date – September 2019

Trust in water

G2 Data Protection Policy

www.ofwat.gov.uk

Table of Contents

1 Introduction

The General Data Protection Regulation (GDPR) and Data Protection Act 2018 set out requirements for data controllers[1] and data processors[2] in relation to personal data. Ofwat needs to collect personal data about people we deal with in order to carry out our regulatory functions. Such people include employees (present, past and prospective), in some circumstances, customers of the companies we regulate, contractors and other business contacts. The personal data we collect depends on the context and source and may include name, address, email address, date of birth, private and confidential information and sensitive information. In addition, we may occasionally be required to collect and use certain types of such personal information to comply with legal requirements, for example we may need to share financial information about an individual with HMRC. No matter how it is collected, recorded and used (e.g. on a computer or on paper) this personal data must be processed lawfully, fairly and in a transparent manner, and in compliance with the GDPR and data protection legislation. This is vital in order to maintain the confidence of all of our stakeholders and to meet our legal obligations.

2 Scope of the policy

This policy applies to all employees, non-executive directors, contractors, agents and representatives including temporary staff, such as secondees and interims working for or on behalf of Ofwat.

The purpose of this policy is to set out the key measures by which Ofwat complies with the requirements of the GDPR and protects the rights and privacy of individuals.

3 Roles and Responsibilities

The Data Protection Officer (DPO) is accountable for compliance with data protection legislation for Ofwat. However the day to day management of compliance rests with the Information Governance Manager (IGM). The DPO is contactable via foi@ofwat.gov.uk All staff need to be aware of the requirements of the GDPR to ensure they are compliant when processing personal and sensitive personal data.

[1] A data controller determines the purposes and the means of processing of personal data
[2] A data processor processes personal data on behalf of a data controller

4 Identifying Information Requests and Security Breaches

As a public sector organisation, we must comply with a number of laws that mean people can request information that we hold usually within 20 working days. Anyone requesting information does not specifically have to reference the legislation under which they are making a request. All staff must read Ofwat's Access to Information policy and the guidance on Ofwat's intranet which explains how to identify these requests and how to respond to them.

All staff should ensure they are aware of relevant security procedures to minimise the risk of any data protection or other security breach. Further information can be found in Ofwat's Security policy, Information and Technology Security policy, ICT Acceptable Use Agreement and Data Breach procedure, as well as in the information set out below. Security incidents must be reported immediately via the incident reporting form on Ofwat's intranet. Any member of staff who disregards the relevant policies will face disciplinary action with potential consequences up to and including dismissal.

5 Impact Assessments

GDPR Article 35(1) says that organisations must complete an impact assessment where a type of processing is **likely to result in a high risk** to the rights and freedoms of individuals. New projects, processes or contracts which involve personal data must complete a checklist to ascertain if a full assessment is necessary. A template is accessible here and must be completed and shared with the IGM via foi@ofwat.gov.uk. Support and assistance in completing it is available from the IGM.

6 Staff Training

Ofwat aims to ensure that guidance and training to all staff is delivered at regular intervals, including training on identifying information requests, breach reporting and the requirements of undertaking data privacy impact assessments. Any changes to the relevant legislation and best practice will be reported to the Security and Information Assurance Group (SIAG) with any proposed recommendations, and to Ofwat's Programme leads in order to ensure that such changes are reflected in Ofwat's activities.

7 General Principles

Ofwat aims to be open and transparent when processing and using personal and special categories of data by ensuring we follow the principles relating to the processing of personal data as set out Article 5 of the GDPR:

Personal data shall be:

- processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1) GDPR, not be considered to be incompatible with the initial purposes ('purpose limitation');
- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');
- accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');
- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) GDPR, subject to implementation of appropriate technical and organisational measures required in order to safeguard the rights and freedoms of the data subject ('storage limitation');
- 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').

Personal data is defined as:

> "any information relating to an identified or identifiable natural person (data subject); an identifiable natural person is one who/that 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[3].

This definition should be considered in light of the extent to which the data relates to the individual's privacy in either their family life, business or professional capacity. In particular, consideration should be given to whether the information is biographical in a significant sense, or whether it has the individual as its focus.

