Data Breach Policy & Reporting

Background

As an organisation, we store, process, and share a reasonable amount of personal information. Data is a valuable asset that needs to be suitably protected. Every care is taken to protect personal data from incidents (either accidentally or deliberately) to avoid a data protection breach that could compromise security. Compromise of information, confidentiality, integrity, or availability may result in harm to individual(s), reputational damage or detrimental effect on the organisation.

Aim

We are obliged under the GDPR to have a process in place designed to ensure the security of all personal data during its lifecycle, including clear lines of responsibility. This policy sets out the procedure to be followed to ensure a consistent and effective approach is in place for managing data breach and information security incidents.

Scope

This policy relates to all personal and sensitive data held by the organisation regardless of format.

This policy applies to everyone at this organisation. This includes temporary, casual or agency staff and contractors, consultants, suppliers and data processors working for, or on behalf of the organisation. The objective of this policy is to contain any breaches, to minimise the risk associated with the breach and consider what action is necessary to secure personal data and prevent further breaches.

Definition/Types of breach

For the purpose of this policy, data security breaches include both confirmed and suspected incidents. An incident in the context of this policy is an event or action that may compromise the confidentiality, integrity or availability of systems or data, either accidentally or deliberately.

An incident includes but is not restricted to, the following:

- Loss or theft of confidential or sensitive data or equipment on which such data is stored (e.g. loss of laptops, USB sticks, iPad/tablet devices, or paper records)
- Equipment theft or failure
- Unauthorised use of, access to or modification of data or information systems
- Attempts (failed or successful) to gain unauthorised access to information or IT system
- Unauthorised disclosure of sensitive/confidential data
- Website defacement
- Cyber attacks
- Unforeseen circumstances such as a fire or flood
- Human error
- Disclosure through Social Engineering where information is obtained by deceiving the organisation who holds it

Personal data breaches can include:

- Access by an unauthorised third party
- Deliberate or accidental action (or inaction) by a controller or processor
- Sending personal data to an incorrect recipient
- Computing devices containing personal data being lost or stolen
- Alteration of personal data without permission
- Loss of availability of personal data

First Step - Containment and Recovery

Appropriate steps must be taken immediately to minimise the effect of the breach. An initial assessment should be made to establish the severity of the breach and to establish whether there is anything that can be done to recover any losses and limit the damage the breach could cause.

The investigation will need to take into account the following:

- The type of data involved
- The sensitivity of involved data
- The protections that are in place (e.g. encryption)
- What's happened to the data, has it been lost or stolen?
- Whether the data could be put to any illegal or inappropriate use
- Who the individuals are, number of individuals involved and the potential effects on those data subject(s)
- Whether there are wider consequences to the breach

Reporting an incident

Any individual who accesses, uses or manages information is responsible for reporting data breach and information security incidents immediately to the appropriate personnel using the form attached.

If the breach occurs or is discovered outside normal working hours, it must be reported as soon as is practicable. 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. An Incident Report Form should be completed as part of the reporting process. All staff should be aware that any breach might result in disciplinary procedures being instigated.

How much time do we have to report a breach?

You must report a notifiable breach to the ICO without undue delay, but not later than 72 hours after becoming aware of it. If you take longer than this, you must give reasons for the delay. Section II of the WP29 Guidelines on personal data breach notification gives more details of when a controller can be considered to have "become aware" of a breach.

The most important consideration is whether a breach is a 'notifiable breach' – this depends on the nature of the breach, scale of loss, and impact on the data subjects involved. Not all breaches are notifiable. It is the responsibility of the Data Lead to decide whether a breach is notifiable and to report the breach to the ICO is necessary.

What breaches do we need to notify the ICO about?

When a personal data breach has occurred, you need to establish the likelihood and severity of the resulting risk to people's rights and freedoms. If it's likely that there will be a risk then you must notify the ICO; if it's unlikely then you don't have to report it. However, if you decide you don't need to report the breach, you need to be able to justify this decision, so you should document it.

In assessing risk to rights and freedoms, it's important to focus on the potential negative consequences for individuals including physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the person concerned.

This means that a breach can have a range of adverse effects on individuals, which include emotional distress, and physical and material damage. Some personal data breaches will not lead to risks beyond possible inconvenience to those who need the data to do their job. Other breaches can significantly affect individuals whose personal data has been compromised. You need to assess this case by case, looking at all relevant factors.

What information must a breach notification to the supervisory authority contain?

When reporting a breach, the GDPR says you must provide a description of the nature of the personal data breach including, where possible:

The categories and approximate number of individuals concerned|The categories and approximate number of personal data records concerned|The name and contact details of the data protection officer (if your organisation has one) or other contact point where more information can be obtained|A description of the likely consequences of the personal data breach|A description of the measures taken, or proposed to be taken, to deal with the personal data breach, including, where appropriate, the measures taken to mitigate any possible adverse effects.

What if we don't have all the required information available yet?

The GDPR recognises that it will not always be possible to investigate a breach fully within 72 hours to understand exactly what has happened and what needs to be done to mitigate it. So Article 33(4) allows you to provide the required information in phases, as long as this is done without undue further delay.

When do we need to tell individuals about a breach?

If a breach is likely to result in a high risk to the rights and freedoms of individuals, the GDPR says you must inform those concerned directly and without undue delay. In other words, this should take place as soon as possible.

A 'high risk' means the threshold for informing individuals is higher than for notifying the ICO. Again, you will need to assess both the severity of the potential or actual impact on individuals as a result of a breach and the likelihood of this occurring. If the impact of the breach is more severe, the risk is higher; if the likelihood of the consequences is greater, then again the risk is higher. In such cases, you will need to promptly inform those affected, particularly if there is a need to mitigate an immediate risk of damage to them. One of the main reasons for informing individuals is to help them take steps to protect themselves from the effects of a breach.

