personal Data on behalf of the Contractor related to this Agreement.

Data Protection Officer: the contact persons appointed both by the Controller and the Processor responsible for the effective compliance with Data Protection legislation and providing advice and guidance.

Personal data: is data that relates to an identifiable living person i.e. the **'Data Subject'.** For example, this could include a person's:-

- Name
- Address

- Phone number
- Date of Birth
- Bank Details
- Email Address

Special Categories of Personal Data: GDPR refers to sensitive personal data as 'Special Categories of Personal Data'. This relates to an identifiable living person but reveals any of the following:-

- Race or ethnicity
- Political opinions
- Religious or similar beliefs or other beliefs
- Physical or mental health
- Sexual orientation
- Trade Union Membership
- Biometrics (where used for ID purposes)

Note: GDPR applies to both automated and manual filing systems which hold personal and sensitive data, where such data are accessible according to specific criteria.

Data Subject Access Request: a request made by, or on behalf of, a Data Subject in accordance with rights granted pursuant to the Data Protection Legislation to access their Personal Data.

Protective Measures: appropriate technical and organisational measures which may include: pseudonymising and encrypting Personal Data, ensuring confidentiality, integrity, availability and resilience of systems and services, ensuring that availability of and access to Personal Data can be restored in a timely manner after an incident, and regularly assessing and evaluating the effectiveness of such measures adopted by it.

Data Protection Impact Assessment: an assessment by the Controller of the impact of the envisaged processing on the protection of Personal Data.

Personal Data Breach: 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.

Data Loss Event: any event that results, or may result, in unauthorised access to Personal Data held by the Contractor under this Agreement, and/or actual or potential loss and/or destruction of Personal Data in breach of this Agreement, including any Personal Data Breach.

1. DATA PROTECTION CONTEXT

1.1 The Parties acknowledge that for the purposes of the Data Protection Legislation, the Client is the Controller and the Contractor is the Processor. The only processing that the Contractor is authorised to do is listed herein at Appendix H, Schedule 1B by the Client and may not be determined by the Contractor.

1.2 The Contractor shall notify the Client immediately if it considers that any of the Client's instructions infringe the Data Protection Legislation.

1.3 The Contractor shall provide all reasonable assistance to the Client in the preparation of any Data Protection Impact Assessment prior to commencing any processing. Such assistance may, at the discretion of the Client, include:

(1.3.1) a systematic description of the envisaged processing operations and the purpose of the processing;

(1.3.2) an assessment of the necessity and proportionality of the processing operations in relation to the services;

(1.3.3) an assessment of the risks to the rights and freedoms of Data Subjects; and

(1.3.4) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of Personal Data.

1.4 The Contractor shall, in relation to any Personal Data processed in connection with its obligations under this Agreement:

(1.4.1) process that Personal Data only in accordance with **Schedule 1B**, unless the Contractor is required to do otherwise by Law. If it is so required the Contractor shall promptly notify the Client before processing the Personal Data unless prohibited by Law;

(1.4.2) ensure that it has in place Protective Measures, which have been reviewed and approved by the Client as appropriate to protect against a Data Loss Event having taken account of the:

(i) nature of the data to be protected;

(ii) harm that might result from a Data Loss Event;

(iii) state of technological development; and

(iv) cost of implementing any measures;

(1.4.3) ensure that:

(i) the Contractor Personnel do not process Personal Data except in accordance with this Agreement and Schedule 1B herein);

(ii) it takes all reasonable steps to ensure the reliability and integrity of any Contractor Personnel who have access to the Personal Data and ensure that they:

(a) are aware of and comply with the Contractor's duties under this clause;

(b) are subject to appropriate confidentiality undertakings with the Contractor or any Sub-processor;

(c) are informed of the confidential nature of the Personal Data and do not publish, disclose or divulge any of the Personal Data to any third Party unless directed in writing to do so by the Client or as otherwise permitted by this Agreement; and

(d) have undergone adequate training in the use, care, protection and handling of Personal Data; and

(1.4.4) not transfer Personal Data outside of the EU unless the prior written consent of the Client has been obtained and the following conditions are fulfilled:

(i) the Client or the Contractor has provided appropriate safeguards in relation to the transfer (whether in accordance with GDPR Article 46) as determined by the Client;

(ii) the Data Subject has enforceable rights and effective legal remedies;

(iii) the Contractor complies with its obligations under the Data Protection Legislation by providing an adequate level of protection to any Personal Data that is transferred (or, if it is not so bound, uses its best endeavours to assist the Client in meeting its obligations); and

(iv) the Contractor complies with any reasonable instructions notified to it in advance by the Client with respect to the processing of the Personal Data;

(1.4.5) at the written direction of the Client, delete or return Personal Data (and any copies of it) to the Client on termination of the Agreement unless the Contractor is required by Law to retain the Personal Data.

