CANARY WHARF
GROUP PLC

# DATA BREACH POLICY

**Contents**

**Paragraph** **Page**

## 1. Principles

1.1. During the course of our activities, Canary Wharf Group plc and all associated group companies ("**Canary Wharf Group**") are required under data protection laws to safeguard the security and confidentiality of the information/data that we process on behalf of our clients, customers and employees.

1.2. Information and personal data is one of our essential assets and every director and employee has a responsibility to ensure the security of this information and personal data.

1.3. Data security breaches can occur for a number of reasons including:

1.3.1. the disclosure of confidential data to unauthorised individuals;

1.3.2. improper disposal of documents leaving personal data deposited in a bin that can be accessed by the general public;

1.3.3. loss or theft of data or equipment on which data is kept;

1.3.4. loss or theft of paper records;

1.3.5. inappropriate access controls allowing unauthorised use of information;

1.3.6. suspected breach of our IT security and related policies;

1.3.7. attempts to gain unauthorised access to computer systems, e.g. hacking;

1.3.8. viruses or other security attacks on our IT equipment systems or networks;

1.3.9. breaches of physical security;

1.3.10. confidential information left unlocked in accessible areas;

1.3.11. emails containing personal or sensitive information sent in error to the wrong recipient;

1.3.12. equipment failure; and

1.3.13. 'blagging' offences whereby information is obtained by deceiving the data processor or data controller.

1.4. The purpose of this policy is to ensure that a standardised approach is implemented throughout our organisation in the event of a data breach.

1.5. We have a legal obligation under data protection laws to ensure appropriate measures are in place to protect against accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. To help develop a wider review and consider what needs to be included in a data breach response plan, **Appendix 1** sets out some key questions to consider.

1.6. The General Data Protection Regulation specifies that all breaches (except those 'unlikely to result in a risk to the rights and freedoms of natural persons) should be reported to the Information Commissioner 'without undue delay…not later than 72 hours after having become aware of it'.

1.7. In the event of a data breach or an information security incident, it is therefore vital that appropriate actions are taken to promptly report the breach internally so that the incident can be appropriately managed and we can minimise any associated risks.

1.8. This policy deals with our legal obligations in the event of a data breach. However we should also consider our obligations to staff, clients, customers and data subjects beyond our strict legal obligations. To help develop a wider review and consider what needs to be included in a data breach response plan, Appendix 1 sets out some key questions for our organisation to consider.

1.9. **Appendix 2** sets out a checklist of steps to take in the first 24 hours after a data breach is discovered.

## 2. Scope and Responsibilities

2.1. This procedure is designed to set out the process that should be followed to ensure a consistent and effective approach is in place for managing a data breach across the organisation and ensure that:

2.1.1. Data breach events are detected, reported and monitored consistently

2.1.2. Incidents are assessed and responded to appropriately

2.1.3. Action is taken to reduce the impact of a breach

2.1.4. Relevant breaches are reported to the Information Commissioner within the 72 hour window

2.1.5. Improvements are made to prevent recurrence

2.1.6. Lessons learnt are communicated to the wider organisation

2.2. Responsibilities

2.2.1. Directors

2.2.1.1. The Directors of the organisation have responsibility to our shareholders, clients, customers and staff to ensure that any privacy risks are managed.

2.2.2. All Staff

2.2.2.1. All users of information assets across the organisation should familiarise themselves with this procedure, be aware of privacy risks and be vigilant in order to ensure breaches are identified, reported and managed in a timely manner.

2.3. We want an open and honest culture where people feel comfortable to report mistakes. Support will be provided to ensure everyone has access to the appropriate skills and training to carry out their role effectively. However gross negligence and intentional violations (including not reporting incidents/mistakes) are taken seriously and will lead to disciplinary action.

## 3. Definitions

3.1. **Personal Data** means any information relating to an identified or identifiable person ('data subject').

3.2. **Data Subject**: An identifiable 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 person.

3.3. **Personal data breach** means 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.

