date – 13th September 2019

Trust in water

Data Breach Procedures

www.ofwat.gov.uk

Table of Contents

1 Introduction

Data breach procedures provide a framework for all staff and are particularly relevant for an organisation that prides itself on its flexible approach and facilitation of mobile working.

Ofwat holds and processes personal data in relation to employees and water sector customers. In addition we have a substantial quantity of non-personal data, including information classifiable as 'Official Sensitive' under the Government Classification Scheme, in particular market sensitive company data. Ofwat processes that data in accordance with the relevant legal requirements, namely data protection legislation, the Government Classification guidance, rules[1] relating to market sensitive information and Section 206 of the Water Industry Act 1991.

Every care is taken to protect personal data from incidents (either accidentally or deliberately) and to avoid a data breach that could compromise security.

Any compromise of the information we hold, whether in terms of breach of confidentiality, integrity, or availability may result in harm to individual(s), reputational damage, a detrimental effect on service provision, amount to legislative non-compliance, and/or financial costs.

2 Purpose of the Policy

The purpose of this Policy is to ensure Ofwat complies with handling any data breaches in accordance with all relevant legislation and guidance binding upon us, that we respond in a consistent and effective way and that all staff are aware of their responsibilities in relation to data breaches.

Our objective is to contain any breaches, to minimise the risk associated with the breach and consider what action is necessary to secure the relevant data and prevent further breaches.

[1] The Market Abuse Regulation, and domestic implementing law i.e. Financial Services and Markets Act 2000 (Market Abuse) Regulations 2016, amending primary and secondary legislation (including the Financial Services and Markets Act 2000 (FSMA) and the Financial Services Act 2012 (FS Act 2012), as well as subsidiary FCA rules set out in the Disclosure and Transparency Rules (DTRs) and FCA handbook.

3 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. It relates specifically to how to deal with breaches or lapses in our information security management. Reference will be made to other relevant policies linked to the management of information or other areas of Ofwat security which are not covered by this policy.

This Policy relates to all personal and commercially sensitive data held by Ofwat regardless of format.

A relatively small percentage of the data that Ofwat holds is personal data. Nevertheless, this Policy covers all data breaches, including not just personal data breaches but also breaches involving other information. For example, a data breach may involve information about companies which is commercially sensitive, or about Ofwat's intended policy not yet made public. In some cases, other serious legal consequences may flow from a data breach, as well as obvious reputational and practical damage to Ofwat and its work[2].

4 What is a data breach?

A data breach is any incident where information is exposed to unauthorised or inappropriate processing, resulting in its security being compromised. The extent of damage or potential damage caused by any data breach will be determined by the volume and sensitivity of the information, and the degree of exposure which results. As technology trends change and the amount of information created increases, new ways are emerging by which data breaches can occur.

A data breach may involve information which is classified as personal data[3]. As of 25 May 2018, the General Data Protection Regulation (GDPR), supplemented by the Data Protection Act 2018, governs the processing of personal data and requires organisations to ensure that appropriate procedures are in place for the handling of data breaches involving Personal Data.

[2] For example, if the information unintentionally disclosed relates to an individual or business and was obtained by virtue of provisions of the Water Industry Act 1991 (WIA 91) – which is the case with a large quantity of the information that Ofwat holds - and the individual or business did not consent to the disclosure, then s206 WIA 91 may have been infringed, which can lead to both a fine and a prison sentence for the person who discloses it.

[3] Personal data means 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 (Article 4 GDPR)

This process applies whether a data breach originates within Ofwat or within any organisation who processes data on our behalf[4].

The GDPR defines a personal data breach as 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[5]. This also includes a temporary data breach, although depending upon the circumstances and the timeliness and effectiveness of Ofwat's response, temporary personal data breaches may require different responses from Ofwat.

A data breach may include one or more of the following elements[6]:-

- "Confidentiality breach" - where there is an unauthorised or accidental disclosure of, or access to, personal data;
- "Availability breach" - where there is an accidental or unauthorised loss of access to, or destruction of, personal data;
- "Integrity breach" - where there is an unauthorised or accidental alteration of personal data.