1.5 Subject to clause 1.6, the Contractor shall notify the Client immediately if it:

(1.5.1) receives a Data Subject Access Request (or purported Data Subject Access Request);

(1.5.2) receives a request to rectify, block or erase any Personal Data;

(1.5.3) receives any other request, complaint or communication relating to

either Party's obligations under the Data Protection Legislation;

(1.5.4) receives any communication from the Information Commissioner's Office UK, the Data Protection Commission in Ireland, or other regulatory authority in connection with Personal Data processed under this Agreement;

(1.5.5) receives a request from any third Party for disclosure of Personal Data where compliance with such request is required or purported to be required by Law;

or

(1.5.6) becomes aware of a Data Loss Event.

1.6 The Contractor's obligation to notify under clause 1.5 shall include the provision of further information to the Client in phases, as details become available.

1.7 Taking into account the nature of the processing, the Contractor shall provide the Client with full assistance in relation to either Party's obligations under Data Protection Legislation and any complaint, communication or request made under clause 1.5 (and insofar as possible within the timescales reasonably required by the Client) including by promptly providing:

(1.7.1) the Client with full details and copies of the complaint, communication or request;

(1.7.2) such assistance as is reasonably requested by the Client to enable the Client to comply with a Data Subject Access Request within the relevant timescales set out in the Data Protection Legislation;

(1.7.3) the Client, at its request, with any Personal Data it holds in relation to a Data Subject;

(i) assistance as requested by the Client following any Data Loss Event;

(ii) assistance as requested by the Client with respect to any request from the Information Commissioner's Office UK or the Data Protection Commission in Ireland or any consultation by the Client with the Information Commissioner's Office UK or the Data Protection Commission in Ireland.

1.8 The Contractor shall maintain complete and accurate records and information to demonstrate its compliance with this clause. This requirement does not apply where the Contractor employs fewer than 250 staff, unless:

(1.8.1) the Client determines that the processing is not occasional;

(1.8.2) the Client determines the processing includes special categories of data as referred to in Article 9(1) of the GDPR or Personal Data relating to criminal convictions and offences referred to in Article 10 of the GDPR; and

(1.8.3) the Client determines that the processing is likely to result in a risk to the rights and freedoms of Data Subjects.

1.9 The Contractor shall allow for audits of its Data Processing activity by the Client or the Client's designated auditor.

1.10 The Contractor shall designate a Data Protection Officer if required by the Data Protection Legislation.

1.11 Before allowing any Sub-processor to process any Personal Data related to this Agreement, the Contractor must:

(i) notify the Client in writing of the intended Sub-processor and processing;

(ii) obtain the written consent of the Client;

(iii) enter into a written agreement with the Sub-processor which give effect to the terms set out in this clause [1.11] such that they apply to the Sub-processor; and

(iv) provide the Client with such information regarding the Sub-processor as the Client may reasonably require.

1.12 The Contractor shall remain fully liable for all acts or omissions of any Sub-processor.

1.13 The Client may, at any time on not less than 30 Working Days' notice, revise this clause by replacing it with any applicable controller to processor standard clauses or similar terms forming part of an applicable certification scheme (which shall apply when incorporated by attachment to this Agreement).

1.14 The Parties agree to take account of any guidance issued by the Information Commissioner's Office UK or the Data Protection Commission in Ireland, as is relevant to the jurisdiction of this contract. The Client may on not less than 30 Working Days' notice to the Contractor amend this agreement to ensure that it complies with any guidance issued by the Information Commissioner's Office UK or the Data Protection Commission in Ireland.

