

**Data Security Breach Reporting Form**

A data security breach can happen for a number of reasons: Loss or theft of data or equipment on which data is stored, inappropriate access controls allowing unauthorised use, equipment failure, human error, unforeseen circumstances such as a fire or flood, hacking attack, ‘blagging’ offences where information is obtained by deceiving the organisation who holds it. Use this form to report such breaches.

**Article 2(2) of the Notification Regulation states:**

The provider shall notify the personal data breach to the competent national authority no later than 24 hours after the detection of the personal data breach, where feasible. The provider shall include in its notification to the competent national authority the information set out in Annex I. The Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR) provide rules about sending marketing and advertising by electronic means, such as by telephone, fax, email, text and picture or video message, or by using an automated calling system. PECR also include other rules relating to cookies, telephone directories, traffic data, location data and security breaches. Detection of a personal data breach shall be deemed to have taken place when the provider has acquired sufficient awareness that a security incident has occurred that led to personal data being compromised, in order to make a meaningful notification as required under this Regulation.

Date and time of Notification of Breach	
Notification of Breach to whom  Name  Contact Details	
Details of Breach	
Nature and content of Data Involved	
Number of individuals affected:	
Name of person investigating breach  Name	

<p>Job Title</p> <p>Contact details</p> <p>Email</p> <p>Phone number</p> <p>Address</p>	
<p>Information Commissioner informed</p> <p>Time and method of contact</p> <p><a href="https://report.ico.org.uk/security-breach/">https://report.ico.org.uk/security-breach/</a></p>	
<p>Police Informed if relevant</p> <p>Time and method of contact</p> <p>Name of person contacted</p> <p>Contact details</p>	
<p>Individuals contacted</p> <p>How many individuals contacted?</p> <p>Method of contact used to contact?</p> <p>Does the breach affect individuals in other EU member states?</p> <p>What are the potential consequences and adverse effects on those individuals?</p> <p>Confirm that details of the nature of the risk to the individuals affected: any measures they can take to safeguard against it; and the likely cost to them of taking those measures is relayed to the individuals involved.</p>	
<p>Staff briefed</p>	
<p>Assessment of ongoing risk</p>	

Containment Actions: technical and organisational security measures have you applied (or were to be applied) to the affected personal data	
Recovery Plan	
Evaluation and response	