Witham Fourth District Internal Drainage Board

Data Protection Policy

1 INTRODUCTION

1.1 The General Data Protection Regulation (GDPR) came into effect in May 2018. Many of the GDPR's main concepts and principles were much the same as those in the current Data Protection Act (DPA), so as we are complying properly with the current law then most of our approach to compliance remains valid under the GDPR. However, there were new elements and significant enhancements, requiring the Board to do some things differently.

1.2 The GDPR applies to controllers and processors and applies to personal data, meaning any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier, and sensitive personal data.

1.3 Sensitive personal data is personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation. The only category that applies to W4IDB is in relation to the collection of Trade Union subscriptions and data relating to health from sick notes and occupational health.

2 LAWFUL BASIS FOR PROCESSING

2.1 The requirement to have a lawful basis in order to process personal data is not new. It replaces and mirrors the previous requirement to satisfy one of the 'conditions for processing' under the Data Protection Act 1998. However, the GDPR places more emphasis on being accountable for and transparent about the Board's lawful basis for processing.

2.2 The six lawful bases for processing under GDPR are broadly similar to the old conditions for processing, although there are some differences. The Board now needs to review our existing processing, identify the most appropriate lawful basis, and check that it applies. In many cases it is likely to be the same as your existing condition for processing.

2.3 The biggest change is for public authorities, such as the Board, who now need to consider the new 'public task' basis first for most of their processing, and have more limited scope to rely on consent or legitimate interests.

2.4 We can choose a new lawful basis if you find that your old condition for processing is no longer appropriate under the GDPR, or decide that a different basis is more appropriate. Once the GDPR is in effect, it will be much harder to swap between lawful bases if the Board finds that our original basis was invalid. The Board will be in breach of the GDPR if we do not clearly identify the appropriate lawful basis (or bases, if more than one applies) from the start.

2.5 The GDPR brings in new accountability and transparency requirements. The Board should therefore make sure it clearly documents the lawful basis so that it can demonstrate its compliance in line with Articles 5(2) and 24.

2.6 The Board must now inform people upfront about the lawful basis for processing their personal data. The Board needs therefore, to communicate this information to individuals by 25 May 2018, and ensure that you include it in all future privacy notices.

2.7 The lawful bases for processing are set out in Article 6 of the GDPR. At least one of these must apply whenever you process personal data:

(a) **Consent**: the individual has given clear consent for the Board to process their personal data for a specific purpose.

(b) **Contract:** the processing is necessary for a contract the Board has have with the individual, or because they have asked the Board to take specific steps before entering into a contract.

(c) **Legal obligation:** the processing is necessary for the Board to comply with the law (not including contractual obligations).

(d) **Vital interests:** the processing is necessary to protect someone's life.

(e) **Public task:** the processing is necessary for the Board to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

(f) **Legitimate interests:** the processing is necessary for the Boards legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks.)

A register of data types held and the lawful basis to process this data is shown at Appendix 1.

3 INDIVIDUAL RIGHTS

3.1 The GDPR provides the following rights for individuals:

(a) **The right to be informed**
Individuals have the right to be informed about the collection and use of their personal data. This is a key transparency requirement under the GDPR. The board achieves this by publishing the Privacy Notice at appendix 2.

(b) **The right of access**
Individuals have the right to access their personal data and supplementary information. The right of access allows individuals to be aware of and verify the lawfulness of the processing.

(c) **The right to rectification**
The GDPR includes a right for individuals to have inaccurate personal data rectified, or completed if it is incomplete. An individual can make a request for rectification verbally or in writing.

(d) **The right to erasure**
The GDPR introduces a right for individuals to have personal data erased. The right to erasure is also known as 'the right to be forgotten'. Individuals can make a request for erasure verbally or in writing. The right is not absolute and only applies in certain circumstances. For example, it does not apply for the performance of a task carried out in the public interest or in the exercise of official authority.

(e) **The right to restrict processing**
Individuals have the right to request the restriction or suppression of their personal data. This is not an absolute right and only applies in certain circumstances. When processing is restricted, we are permitted to store the personal data, but not use it. An individual can make a request for restriction verbally or in writing.