3.4. **Special Category Data** is data which requires extra care and precautions to be taken in its processing and which details or consists of;

3.4.1. the racial or ethnic origin of the subject

3.4.2. their political opinions

3.4.3. their religious or philosophical beliefs

3.4.4. whether they are a member of a trade union

3.4.5. processing of genetic data

3.4.6. processing of biometric data

3.4.7. data concerning health

3.4.8. their sexual life/sexual orientation

## 4. Steps to take in the event of a data breach

4.1. Step 1: Investigate the Incident

4.1.1. Is the Incident a Personal Data Breach?

4.1.1.1. A personal data breach may involve loss of personal data or the unlawful accessing or processing of personal data. Only if an incident actually resulted in a breach of personal data the mandatory notification obligation applies. For instance, lost USB sticks, stolen laptops, malware infections or hacked databases containing personal data are considered personal data breaches.

4.1.1.2. A threat or a shortcoming in security measures, such as weak passwords or outdated firewalls, are not considered a personal data breach as long as no personal data has been leaked. Therefore, these issues in security measures do not fall within the mandatory notification obligation.

4.1.2. Details of breaches should be recorded accurately, including:

4.1.2.1. the date and time the breach occurred;

4.1.2.2. the date and time it was discovered;

4.1.2.3. who/what reported the breach;

4.1.2.4. description of the breach;

4.1.2.5. details of any ICT systems involved;

4.1.2.6. and any other substantiating material.

4.1.3. Containment and Recovery

4.1.3.1. Containment comprises restricting both the scope and impact of the breach.

4.1.3.2. If a breach occurs, we should:

4.1.3.2.1. Decide on who will take the lead in investigating the breach (usually this will be the Data Protection officer) and ensure that the appropriate resources are available to the DPO for investigation.

4.1.3.2.2. The DPO will establish who needs to be alerted to the breach and inform them of what they are expected to do to support in containing same.

4.1.3.2.3. The DPO will then establish whether there is anything that can be done to recoup losses and/ limit the damage the breach may cause.

4.2. Step 2: Investigate the Scope, Nature and Possible Consequences

4.2.1. For this investigation the answers to the following questions can be relevant:

4.2.1.1. What is the source of the personal data breach? For instance, is it a stolen device or is it an internal security measure which has been hacked?

4.2.1.2. How many individuals are affected by the personal data breach and is the data breach likely to result in a risk to the rights and freedoms of the individuals affected? For instance, a hack of a customer database could most likely have a severe impact on private lives of many people. On the other hand, a breach concerning only business contact details of one customer may have minimal impact only.

4.2.1.3. Does the personal data compromised include special categories of data or data relevant to identity theft? For instance, credit card details, passport numbers or health data.

4.2.1.4. Was the compromised personal data encrypted or secured in a manner which makes it impossible for a third party to assess? For instance, if adequate encryption is used or the data is adequately hashed and salted it can be assumed that third parties will not be able to access the personal data.

4.2.1.5. Which steps are taken to mitigate (further) loss of personal data? For instance, if it is possible to wipe all personal data remotely so that loss of personal data can be prevented or if access to hacked database could be regained, it is possible to mitigate further loss.

4.2.1.6. Which parties are involved in the data breach? For instance, if a shared database is hacked, it cannot be excluded that several parties will be involved and/or affected by the data breach.

4.3. Step 3: Investigate Notification Obligation to Information Commissioner

4.3.1. The Information Commissioner should be notified by the controller of any personal data breach that results in or is likely to result in "a risk to the rights and freedoms of natural persons." This has to be assessed on a case by case basis. For example, we will need to notify the Information Commissioner about a loss of customer details where the breach leaves individuals open to identity theft. On the other hand, the loss or inappropriate alteration of an internal telephone list, for example, would not normally meet this threshold.

4.3.2. In this respect it is relevant to know the answers to the above questions and have an idea of the reasonable consequences the breach may have (for example, result in discrimination, damage to reputation, financial loss, loss of confidentiality or any other significant economic or social disadvantage). If not yet all information is available, the controller should still notify the Information Commissioner. If needed, the notification may be amended at a later stage when the full details are known or the notification could be withdrawn if not needed after all.

4.3.3. If notification to the Information Commissioner is required

4.3.3.1. Where a notification with the Information Commissioner is required, it is recommended first checking if the Information Commissioner uses a standard breach notification form. If such form is not available, the notification includes at least the following information:

4.3.3.1.1. the scope and nature of the personal data breach, including the categories and number of data subjects and data records concerned;

4.3.3.1.2. the name and contact details of the Data Protection Officer or other contact point where more information can be obtained;

4.3.3.1.3. a description of the likely consequences of the personal data breach;

4.3.3.1.4. a description of the measures taken or proposed to be taken to address the breach, including measures to mitigate any possible adverse effects.

