# Data Breach Policy

## Data breach policy, letter and reporting template guidance

### How should I use my data breach policy and reporting log?

Our data breach policy and reporting log document outline the policy we should adopt and processes we should enact in the event of a data breach. The accompanying reporting log will provide us with a space to record and report those breaches. We should complete this log where necessary, and store these with our GDPR documents for safekeeping.

### Will I need to update our data breach policy and reporting log?

Yes. It is a crucial aspect of our GDPR compliance to ensure that we have a clearly defined policy in place dictating what we will do in the event of a data breach. We should review this policy at least every 12 months and amend as necessary to ensure we remain GDPR compliant.

## Data breach policy and reporting log

We take privacy seriously. That is why we take every possible precaution to protect personal data, and actively work to avoid any data protection breaches which could compromise our data security, or the personal rights of our clients, customers, stakeholders or anyone else associated with our company.

To mitigate the risk that any such data compromise could pose, we have developed the

following data breach policy. It is an integral part of our compliance responsibilities under the UK General Data Protection Regulation and Data Protection Act 2018, and is designed to develop clear lines of responsibility and processes that must be followed to adequately mitigate and manage data breach and security incidents.

### What does this policy cover?

The scope of this data breach policy encompasses all personal and sensitive data our company holds. This data breach policy applies to everyone at our company – including employees, temporary or casual staff, consultants, suppliers, contractors, freelance workers or other data processors who are storing or processing data on the behalf of our company.

### What is the purpose of this policy?

The purpose of this data breach policy is to contain all data breaches and to minimise the risks associated with any breaches. It also outlines the actions that should be taken in the event of a breach to ensure data is secure and to prevent further breaches.

### About data breaches

A data breach is defined as any incident, event or action that has the potential to compromise the availability of data, the integrity of data, confidentiality or our company’s data systems.

This includes incidents or events that happen by accident or deliberately. Both confirmed and suspected incidents may qualify as a data breach.

For the purposes of this data breach policy, an incident may include (but is not limited to) any of the following:

• Unauthorised use or accessing of data

• Unauthorised modification of data

• Loss of personal or sensitive data

• Theft of personal or sensitive data

• Loss or theft of equipment on which data has been stored

• Individual error

• Any attempts to gain access to data or our company IT systems (both successful or

failed)

• Defacement of web property

• Physical incidents, like a fire, which could compromise IT systems

### How to report a data breach

All employees who access, manage or use data in any way are responsible for reporting a data breach or any other type of security incident. This report should be made immediately to the employee’s line manager, using the data breach reporting log.

This report must include full details of the incident or breach, when it occurred, who the data

relates to and how. It must also include details about the individual reporting the incident.

If a data breach or a data security incident occurs outside of normal company hours, or a data breach or data security incident is discovered outside of normal company hours, it must be reported as soon as possible.

Any violation of this data breach policy could result in disciplinary action procedures taking

place for company employees.

### Data breach containment and data recovery

All necessary steps must be immediately carried out to minimise the effects of any data

security breach or data security incident. This process of containment should begin with an

initial assessment designed to establish the severity of the incident. The initial assessment

should also include analysing whether there is any way to recover the lost data, and mitigate

further risks associated with the incident.

Your initial assessment should include the following information:

• The data involved

• Whether the data involved is sensitive in nature

• The individuals affected

• The security measures that are in place to protect the data

• What has happened to the data

• Whether the data involved could be used in an illegal or otherwise inappropriate way

• Any perceived wider consequences associated with the breach or incident

### Data breach notification

The management team and DPO will determine which individuals must be notified in the event of a data breach or data security incident. Each incident must be assessed on a case-by-case basis. In every instance, the following considerations will be made:

• Any contractual notification requirements

• Any legal notification requirements

• How many people are affected

• What consequences may occur as a result of the data breach or data security incident

• Whether notification of a breach or incident would help the individual to mitigate risks

associated with the incident

• Whether notification could assist the company in meeting its legal obligations under

UK GDPR and Data Protection Act 2018

• Whether notifying an individual could prevent the unauthorized or illegal use of data

• Whether we must notify the Information Commissioner’s Office

All data breaches and data security incidents, both suspected and verified, must be recorded, to assist in further analysis and to help prevent further breaches.

### The danger of notifying too many individuals

There will be data security incidents in which a large number of individuals will need to be

notified. However, there will be other incidents in which notifying a large number of individuals may have the potential to cause disproportionate enquiries.

Whenever we notify an individual whose personal data has been affected by an incident or

breach, that notification must include a description of when the breach occurred, how the

breach occurred and what data was involved. Notifications must also include explicit guidance concerning what said individual can do to protect themselves. We should also outline to concerned individuals what steps our company has already taken to mitigate risks.

### Data breach evaluation and response

After the data breach or data security incident has been contained by carrying out all

necessary measures, we will conduct an extensive review detailing:

• The cause(s) of the breach

• The effectiveness of any responses

• Whether changes to existing IT systems, company procedures or policies must be

implemented

All existing protocols must be reviewed to analyse their adequacy. Any necessary amendments to protocols must be identified and carried out as soon as possible.