DATA BREACH POLICY, LETTER AND REPORTING TEMPLATE

Data breach policy, letter and reporting template guidance

How should I use my data breach policy, letter and reporting template?

Your company's data breach policy, letter and reporting template document outline the policy your company should adopt, and processes you should enact in the event of a data breach. The accompanying reporting template will provide your company with a space to record and report those breaches. You should complete these templates where necessary, and store these with your GDPR documents for safekeeping.

Will I need to update my data breach policy, letter and reporting template?

Yes. It is a crucial aspect of your company's GDPR compliance to ensure that you have a clearly defined policy in place dictating what your company will do in the event of a data breach. You should review this policy at least every 6 months and amend as necessary to ensure your company remains GDPR compliant.

Data breach policy, letter and reporting template

Here at [COMPANY NAME], 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 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 form.

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

[COMPANY NAME] 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 GDPR and Data Protection Act 2018

- Whether notifying an individual could prevent the unauthorised or illegal use of data
- Whether [COMPANY NAME] 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, [COMPANY NAME] 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.

Data breach report form

Please complete this form in the event of a data breach or data security incident:

To be completed by employee	
Date of incident	
Date incident was discovered	
Name of the individual reporting incident	
Contact details of the individual reporting incident	
Where the incident occurred	
Description of the incident	
Number of data subjects affected by incident	
Personal data placed at risk by incident	
Description of any actions taken at the point of discovery	

To be completed by the Data Protection Officer or [COMPANY NAME] management	
Name of individual receiving report	
Date report received	
Name of individual the report was forwarded to for action	
Date the report was forwarded for action	

Data breach letter template

Dear [Customer Title and Surname],

We regret to inform you that [COMPANY NAME] has discovered a breach in our processing system that has exposed your personal data to unauthorised use by external parties. We have notified the Information Commissioner's Office (ICO) and relevant law enforcement agency about this incident and will work with cyber security experts and legal counsel where needed to minimise any further risk posed to you by this incident.

About the incident

We appreciate you're going to have questions and concerns relating to this data incident, and we will do our best to explain the situation, what happened and why.

[COMPANY NAME] has conducted an investigation and we believe the following events led to the data security incident in question:

- [List timeline of events here]
- *DETAILS*

About the data involved

We believe the following personal information about you may have been unlawfully accessed or affected by this data security incident:

- [List details here]
- *DETAILS*

What this means for you

Following the investigation [COMPANY NAME] has carried out as part of this data security incident, and bearing in mind the type of information or data relating to the incident, we believe you may experience the following consequences as a result of this incident:

- [List details here]
- *DETAILS*

As a result, we would recommend you take the following actions as soon as possible to further protect yourself from additional risks associated with this incident:

- [List details here]
- *DETAILS*

What will we do to prevent this from happening in the future?

Here at [COMPANY NAME], your privacy is one of our top concerns. We do everything we can to ensure your personal data is made secure and your individual rights are preserved and upheld at all times. On this occasion we have fallen short, and we wholeheartedly and unreservedly apologise.

To ensure that data security incidents like this do not occur in the future, [COMPANY NAME] is already taking the following steps to eliminate future risk and minimise the impact such threats could pose to you in the future:

- [List details here]
- *DETAILS*

What happens next?

We will not send you further email updates relating to this incident unless you explicitly request information. Any further emails you may receive about this security incident should be treated as suspicious, and we would encourage you to verify the authenticity of any further correspondence relating to this incident by contacting our Data Protection Officer, [DATA PROTECTION OFFICER NAME] at [DATA PROTECTION OFFICER EMAIL ADDRESS].

We will publish future updates relating to this data security incident on our website, which you can access here: *COMPANY WEBSITE URL*.

Once again, we would like to take this opportunity to apologise for this breach of security. We promise to do everything within our power to make sure this never happens again.

If have additional questions about this incident or your individual rights, please contact our Data Protection Officer, [DATA PROTECTION OFFICER NAME] at [DATA PROTECTION OFFICER EMAIL ADDRESS].

Yours Sincerely,

[Name of employee]
[Job title]
[Company contact details]

Data breach reporting template

Please complete all fields of this form.

Breach identification number	Date logged	Impact on Data Subject	Breach confined	ICO notified of the Breach	Data subjects notified