(f) **The right to data portability**
The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services. It allows them to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability.

(g) **The right to object**
Individuals have the right to object to processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling), direct marketing (including profiling) and processing for purposes of scientific/historical research and statistics. Details of how to object are included in our Privacy Notice at appendix 2.

(h) **Rights in relation to automated decision making and profiling.**
The GDPR has provisions on: automated individual decision-making (making a decision solely by automated means without any human involvement); and profiling (automated processing of personal data to evaluate certain things about an individual). Profiling can be part of an automated decision-making process. The GDPR applies to all automated individual decision-making and profiling.

4 ACCOUNTABILITY AND GOVERNANCE

4.1 The GDPR includes provisions that promote accountability and governance. These complement the GDPR's transparency requirements. While the principles of accountability and transparency have previously been implicit requirements of data protection law, the GDPR's emphasis elevates their significance. We are expected to put into place comprehensive but proportionate governance measures. Good practice tools that the ICO has championed for a long time such as privacy impact assessments and privacy by design are now legally required in certain circumstances. Ultimately, these measures should minimise the risk of breaches and uphold the protection of personal data. Practically, this is likely to mean more policies and procedures for organisations, although many organisations will already have good governance measures in place.

4.2 **Documentation**

The GDPR contains explicit provisions about documenting the Board's processing activities. We must maintain records on several things such as processing purposes, data sharing and retention. A register can be found at appendix 1.

The Board may be required to make the records available to the ICO on request. Records must be kept in writing. Records must be kept up to date and reflect our current processing activities.

4.3 **Data protection by design and default**

Under the GDPR, the Board has a general obligation to implement technical and organisational measures to show that the Board has considered and integrated data protection into the Boards processing activities. Privacy by design has always been an implicit requirement of data protection that the ICO has consistently championed.

4.4 **Data protection impact assessments**

A data protection impact assessment (DPIA) is a process to help the Board identify and minimise the data protection risks of a project. The Board must do a DPIA for certain listed types of processing, or any other processing that is likely to result in a high risk to individuals' interests.

It is also good practice to do a DPIA for any other major project which requires the processing of personal data. To assess the level of risk, the Board must consider both the likelihood and the severity of any impact on individuals. High risk could result from either a high probability of some harm, or a lower possibility of serious harm.

This is not likely to apply to the Board but should be borne in mind.

4.5 **Data Protection Officer**

The GDPR introduces a duty for the Board to appoint a data protection officer (DPO) as we are a public authority. DPOs assist to monitor internal compliance, inform and advise on data protection obligations, provide advice regarding Data Protection Impact Assessments (DPIAs) and act as a contact point for data subjects and the supervisory authority.

The DPO must be independent, an expert in data protection, adequately resourced, and report to the highest management level. A DPO can be an existing employee or externally appointed.

Peter Bateson BA FCCA MBA Chief Executive and Finance Manager is appointed at the Boards Data Protection Officer.

4.6 **Security**

The GDPR requires personal data to be processed in a manner that ensures its security. This includes protection against unauthorised or unlawful processing and against accidental loss, destruction or damage. It requires that appropriate technical or organisational measures are used.

4.7 **Personal data breaches**

The GDPR introduces a duty on all organisations to report certain types of personal data breach to the relevant supervisory authority. The Board must do this within 72 hours of becoming aware of the breach, where feasible. If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, the Board must also inform those individuals without undue delay.

The Board should ensure it has robust breach detection, investigation and internal reporting procedures in place. This will facilitate decision-making about whether or not you need to notify the relevant supervisory authority and the affected individuals. The Board must also keep a record of any personal data breaches, regardless of whether you are required to notify.

4.8 **Children**

It is not envisaged that the personal details of children will be processed and the DPO should be consulted if this becomes a requirement.

5 DATA PROTECTION PRINCIPLES

5.1 Black Sluice Internal Drainage Board fully endorses the eight data protection principles, adhering to them at all times.

These principles are:

(a) Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless specific conditions are met.

(b) Personal data shall be obtained only for one or more specified and lawful purposes and shall not be further processed in any way incompatible with that purpose or those purposes.