All staff must be aware that any recorded information may be required to be provided to the public. Wherever possible Ofwat endeavours to be as transparent as possible and we aim to ensure that Government guidance on transparency is met. In some instances a statutory exemption may prevent us from disclosing certain information and in some instances we will disclose information in a redacted format.

8 Subject Access Requests (SAR)

The GDPR provides all living individuals (data subjects) with the right to obtain from a data controller confirmation as to whether personal data is held about him/her, access to that information and specific elements of information listed at Article 15 GDPR. This is referred to as a Subject Access Request.

Any request in which any individual makes a request relating to their own information should be sent to foi@ofwat.gov.uk who will manage the request in its entirety. If any member of staff is unsure as to whether a Subject Access Request has been made, advice can be obtained from the IGM or the DPO.

Individuals also have the right to request amendments or deletions if any of their personal data is inaccurate.

An SAR form can be found and downloaded on our website at the following link: https://www.ofwat.gov.uk/publication/ofwat-subject-access-request-form/

In response to requests under the Freedom of Information Act (FOIA) 2000, Ofwat may be required to disclose personal data relating to staff. In considering whether to do so, we will give due consideration to whether in all the circumstances the disclosure would be fair to the individual, and we will balance our duty of care to staff

[3] GDPR Article 4(1)

in respect of protecting their personal information from unwarranted intrusion with our legal obligations to disclose information under FOI.

When handling FOI requests for personal information there will be a presumption in favour of protecting personal privacy, and in particular our starting point in any analysis of a FOI request will be that:

a. Board and Senior Leadership Team (SLT) Members details are already located on Ofwat's website. It is not normal policy to disclose staff name details below this level unless it is reasonable to do so. There will be a presumption to disclose job titles.

b. No personal contact details will be disclosed, unless these are already in the public domain.

For more information on FOI please see Ofwat's FOI & EIR policy.

9 Contracts

All contracts with third parties that involve the processing of personal data will include specific obligations to comply with the GDPR and will make reference to specific legislation and to the third party's obligations where relevant, for example data processing and FOI.

In accordance with our transparency obligations Ofwat publishes contracts over £10,000 on the Government website Contract Finder. Personal data will be redacted (removed) before publishing unless the information is already in the public domain and considered reasonable to disclose.

10 Retention and disposal

Personal data will be held in accordance with Ofwat's Retention and Disposal policy. Further information on retention and disposal should be addressed to the IGM.

11 Complaints

If you are unhappy with a response to a request for information or you feel that the information Ofwat holds is incorrect, please contact the DPO via foi@ofwat.gov.uk. If after this you are not content with the response to your complaint, you have the right to complain directly to the Information Commissioner's office (ICO). The ICO is the independent regulator for information governance legislation.

12 Links to Any Associated Documents

ICT 2 Security Policy

ICT 4 Retention and Disposal Policy

ICT 5 Information and Technology Security Policy

ICT 6 Acceptable Use Agreement

Ofwat Code of Conduct

G1 Access to Information Policy

G2 Data Protection Policy

G3 FOI/EIR Policy

G5 Privacy Policy

Data Breach Procedure

Impact Assessment Checklist and Templates

IT Disaster Response Plan

13 Document control

Version history

Version	Status	Date	Author	Summary of changes
0.1	Draft	May 2016	SA FOI	
0.2	Draft	May 2016	SA FOI	Minor changes
0.3	Draft	25.05.2016	SA FOI	Minor changes
0.4	Draft	12.03.2018	SA FOI	Minor changes to reflect GDPR
0.5	Draft	20.03.2018	Pr Legal	Further changes to reflect GDPR
0.6	Draft	09/04/2018	SA FOI	Minor changes to reflect GDPR
0.7	Draft	24/04/2018	Dir PPM	Minor changes
0.8	Draft	03/09/2019	IGM	Minor changes

Sign off

Job Title	Date	Version No.	Date of Next review
DPO	**September 2019**	**0.8**	**September 2021**