4.3.4. In the event of a personal data breach which is likely to result in risk to the rights and freedoms of natural persons, we shall notify the breach to the Information Commissioner's Office without undue delay, or in any case within 72 hours of becoming aware of the breach. Where notification is not made to the ICO within 72 hours, it shall be accompanied by reasons for the delay.

4.4. Step 4: Investigate Notification Obligation Individuals

4.4.1. Where a personal data breach is likely to result in a "high risk" to the rights and freedoms of individuals, we must notify those concerned directly. A "high risk" means the threshold for notifying individuals is higher than for notifying the Information Commissioner.

4.4.2. If affected individuals must be informed, we should provide at least the following information in clear and plain language:

4.4.2.1. the scope and nature of the personal data breach;

4.4.2.2. the name and contact details of the Data Protection Officer or other contact point where more information can be obtained;

4.4.2.3. a description of the likely consequences of the personal data breach;

4.4.2.4. a description of the measures taken or proposed to taken to address the breach including measures to mitigate any possible adverse effects (e.g. contact your credit card provider, change your password, etc.).

4.4.3. Notification to individuals shall not be necessary if the controller can demonstrate that "appropriate technological protection measures" were applied to the data concerned by the personal data breach, which "shall render the data unintelligible to any person who is not authorised to access it.', such as encryption, or if it has subsequently taken measures which ensure that the high risk for the rights and freedoms of data subjects is longer likely to materialise.

4.4.4. If individual notifications would be a disproportionate effort, the controller can use some form of public communication instead provided that this will be equally effective in informing individuals.

4.4.5. The Information Commissioner has the power to overrule controllers and order them to notify the affected individuals if they disagree with a controller's assessment of the risk.

4.5. Step 5: Create and Maintain an Internal Breach Register

4.5.1. Controllers are obliged to document any personal data breaches, which shall at least include information on the facts relating to the personal data breach, the effects of the breach and the efforts and remedial actions taken. We must document any communication with Information Commissioner and affected individuals. Moreover, in the event a decision was made not to notify the Information Commissioner and/or affected individuals, we must keep a record of the facts and the reasons why such decision was made as the Information Commissioner may initiate an audit or request for information at any time.

4.5.2. Processors should keep an internal breach register, amongst other to demonstrate to (potential) customers the effectiveness of the implemented security measures or the maturity when it comes to handling data breaches.

4.6. Step 6: Evaluate the Personal Data Breach and Update Technology and Policies

4.6.1. The new principle of accountability requires controllers to be responsible for and to be able to "demonstrate" and "evidence" compliance with the data protection principles, which include security obligations. In view of the accountability requirement, we must document what we have done to prevent future personal data breaches originating from the same source as well as regularly reviewing and updating our breach detection, investigation and internal reporting procedures.

4.6.2. Subsequent to a data breach a thorough review of the event should be undertaken by the DPO who will consider:

4.6.2.1. What action needs to be taken to reduce the risk of future breaches and minimise their impact?

4.6.2.2. Whether policies, procedures or reporting lines need to be amended to increase the effectiveness of the response to the breach?

4.6.2.3. Are there weak points in security controls that need to be strengthened?

4.6.2.4. Are all directors and employees aware of their responsibilities for information security and adequately trained?

4.6.2.5. Is additional investment required to lessen exposure and if so what are the resource implications?

4.6.3. Any changes to policies and/or procedures must be documented and implemented as soon as possible thereafter by the board of directors.

**5. Review & Update**

5.1. This policy will be reviewed and updated annually or more frequently if necessary, to ensure that any changes to our business practices/business plan are accurately reflected.

**Appendix 1 - Developing a breach response plan**

**1. Initial questions**

1.1. Do we know who should be notified within the organisation if there is a data breach?
1.2. What happens if one of the team is away on holiday or absent? Is there a back-up plan?
1.3. Do we have clear reporting lines and decision-making responsibility?
1.4. Do we understand what external assistance we might need, with providers in place in advance?
1.5. Do we have designated person(s) responsible for managing breaches?
1.6. Do we have processes for triaging incidents and activating the breach response team?