(c) Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

(d) Personal data shall be accurate and where necessary, kept up to date.

(e) Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

(f) Personal data shall be processed in accordance with the rights of data subjects under GDPR.

(g) Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
(h) Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedom of data subjects in relation to the processing of personal data.

5.2 **Witham Fourth District Internal Drainage Board's commitment to the Data Protection Principles**

W4IDB will do the following to comply with the principles:

(a) Observe fully the conditions regarding the fair collection and use of information.
(b) Meet its legal obligations to specify the purposes for which information is used.
(c) Collect and process appropriate information and only to the extent that it is required to fulfil operational needs or to comply with any legal requirements.
(d) Ensure the quality of information used.
(e) Ensure that information held is erased at the appropriate time.
(f) Ensure that the rights of individuals about whom we hold information can be exercised fully under GDPR.
(g) Take appropriate technical and organisational security measures to safeguard personal information.
(h) Ensure that personal information is not transferred abroad without suitable safeguards.

5.3 **Witham Fourth District Internal Drainage Board adheres to its commitment to Data Protection by:**

(a) Allocation of specific responsibility for data protection to at least one person known as the Data Protection Officer.
(b) Ensure that employees handling personal information are supervised appropriately.
(c) Requests for access to an individual's own personal information are dealt with in a timely and courteous manner.
(d) Record any incidents of breach in data protection policy and keep a register.
(e) Undertake regular review of management of personal information and update when necessary.

5.4 **Access to personal information**

For information about how to request subject access to personal information please contact: drainage@w4idb.co.uk

Organisation Name and Contact Details		Data Protection Officer	
Name and Contact Details	Witham Fourth District IDB	Name and Contact Details	Peter Bateson
Address	47 Norfolk Street, Boston, PE21 6PP	Address	47 Norfolk Street, Boston, PE21 6PP
Email	drainage@w4idb.co.uk	Email	peter@w4idb.co.uk
Telephone	01205 310088	Telephone	01205 310088

Article 6(1)a) - Consent	
Article 6(1)b) - Contract	
Article 6(1)c) - Legal Obligation	
Article 6(1)d) - Vital interests	
Article 6(1)e) - Public Task	**Article 9(2)a) - Consent**
Article 6(1)f) - Legitimate Interests	**Article 9(2)b) - Employment**

Business Function	Purpose of Processing	Name and Contact details of joint controller (if applicable)	Category of Individual	Category of personal data	Category of recipient	General description of technical and organisational security	Article 6 lawful basis for processing personal data	Article 9 basis for processing special category data
Rating	Rating records	N/A	Ratepayers	Contact details	Public		**Article 6(1)e) - Public Task**	
Planning & Consenting	Planning consultation	Boston Borough Council	Public	Contact details	District/Borough Council	Encrypted storage	**Article 6(1)e) - Public Task**	
Planning & Consenting	Planning consultation	East Lindsey District Council	Public	Contact details	District/Borough Council	Encrypted storage	**Article 6(1)e) - Public Task**	
Planning & Consenting	Consent application	N/A	Applicant	Contact details	N/A	Encrypted storage	**Article 6(1)e) - Public Task**	
Planning & Consenting	Consent application (LCC ext area)	Lincolnshire County Council	Applicant	Contact details	N/A	Encrypted storage	**Article 6(1)e) - Public Task**	
Finance	Payroll	N/A	Employees	Contact details	HMRC	Encrypted storage/transfer	**Article 6(1)c) - Legal Obligation**	
Finance	Payroll	N/A	Employees	Bank/pension/tax details	HMRC	Encrypted storage/transfer	**Article 6(1)c) - Legal Obligation**	
Finance	Sales	N/A	Customers	Contact details	N/A	Encrypted storage	**Article 6(1)b) - Contract**	
Finance	Purchases	N/A	Suppliers	Contact details/bank details	N/A	Encrypted storage	**Article 6(1)b) - Contract**	
Human Resources	Personnel file	N/A	Employees	Contract details	N/A	Encrypted storage	**Article 6(1)b) - Contract**	
Human Resources	Personnel file	N/A	Employees	Pay & Leave records	N/A	Encrypted storage	**Article 6(1)b) - Contract**	
Human Resources	Personnel file	N/A	Employees	Sickness Records	N/A	Encrypted storage	**Article 6(1)b) - Contract**	**Article 9(2)b) - Employment**
Human Resources	Personnel file	N/A	Employees	Driver declarations	N/A	Encrypted storage	**Article 6(1)b) - Contract**	
Human Resources	Personnel file	N/A	Employees	Annual health declaration	N/A	Encrypted storage	**Article 6(1)b) - Contract**	**Article 9(2)b) - Employment**
Admin	Board Functions	N/A	Board Members	Contact details	N/A	Encrypted storage	**Article 6(1)e) - Public Task**	

