Data Breach Notification Procedure

Ark Build PLC

January 2025

Data Breach Procedure – January 2025

Table of Contents

Data Breach Procedure – January 2025

Introduction

The following breach procedure is designed to be used when an incident has occurred that has resulted in, or is believed to have resulted in, a breach under the EU General Data Protection Regulations (GDPR). This could be either a loss of confidentiality, integrity or availability of the personal data for which Ark Build Plc (the Company), is either the “Data Controller” or “Data Processor” for client data.

It is a requirement of the EU General Data Protection Regulations (GDPR), that a “Data Controller” must report without undue delay, and where feasible within 72 hours, any incidents which are likely to result in a risk to the rights and freedoms of data subjects, to the Supervisory Authority. In the U.K. this is the Information Commissioners Office (ICO). If it is not possible to meet the 72-hour deadline then clear reasons for the delay must be provided. It is also a requirement that a data processor must inform the data controller without undue delay when they become aware of a breach, so that the data controller is able to meet its obligations.

As a data controller, where the incident affects personal data, a decision must be made with regards to the extent, timing and content of any communication to “Data Subjects”. The GDPR requires that this communication must happen “without undue delay” if the breach is likely to result in a “high risk to the rights and freedoms of natural persons”.

As a data processor, initial communication should be made to the data controller, however direct communications to the Supervisory Authority may be necessary later.

This document should only be used for guidance when responding to an incident, as the nature and extent of each incident cannot be predicted. Common sense should always be applied when deciding on a course of action, however following the steps included here should ensure the Company is meeting it obligations under GDPR.

Personal Data Breach Notification Procedure – Data Controller

Once a breach of personal data has been ascertained, there are two parties under GDPR who may need to be informed. These are;

1. The supervisory authority (ICO)
2. The data subjects affected

It cannot be assumed that as a breach has occurred, that in all cases that the breach needs to be notified. This will depend on the assessment of the risk that the breach represents to "the rights and freedoms of natural persons" (GDPR Article 33).

The following sections describe the decision-making process and what to do if notification is required.

Supervisory Authority contact details

The following table details the contact details of the Supervisory Authority for the purposes of GDPR for the company.

Name:	Information Commissioners Office.
Address:	The Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF
Telephone:	0303 123 1113
Email:	casework@ico.org.uk

Table 1 - Supervisory Authority Contact Details

Deciding whether to notify the Supervisory Authority

Under Article 33 of the GDPR, it states that a personal data breach shall be notified to the Supervisory Body "unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons". This therefore means that before notification, the Company must assess the level of risk before deciding on its course of action and whether to notify or not. This decision should be documented and retained.

Factors that should be taken into consideration as part of this risk assessment should include:

- The Data items included e.g. name, address, bank details, health records
- Whether the personal data was encrypted and if so the strength of the encryption used.

- Whether the personal data was pseudonymised (i.e. whether a living individual can be identified from the data)
- The volume of data involved.
- The number of data subjects affected
- Nature of the breach e.g. accidental destruction, theft, loss of availability
- Any other factors that may be relevant to the incident.

The breach risk assessment will be carried out by members of the Information Security Group (ISG), and will result in a formal document that outlines the conclusion of the assessment, and any necessary steps to be taken.

This will then require sign-off by either the MD.