Examples of breach:

- Loss or theft of confidential or sensitive data or equipment on which such data is stored (e.g. loss of Surface Pro, mobile phone or paper records); attempts (failed or successful) to gain unauthorised access to information or IT system(s), e.g. hacking including where data on those systems is modified (e.g. website defacement)
- Unauthorised disclosure of sensitive / confidential data
- Unforeseen circumstances such as a fire or flood
- Human error (e.g. email containing personal data sent to incorrect email addresses)
- 'Blagging' offences where information is obtained by deceiving the organisation who holds it

5 Responsibilities

Ofwat recognises that it has a corporate responsibility to ensure that all Ofwat data is processed in accordance with any relevant legislation and guidance to which it is subject.

[4] Ofwat requires any third-party contractors who process personal data on our behalf to have in place appropriate measures to protect against data breaches and to notify us of a data breach within 24 hours.

[5] GDPR Article 4

[6] As set out in the GDPR Working Party 29 guidelines on breach process. Note that this explanation is provided in respect of personal data, but can equally be applied to data breaches concerning other types of data.

All persons covered by the scope of this policy are responsible for reporting actual, suspected, threatened or potential data breaches and for assisting with investigations as required, particularly if urgent action must be taken to prevent any or further damage.

The Data Protection Officer (DPO) is responsible for drawing up guidance on access to information, including data protection and promoting compliance with this policy in such a way as to ensure the easy, appropriate and timely management of incidents.

Resource Managers should ensure that all staff are aware of these legal requirements and procedures relating to information management. All new staff are provided with an introductory briefing on information management and security procedures. Corporate training on information rights compliance is provided quarterly for all staff to attend, incorporating records management, information security and breach reporting.

Failure to comply with the policy may result in an administrative fine for the organisation by the Information Commissioner's Office (ICO) and/or disciplinary action against individuals under Ofwat's procedures.

6 Available guidance

All relevant policies relating to information management and security are available for staff on the Ofwat intranet. This guidance is reviewed regularly and updated to incorporate any legislative changes and recommendations from learning.

7 Incident Management

1. Reporting an Incident

Any person becoming aware of an actual or suspected breach or weakness must report this immediately. Staff are encouraged to use the information incident reporting log on the intranet. This is also accessible via the apps page on the Source by selecting the exclamation mark. It is essential that incidents are reported as soon as an issue is suspected. If the incident involves lost IT equipment including mobile phones and it is not possible to access the incident reporting form then call 0777 816 08081 and leave details.

If the breach occurs or is discovered outside normal working hours, it must be reported as soon as possible. The report will include full and accurate details of

the incident, when the breach occurred (dates and times), who is reporting it, if the data relates to people, the nature of the information, and how many individuals are involved. Ofwat's incident reporting form identifies the pool/programme involved, type of incident e.g. loss of equipment and level of compromise. This information must be included in reports made or submitted that do not use the standard form.

Theft or losses involving Ofwat equipment should also be reported to the local police area and a crime number obtained. Once received the crime number should be given to Ofwat security.

2. Containment and Recovery

All efforts must be made in order to minimise a further breach. In the event of loss of equipment all efforts should be made with any organisations involved to recover the equipment. This may include Ofwat security liaising with the Police, the public transport network and event organisers. It is also essential that breaches involving the loss of equipment are reported to Ofwat security without delay so that disablement or remote wiping can be undertaken immediately. In the event of an email breach, staff should speak to their resource manager or work manager.

3. Investigation and Risk Assessment

An initial assessment of the extent of potential harm (see Appendix A) will be made by the DPO and/or other relevant personnel such as the Deputy Security Advisor (DSA) or Information Governance Manager (IGM), within the first 24 hours wherever possible. If the incident is ongoing consideration should be given to how to contain and minimise further damage.

Consideration will include:

- Types of data involved (including personal & personal sensitive[7] or commercially sensitive data)
- Volume of data involved
- Quantity of data subjects (persons affected) involved, if relevant
- Assessment of ongoing risk e.g. number of recipients involved (if known)

[7] Sensitive personal data is defined as a special category of data including health, religion ethnicity, trade union membership etc.