PRIVACY NOTICE

We regard your privacy as important and comply with the Data Protection Act 2018 and the General Data Protection Regulations (GDPR).

We process and hold information in order to provide public services. This notice explains how we use and share your information. Information may be collected in paper or electronic form, by telephone, email or by a member of our staff.

We record personal information if:

- You contact us to inform us that you have acquired land in The Board's drainage district,
- You contact us to inform us of changes to your land ownership,
- You contact us to ask for consent to do work on a watercourse in our drainage district,
- Your details are given to us by a third party e.g. solicitor, informing us of changes in land ownership

Why we collect information

The Board collects and holds information about you, in order to:

- deliver public services under Acts of Parliament, in particular, the Land Drainage Act 1991 and the Flood and Water Management Act 2010
- confirm your identity to provide some services
- contact you by post, email or telephone
- update your ratepayer record
- allow us to undertake statutory functions efficiently and effectively
- make sure we meet our statutory obligations.

Our Right to Process Information

We are permitted to process information under GDPR Article 6 (1) (a) (b) and (e) when:

- Processing is with consent of the data subject, or
- Processing is necessary for compliance with a legal obligation, or
- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller

How we use your information

We will only use any personal information we hold for the purposes for which it was provided. We will only hold your information for as long as necessary. All employees who have access to your personal data and are associated with the handling of that data are obliged to respect the confidentiality of your data. All your communications to us are protected against unauthorised access by third parties.

The Board tries to keep the information we have about you accurate. If, however, you find errors or inaccuracies in your data, we will erase, complete or amend that information upon request.

We will process your information for the following purposes:

- to ensure that we meet our legal obligations.
- where necessary for our consenting and enforcement duties.
- where necessary to protect individuals from harm or injury.

Information sharing

Where we need to disclose your personal information to other authorities e.g. the Environment Agency, we will do so only with your prior explicit consent or where we are legally required to. We may disclose information when necessary to prevent risk of harm to an individual.

Information Security

The Board seeks to ensure the security of personal data. We make sure that your information is protected from unauthorised access, loss, manipulation, falsification, destruction or unauthorised disclosure. This is done through appropriate technical measures and appropriate policies. We will only keep your data for the purpose it was collected for and only for as long as is necessary. After which it will be deleted.

Your Rights

Access to Information

You have the right to request access to the information we have about you. You can do this by contacting our Data Controller: peter@w4idb.co.uk

Information Correction and deletion

If you believe that the information we have about you is incorrect, you may contact us so that we can update it and keep your data accurate. Please contact: peter@w4idb.co.uk

Right to Object

If you believe that your data is not being processed for the purpose it has been collected for, you may object: Please contact peter@w4idb.co.uk

To Sum Up

In accordance with the law, we only collect a limited amount of information about you that is necessary for correspondence, information and service provision. We do not use profiling, we do not sell your data, we do not pass your data to third parties without your consent. We do not use your data for purposes other than those specified. We make sure your data is stored securely. We delete all information deemed to be no longer necessary. We constantly review our Privacy Policies to keep it up to date in protecting your data.

Complaints

If you have a complaint regarding the way your personal data has been processed you may make a complaint to The Board's Data Controller: peter@w4idb.co.uk and the Information Commissioners Office

casework@ico.org.uk Tel: 0303 123 1113

Witham Fourth District Internal Drainage Board
47 Norfolk Street
Boston
PE21 6PP

Email: **drainage@w4idb.co.uk**

This Notice was last updated in November 2019.