



THE CONSERVATORY INSULATION COMPANY

Data Breach Policy and Reporting

Version: 0.2
Date: 17.04.2023
Created by: GDPR Local
Stored at: Safe storage

Data Breach Policy	1	
The Conservatory Insulation Company ©2023 All Rights Reserved.		

Background

As an organisation, we store, process, and share a reasonable amount of personal information. Personal data is a valuable asset that needs to be adequately 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 its format.

This policy applies to everyone at this organisation. This includes temporary, casual or agency staff and contractors, consultants, suppliers, and data processors/sub-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

Data Breach Policy	2	
The Conservatory Insulation Company ©2023 All Rights Reserved.		

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 IT systems
- Attempts (failed or successful) to gain unauthorised access to information or IT system
- Unauthorised disclosure of sensitive/confidential data
- Website defacement
- Hardware or software failure
- Failure of our servers or other infrastructure components
- 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
- Illegal actions by employees, contractors, volunteers, or other third parties

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

Data Breach Policy	3	
The Conservatory Insulation Company ©2023 All Rights Reserved.		

- Loss of availability of personal data

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 the data involved
- The protections that are in place (e.g., encryption)
- What has happened to the data (has it been lost, stolen, disclosed to unauthorised parties?)
- 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 to the competent Supervisory Authority

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 would be completed as part of the reporting process. All staff should be aware that any breach might result in disciplinary procedures being instigated.

Data Breach Policy	4	
The Conservatory Insulation Company ©2023 All Rights Reserved.		

Reporting an incident to other Authorities

It may be necessary to report the incident to other relevant authorities such as:

- Technical support organisations [cyber security experts]
- Other Data Protection Supervisory Authorities
- Law enforcement
- Customers / clients / other third parties
- other third parties such as banks, suppliers, and other affected parties

How much time do we have to report a breach?

We would report a notifiable breach to the competent Supervisory Authority without undue delay, but not later than 72 hours after becoming aware of it. Shall it take longer than this, we 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 competent Supervisory Authority.

What breaches do we need to notify the competent Supervisory Authority about?

When a personal data breach has occurred, we would establish the likelihood and severity of the resulting risk to people’s rights and freedoms. If it is likely that there will be a risk, then we must notify the competent Supervisory Authority, if it’s unlikely then we are under no obligation to report it. However, shall we decide the breach is not notifiable, we shall be able to justify this decision. In each case [reportable or non-reportable], we will document the breach internally.

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

Data Breach Policy	5	
The Conservatory Insulation Company ©2023 All Rights Reserved.		

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 stipulates to 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. Article 33(4) allows us to provide the required information in phases, as long as this is done without further undue delay.

Data Breach Policy	6	
The Conservatory Insulation Company ©2023 All Rights Reserved.		

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 stipulates we must inform the affected data subjects 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 competent Supervisory Authority. Again, we shall 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, we 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?

We shall describe, in clear and plain language, the nature of the personal data breach and, at least:

- The name and contact details of our Data Protection Officer (or nominated Data Lead) or other contact point where more information can be obtained
- The name and contact details of our EU/UK Representative, if applicable
- 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.

Data Breach Policy	7	
The Conservatory Insulation Company ©2023 All Rights Reserved.		

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

We shall ensure that all breaches are recorded, regardless of whether or not they need to be reported to the competent Supervisory Authority.

Article 33(5) of the GDPR requires documents relating to the breach, its effects and the remedial action taken. This is part of our overall obligation to comply with the accountability principle.

As with any security incident, we shall investigate whether 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 shall 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 individuals affected, or are there very serious consequences?
- Whether the competent Supervisory Authority shall be notified

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

Data Breach Policy	8	
The Conservatory Insulation Company ©2023 All Rights Reserved.		

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 20 million euros or 4% of your global turnover. The fine can be combined with the competent Supervisory Authority's other corrective powers under Article 58 of the GDPR. We have a robust breach-reporting process in place to ensure we 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.

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 the Data Protection Lead:

Name of Data Protection Lead: James Murray

Company name: The Conservatory Insulation Company

Email: info@theconservatoryinsulationcompany

Data Breach Policy	9	
The Conservatory Insulation Company ©2023 All Rights Reserved.		

Data Protection Lead Address: Grangefield mill, Grangefield road, Leeds, LS28
6JT

Data Protection Lead Number: 08009991931

Data Breach Policy	10	
The Conservatory Insulation Company ©2023 All Rights Reserved.		

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 the person reporting an incident
Date when the incident was discovered	
Date(s) of incident	
Place of incident	
Name of person reporting the incident	
Contact details of person reporting the incident (email address, telephone number)	
Brief description of the 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 Policy	12	
The Conservatory Insulation Company ©2023 All Rights Reserved.		

Data Breach Form Letter

Dear [insert data subject's name]

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 [insert the competent Supervisory Authority] 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...

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 have to take. e.g., will they need to change their password or seek legal advice. The competent Supervisory Authority 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

Data Breach Policy	13	
The Conservatory Insulation Company ©2023 All Rights Reserved.		

subject as possible

For further information please contact the Data Protection Lead

Name of Data Protection Lead: James Murray

Company name: The Conservatory Insulation Company

Email: info@theconservatoryinsulationcompany

Data Protection Lead Address: Grangefield mill, Grangefield road, Leeds, LS28 6JT

Data Protection Lead Number: 08009991931

Data Breach Policy	14	
The Conservatory Insulation Company ©2023 All Rights Reserved.		

Breach Log Template

Complete the following table to track data breach events.

Breach Number	Date Received	Data Subject Impact	Breach Contained	Breach Reported to the Supervisory Authority	Data Subjects Informed

Data Breach Policy	15	
The Conservatory Insulation Company ©2023 All Rights Reserved.		