What information must we provide to individuals when telling them about a breach?

You need to describe, in clear and plain language, the nature of the personal data breach and, at least:

- The name and contact details of your data protection officer (or nominated Data Lead) or other contact point where more information can be obtained
- A description of the likely consequences of the personal data breach
- A description of the measures taken, or proposed to be taken, to deal with the personal data breach
- Where appropriate, the measures taken to mitigate any possible adverse effects.

Does the GDPR require us to take any other steps in response to a breach?

You should ensure that you record all breaches, regardless of whether or not they need to be reported to the ICO.

Article 33(5) requires you to document the facts relating to the breach, its effects and the remedial action taken. This is part of your overall obligation to comply with the accountability principle, and allows the ICO to verify your organisation's compliance with its notification duties under the GDPR.

As with any security incident, you should investigate whether or not the breach was a result of human error or a systemic issue and see how a recurrence can be prevented – whether this is through better processes, further training or other corrective steps.

Notification

Management shall determine who needs to be notified of the breach. Every incident will be assessed on a case-by-case basis. However, the following will need to be considered:

- Whether there are any legal/contractual notification requirements
- Whether notification would assist the individual affected – could they act on the information to mitigate risks?
- Whether notification would help prevent the unauthorised or unlawful use of personal data
- Would notification help the company meet its obligations under the seventh data protection principle?
- Is there a large number of people affected, or are there very serious consequences?
- Whether the Information Commissioner's Office (ICO) should be notified. The ICO will only be notified if personal data is involved. Guidance on when and how to notify ICO is available from their website at: https://ico.org.uk/media/1536/breach_reporting.pdf

All suspected and actual breaches should be recorded on the appropriate log to facilitate further evaluation and breach avoidance activity.

What happens if we fail to notify?

Failing to notify a breach when required to do so can result in a significant fine up to 10 million euros or 2% of your global turnover. The fine can be combined the ICO's other corrective powers under Article 58. So it's important to make sure you have a robust breach-reporting process in place to ensure you detect and can notify a breach, on time; and to provide the necessary details.

The dangers of over notifying

Not every incident warrants notification and over notification may cause disproportionate enquiries and work. Notification to the individuals whose personal data has been affected by the incident will include a description of how and when the breach occurred and the data involved. Specific and clear advice will be given on what they can do to protect themselves, and include what action has already been taken to mitigate the risks. Individuals will also be provided with information on what has occurred.

Evaluation and response

Once the initial incident is contained, the organisation will carry out a full review of the causes of the breach, the effectiveness of the response(s) and whether any changes to systems, policies and procedures should be undertaken. Existing controls should be reviewed to determine their adequacy and whether any corrective action should be taken to minimise the risk of similar incidents occurring.

What should I do first?

Where possible action should be taken to halt a breach and stop any further loss of data or other damage. Before reporting any incident, you must refer to your Data Protection Lead:

Sjoerd Klinkhamer

QubiqDigital

WG Plein 112 1054SC Amsterdam

Data Breach Reporting Form

The following form should be used to report/record a data breach:

Notification of Data Security Breach	To be completed by person reporting incident
Date incident was discovered	
Date(s) of incident	
Place of incident	
Name of person reporting incident	
Contact details of person reporting incident (email address, telephone number)	
Brief description of incident or details of the information lost	
Number of Data Subjects affected, if known	
Has any personal data been placed at risk? If, so please provide details	

Brief description of any action taken at the time of discovery	

For use by the Data Controller/Data Protection Officer/Management	
Received by	
On (date)	
Forwarded for action to	
On (date)	

Data Breach Form Letter

Dear *Name of customer*

Sadly, it has come to our attention that a breach in our processing system has exposed items of your personal data to *unauthorised external parties/unlawful processing*. As an immediate course of action, we have notified the ICO (Information Commissioner's Office) and the relevant law enforcement agency. If needed, we will work with cyber security experts, forensic examiners and legal counsel to ensure everything is being done to minimise further exposure.

What happened?

At time of writing, we believe the following timeline of events to have taken place leading to the reported breach.

- *List the timeline of events contributing to the breach event. There is no requirement to expose sensitive information about the organisation unless it is crucial in describing the breach.*

The following items of personal data were involved

- *List the types of personal data. For example, first name, surname and DOB*

What this means for you

Considering the nature of the breach and the types of personal data involved in the breach, we believe the consequences to you are as follows

- *Try to list any personal actions the data subject will need to take. e.g will they need to change their password or seek legal advice. The ICO would like to see the data controller taking the lead when it comes to repairing or containing damage.*

How we will stop this from happening again

In order to prevent such a breach taking place again and to minimise the impact on our customers, we have started to take the following steps.

- *List the actions your organisation is taking to ensure that this breach is not repeated. Again, this does not need to compromise the organisation's confidentiality but should be as reassuring to data subject as possible*

Please note, we will not send further email updates about this incident. All future updates in regards to this security breach can be found on our website at: qubiqdigital.com. Any emails you receive about this security incident should be treated as suspicious.

We apologise wholeheartedly for this breach of security, but please be assured that we are doing everything in our power to ensure that the damage is mitigated and that this doesn't happen again in the future. For further information please contact [data controller name] at [controller email].

Breach Log Template

Complete the following table to track data breach events.

Breach Number	Date Received	Data Subject Impact	Breach Contained	Breach Reported To ICO	Data Subjects Informed