Data Breach Response Plan

SeguraTech Ltd

Date created: December 2025
Date modified: December 2025
Version: 1.0

Purpose

This procedure defines how SeguraTech Ltd identifies, assesses, manages, and reports personal data breaches in line with UK GDPR.

Responsibility

Responsible persons:
Mike Richards
Swetha Stejskal

Either authorised data handler may initiate the breach response process.

What constitutes a data breach

A personal data breach is any incident leading to the accidental or unlawful loss, destruction, alteration, unauthorised disclosure of, or access to personal data.

Examples include emails sent to the wrong recipient, loss or theft of a device, unauthorised account access, accidental deletion of data, or disclosure to an unintended party.

Immediate response

Upon becoming aware of a suspected breach, immediate steps are taken to contain the incident, secure systems, preserve evidence, and notify the other authorised data handler.

Assessment

The breach is assessed to determine the type of data involved, the number of individuals affected, whether the data was protected, and the likelihood and severity of harm.

ICO notification

The Information Commissioner's Office will be notified within 72 hours where the breach is likely to result in a risk to the rights and freedoms of individuals.

Where notification is not required, the reasoning is documented.

Notification to individuals

Affected individuals will be informed without undue delay where the breach is likely to result in a high risk to their rights and freedoms.

Documentation and review

All breaches, whether reportable or not, are documented internally.

Following any incident, controls and procedures are reviewed and updated where necessary to reduce the risk of recurrence.