- Any mitigating features, for example files are encrypted or password protected

Any breach identified as a moderate or severe risk by this assessment will be reported to Ofwat's Senior Information Risk Owner (SIRO). If a breach includes Ofwat systems or hardware the Director of IT and Digital will also be notified by the DSA or the IGM. The SIRO will inform the Chief Executive if the breach is categorised as a moderate or severe risk. Consideration should be given to escalation to the CEO by the DPO and DSA or IGM of any minimal risk incidents in any event, particularly if they form a pattern of incidents of a similar nature.

It may be necessary for the DPO and/or DSA or IGM to collate additional information or consult with additional persons, in order to fully understand the level of risk to Ofwat or to any individuals or companies concerned. Any request for information should be treated with urgency and confidentiality in order to mitigate any further risk and as a matter of respect to any individuals concerned. It may also be necessary to assign additional resources to assist with an investigation and for steps to be taken during this period to minimise the impact of the data breach (e.g. communicating with recipients of a misdirected email and requesting them to delete the message unread).

4. Evaluation and Response

Once all the facts have been established, the DPO and/or DSA or IGM will make a decision on how to ensure both that any damage caused by the breach has been mitigated as far as possible, that any relevant legal obligations have been complied with, and that appropriate steps have been taken to prevent recurrence of the breach. In respect of mitigation of the impact of the breach and any ongoing risks, and compliance with legal obligations, the following steps must be decided:

- In the case of a breach involving personal data, do we need to report to the ICO? This assessment will need to be immediate as personal data breaches that require reporting to the ICO need to be undertaken within 72 hours[8].
- In accordance with Cabinet Office standards, a significant breach must be reported to the Cabinet Office.

[8] A temporary loss of personal data may not need to be reported to the ICO, depending on all the circumstances.

- In the case of a breach involving personal data, do we need to contact all/any of the individuals whose personal data was affected? And in the case of information concerning a business, do we need to contact that business? If yes, how best should we manage these communications[9]?
- Do we need to contact any external recipients, including stakeholders? If yes, how best should we manage these communications?
- Is any subsequent action against any individual or business required, for example if it is the result of a deliberate or malicious action, or breach of contract?
- Is the breach as a result of our Cloud Provider? Is yes then Ofwat would need to take into account any legal requirements placed on us by the Network & Information Systems (NIS) regulations.

The DPO will liaise with the Communications Team as appropriate as to whether a press release is required and to be ready to handle any incoming press enquiries. All actions will be recorded by the DPO.

In order to ensure that appropriate measures are in place to prevent a recurrence of the data breach, and to ensure that the data breach process itself is working effectively, the relevant Programme or Pool will then carry out a Lessons Learned exercise and implement any changes that this identifies as required to prevent future data breaches and ensure effective operation of the data breach process[10]. The Lessons Learned exercise should be reasonable and proportionate in terms of scope and use of resource, by reference to the severity of the data breach and/or any underlying issue indicated by it.

Factors to consider include:

- Was the breach caused, even in part, by any systemic or ongoing problem?
- Was the breach caused by an external factor? If yes how had we prepared for this, e.g.an Impact Assessment or Information Security Assessment
- Human element - are there any areas where colleagues need additional training or tailored advice?

[9] Article 34 GDPR requires that when the personal data breach is likely to result in a severe risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay.

[10] Article 32 GDPR makes clear that the ability to restore availability and access to personal data in a timely manner in the event of a physical or technical incident is part of the obligation to implement appropriate technical and organisational measures

- Are there any weaknesses in security, for example the portable storage of devices or access to Ofwat's network?
- Sharing or disclosing information - are transmission methods appropriate or even necessary, for example email protocols or anonymisation?
- Did we react quickly enough to the incident?
- Were we clear on what next steps to take, including damage mitigation at as early a stage as possible?
- Were the right people informed/involved at every stage.

If deemed necessary a report recommending any changes to systems, policies and procedures will be considered by SLT, ARAC and/or the Board.

