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.

Example: Reportable Theft or loss of an unencrypted laptop computer or other unencrypted portable electronic/digital media holding names, addresses, dates of birth and National Insurance Numbers of individuals. A manual paper-based filing system (or unencrypted digital media) holding the personal data relating to named individuals and their financial records etc. More information can be found using the below link:

https://ico.org.uk/media/fororganisations/documents/1562/guidance on data security breach management.pdf

Breach Containment and Recovery

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	
Job Title	
Contact details	
Email	
Phone number	
Address	
Information Commissioner informed	
Time and method of contact	
https://report.ico.org.uk/security-breach/	
Police Informed if relevant	
Time and method of contact	
Name of person contacted	
Contact details	
Individuals contacted	
Manager Call Manager and A2	
How many individuals contacted?	
Nacth and of courts at wood to courts at 2	
Method of contact used to contact?	
Doos the buses by offerst individuals in other FU	
Does the breach affect individuals in other EU	
member states?	
What are the notential concessioned adverse	
What are the potential consequences and adverse	
effects on those individuals?	
Confirm that dataile of the nations of the will to the	
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.	
Staff briefed	
Assessment of ongoing risk	
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	