**2. Legal issues**

2.1. Do we have a process for maintaining legal privilege and confidentiality?
2.2. Can we pause document destruction processes?
2.3. Do we have appropriate evidence gathering capability so we can collect information about the breach?
2.4. Do we know who our specialist external lawyers are?
2.5. Do we have a process for managing and logging steps taken in the investigation?
2.6. Do we understand our contractual rights and obligations with third parties?
2.7. Can we quickly identify third parties we may need to notify?
2.8. Do we have appropriate contractual rights to be notified of breaches by third parties?
2.9. Do we know how to contact the Information Commissioners Office ("ICO") and law enforcement who we can involve quickly if necessary?
2.10. If we hold credit/ debit card data, do we need to notify our payment processor?
2.11. Do we need advice on the legal options available to quickly gather evidence from third parties?
2.12. Do we understand our potential liabilities to third parties?
2.13. Can we gather information about the breach including taking statements from staff who might have seen unusual activity?
2.14. Do we understand when we should consider notifying data subjects and / or regulators?

**3. Forensic IT**

3.1. Do we have appropriately qualified forensic IT capability, either internally or externally?
3.2. Do we understand the basic IT do's and don'ts of immediate response to data breaches?
3.3. Do we have an appropriate asset inventory to help we identify potentially compromised devices, where those devices are and in whose possession?
3.4. Do we understand how data flows in our organisation, in practice?
3.5. Can we quickly secure and isolate potentially compromised devices without destroying evidence?
3.6. Can we quickly ensure physical security of premises?

**4. Cyber breach insurance**

4.1. Do we have cyber breach insurance, or other insurance which may cover a data breach?
4.2. Do we understand the process for notifying breaches to insurers?
4.3. Do we have emergency contact details for our brokers?

**5. Data**

5.1. Do we know what data we hold (and what we shouldn't hold)?
5.2. Is our data appropriately classified?
5.3. Do we have, and apply, appropriate data destruction policies?
5.4. Do we know what data is encrypted, how it is encrypted, and when it may be unencrypted on our systems?
5.5. Do we have appropriate checks to ensure we are storing only the data we should be?
5.6. Do we have appropriate additional protection for sensitive data?
5.7. Do we have data loss prevention or similar tools?
5.8. Do we understand our logs, how long we retain them for, and what they can (or cannot) tell you?
5.9. Do we have appropriate logging of staff access to data?

**6. Data subjects**

6.1. Do we understand when we should consider notifying data subjects?
6.2. Do we understand the contractual and legal rights of data subjects?
6.3. Can we quickly prepare appropriately worded notifications to data subjects?
6.4. Do we understand the potential harm to data subjects of loss of the different types of data that we hold?
6.5. Do we have the ability to appropriately triage and deal with a breach?
6.6. Are staff appropriately trained as to how to deal with data subjects in a breach scenario?

**7. Public Relations ("PR")**

7.1. Do we have PR capability experienced in dealing with data breaches?
7.2. Do we have template pro-active and re-active press statements?
7.3. Can we actively monitor social media after a breach?

**Appendix 2 - What to do in the first 24 hours after a data breach**

**1.** Mobilise crisis management team with support from communications and legal advisers, as appropriate

**2.** Record the date and time when the breach was discovered, as well as the current date and time when response efforts begin, i.e. when someone on the response team is alerted to the breach

**3.** Alert and activate everyone on the response team, including external resources, to begin executing your incident response plan

**4.** Protect your reputation with an internal and external communications strategy, supported as necessary by crisis communications specialists and/or reputation lawyers

**5.** Secure the IT systems affected by the cyber attack to help preserve evidence

**6.** Stop additional data loss. Take affected equipment offline but do not turn them off or start probing into the computer until your forensics team arrives

**7.** Document everything known thus far about the breach

**8.** Interview those involved in discovering the breach and anyone else who may know about it.

**9.** Review protocols regarding disseminating information about the breach for everyone involved in this early stage.

**10.** Bring in your forensics team to begin an in-depth investigation

**11.** Report to police, if/when considered appropriate

**12.** Notify regulators, if needed, after consulting with legal counsel and upper management and insurance broker(s) to ensure compliance with policy terms