8 Links to Any Associated Documents

ICT 2 Security Policy
ICT 5 Information and Technology Security Policy
ICT 6 Acceptable Use Agreement
Ofwat Code of Conduct
G2 Data Protection Policy
G5 Privacy Policy

9 Document control

Version history

Version	Status	Date	Author	Summary of changes
0.1	draft	07/2017	SA FOI	
0.2	draft	12/2018	IGM	Minor updates
0.3	draft	09/2019	IGM	Minor updates

Sign off

Name	Date	Version No.	Date of Next review
DPO	Sept 2019	0.3	September 2021

Appendix A: Assessment of Severity of Breach

To be completed by the DPO and/or other member of Ofwat staff as appropriate (see Incident Management, section 3) in consultation with the relevant personnel affected by the breach and IT staff where applicable.

Details of Breach	
Date and time incident was identified and by whom. Include crime number if applicable.	
Name and contact details (email, telephone number) of person making the report	
Details of the IT systems, equipment, devices, records involved in the incident. Include the type and amount of information lost or compromised, how this occurred, and any mitigating features e.g. files encrypted / password protected	
Assessment of Severity	
Is a data breach confirmed or suspected?	
Is the incident ongoing or contained? If on-going, provide details of what has been done to contain the breach. If contained, provide details of how this has been achieved.	
Activity undertaken to recover the data and mitigate the impact of the incident, e.g. report theft to police, contact incorrect recipient of email	
Have the data subject(s) / companies impacted been informed? If yes, confirm who has been contacted, the date and time of contact, how (e.g. telephone, email, etc.), what has been said.	
Is the information unique? Will its loss or compromise or have adverse operational, financial, legal or reputational impacts or consequences for Ofwat or any third party?	

If personal data is involved, how many data subjects are affected and in what way are they likely to be affected? For example, did the data breach include a personal address, bank account details, medical information, etc.	
What contractual security arrangements apply? Speak to procurement and/or legal if further assistance is required.	
What is the nature of the sensitivity of any personal data or commercial data lost or compromised? Please provide details of any types of information as classified below: • Sensitive/special categories of personal data (as defined by data protection legislation) relating to a living, identifiable individual's: a) racial or ethnic origin; b) political opinions or religious or philosophical beliefs; c) membership of a trade union; d) physical or mental health or condition or sexual life; genetic or biometric data; e) commission or alleged commission of any offence, or f) proceedings for an offence committed or alleged to have been committed by the data subject, the disposal of such proceedings or the sentence of any court in such proceedings.	
• Information that could be used to commit identity fraud such as: personal bank account and other financial information; national identifiers, such as National Insurance Number and copies of passports and visas;	
• Detailed profiles of individuals including information about work performance, salaries or personal life that would cause significant damage or distress	
• Non-personal data (include market sensitive, commercially sensitive; data supplied by a 3rd party)	

Assessment (see matrix below), e.g. severe, moderate, minimal	
Other relevant factors	
Reported to ICO?	Yes/No
Reason for not reporting?	
Outcome	

Assessment Matrix

The severity of each breach will depend upon all the circumstances. Factors which are likely to be relevant to the severity of a data breach are set out below, although these are not exhaustive, and judgement must be applied on a case by case basis.

Severe:

- The data easily identifies an individual, and/or is special category personal data, e.g. data concerning health
- The data would affect a company's commercial interests
- The information could be improperly used if disclosed
- Significant or irreversible consequences to individuals / companies affected
- Likely media coverage
- Immediate response required regardless of whether the incident is contained or not
- Requires significant response beyond normal operating procedures

Moderate:

- The data has the potential to enable identification of an individual
- The data has the potential to affect a company's commercial interests
- The probability of improper use or disclosure of the data is uncertain
- Significant inconvenience will be experienced by individuals / companies affected
- Incident may not yet be contained
- Incident does not require immediate response

Minimal:

- The data is unlikely to indentify an individual
- The data is unlikely to affect a company's commercial interests

- The data has a minimal probability of being improperly used or disclosed
- Risk to Ofwat is low
- Limited inconvenience may be suffered by individuals / company affected
- Loss of data is contained / encrypted / password protected
- Incident can be responded to during working hours

A data breach may contain one or more of the identifiers listed above. For example, a breach containing market sensitive data that has been found to affect a company's commercial interests would be categorised as Severe. However, an email sent to an external recipient containing customer contact details may be classed as inconvenient to an individual, has the possibility of being able to identify an individual as a result, but is classified as a low risk.