Appendix H (SCHEDULE 1B)

GDPR SCHEDULE OF PROCESSING, PERSONAL DATA AND DATA SUBJECTS

1. The Contractor shall comply with any further written instructions with respect to processing by the Client.

2. Any such further instructions shall be incorporated into this Schedule 1B.

Description	Details
Subject matter of the processing	*[This should be a high level, short description of what the processing is about i.e. its subject matter]*
Duration of the processing	*[Clearly set out the duration of the processing including dates]*

Nature and purpose of the processing	*[Please be as specific as possible, but make sure that you cover all intended purposes.* *The nature of the processing: means any operation 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 of data (whether or not by automated means) etc.* *The purpose might include: employment processing, statutory obligation, recruitment assessment etc]*

Type of Personal Data	*[Examples here include: name, address, date of birth, National Insurance Number (UK) or Personal Public Service Number (Ireland), telephone number, pay, images, biometric data etc]*
Categories of Data Subject	*[Examples include: Staff (including volunteers, agents, and temporary workers), customers/ clients, suppliers, patients, students / pupils, members of the public, users of a particular website etc]*
Plan for return and destruction of the data once the processing is complete UNLESS requirement under union or member state law to preserve that type of data	*[Describe how long the data will be retained for, how it will be returned or destroyed]*

Name of Waterways Ireland representative: …….

Signature of Waterways Ireland representative: ……

Date ……..

Name of Processor's representative: ……

Signature of Processor's representative: ……

Date ……

Appendix I

WATERWAYS IRELAND
DATA PROTECTION IMPACT ASSESSMENT PRO FORMA

The completion of this pro forma will enable you to record your Data Protection Impact Assessment (DPIA) Process and outcome in accordance with **section 16 of Waterways Ireland's Data Protection Policy**. It follows the guidance set out by the Information Commissioner's office (ICO) UK and should be read alongside the European guidelines on DPIAs which will be made available to you by the Data Protection Officer (DPO).

You should begin to complete the pro forma at the start of any major project involving the use of personal data, if you are making a significant change to an existing process, or you plan to carry out data collection or other processing activities as defined in section 16.1 of the Data Protection Policy. The final outcomes should be integrated into your project plan.

The completed DPIA must be approved and signed by a Director, Regional Manager or equivalent and copied to the Data Protection Officer.

Step 1: Identify the need for a DPIA

Explain broadly what the project aims to achieve and what type of processing it involves. You may find it helpful to refer or link to other documents, such as a project proposal. Summarise why you identified the need for a DPIA.

Step 2: Describe the processing

Describe the nature of the processing: how will you collect, use, store and delete data? What is the source of the data? Will you be sharing data with anyone? You might find it useful to refer to a flow diagram or other way of describing data flows. What types of processing identified as likely high risk are involved?

Describe the scope of the processing: what is the nature of the data, and does it include special category or criminal offence data? How much data will you be collecting and using? How often? How long will you keep it? How many individuals are affected? What geographical area does it cover?

Describe the context of the processing: what is the nature of your relationship with the individuals? How much control will they have? Would they expect you to use their data in this way? Do they include children or other vulnerable groups? Are there prior concerns over this type of processing or security flaws? Is it novel in any way? What is the current state of technology in this area? Are there any current issues of public concern that you should factor in? Are you signed up to any approved code of conduct or certification scheme (once any have been approved)?

Describe the purposes of the processing: what do you want to achieve? What is the intended effect on individuals? What are the benefits of the processing – for you, and more broadly?

Step 3: Consultation process

Consider how to consult with relevant stakeholders: describe when and how you will seek individuals' views – or justify why it's not appropriate to do so. Who else do you need to involve within your organisation? Do you need to ask your processors to assist? Do you plan to consult information security experts, or any other experts?

Step 4: Assess necessity and proportionality

Describe compliance and proportionality measures, in particular: what is your lawful basis for processing? Does the processing actually achieve your purpose? Is there another way to achieve the same outcome? How will you prevent function creep? How will you ensure data quality and data minimisation? What information will you give individuals? How will you help to support their rights? What measures do you take to ensure processors comply? How do you safeguard any international transfers?

Step 5: Identify and assess risks

Describe source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.	**Likelihood of harm**	**Severity of harm**	**Overall risk**
	Remote, possible or probable	Minimal, significant or severe	Low, medium or high

Step 6: Identify measures to reduce risk

Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in step 5				
Risk	**Options to reduce or eliminate risk**	**Effect on risk**	**Residual risk**	**Measure approved**
		Eliminated reduced accepted	Low medium high	Yes/no

Step 7: Sign off and record outcomes

Item	Name/date	Notes
Measures approved by:		Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:		If accepting any residual high risk, consult the ICO before going ahead
DPO advice provided:		DPO should advise on compliance, step 6 measures and whether processing can proceed
Summary of DPO advice:		
DPO advice accepted or overruled by:		If overruled, you must explain your reasons
Comments:		
Consultation responses reviewed by:		If your decision departs from individuals' views, you must explain your reasons
Comments:		
This DPIA will kept under review by:		The DPO should also review ongoing compliance with DPIA