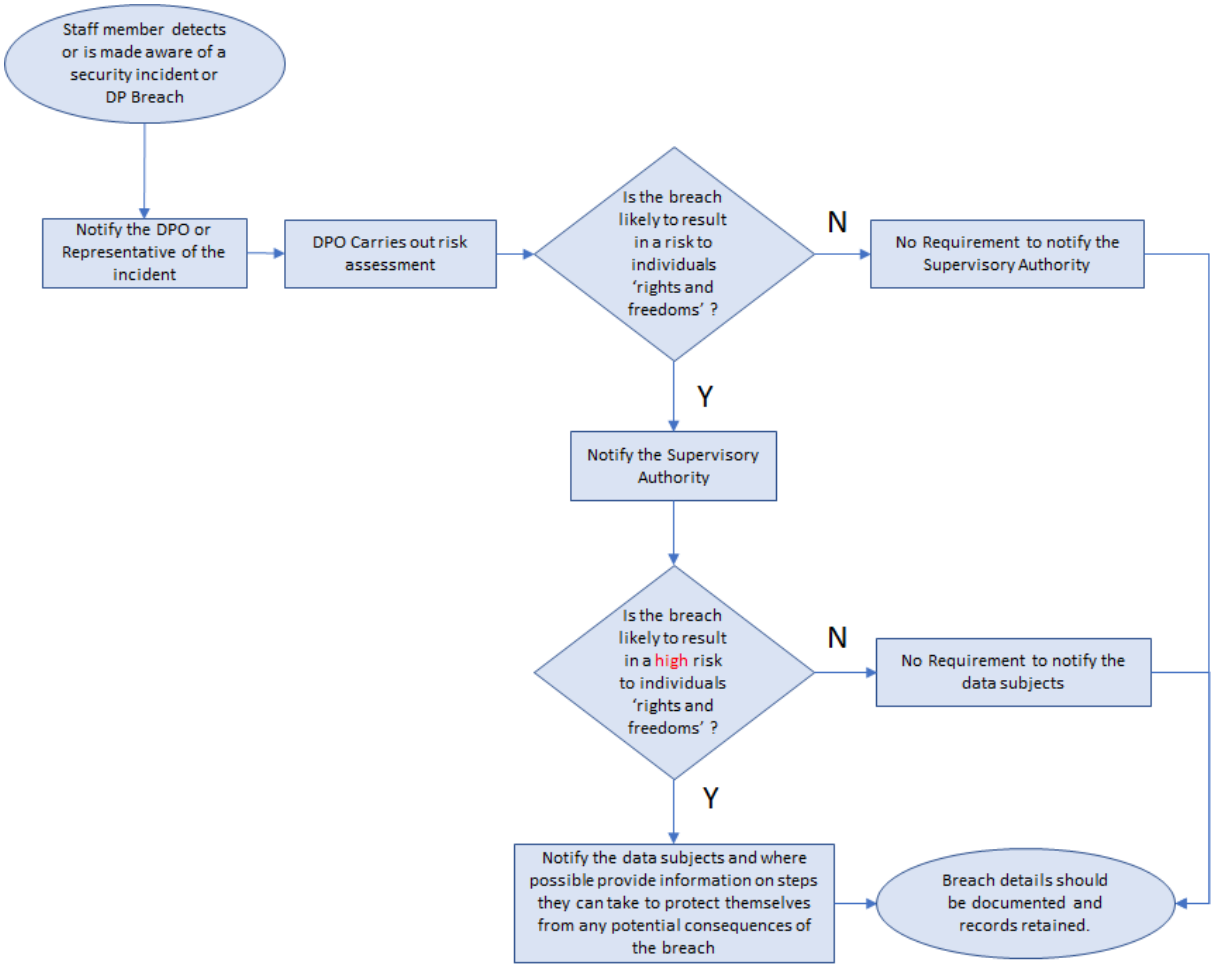
The conclusion should include one of the following;

1. The breach does require notification to the Supervisory Authority and the data subject
2. The beach only requires notification to the Supervisory Authority
3. Notification of the breach is not necessary.

This conclusion may change as further evidence is discovered as part of the investigation or upon feedback received from the supervisory authority.

Note – it has been stated that where any data that has been lost has been encrypted using a tool that meets FIP140-2 standards, such as Bitlocker, this would negate the need to notify the Supervisory Authority.

To help clarify the decision to notify the Supervisory Authority or not, the following Flowchart gives an overview of the process. Examples of potential scenarios, provided by the EU working party on data protection, can also be found in Annex A.



Notifying the Supervisory Authority

If it has been concluded that it is necessary to contact the Supervisory Authority, then GDPR requires that this should be carried out "without undue delay and where feasible, not less than 72 hours after becoming aware of it" (Article 33). However, if there are legitimate reasons for not giving notification within the above timescale, then these reasons must also be stated when notification is given.

In some cases, it may not be possible to get a comprehensive report outlining all aspects of the investigation into the breach within the notification deadline and the Supervisory Authority would not expect to receive this. However, as a minimum the notification should include the scope of the breach, cause, mitigation actions being taken and how the problem will be addressed to prevent further reoccurrence. When or if further details come to light, these can be added later.

Notification should be given via secure means to the body listed in *Table 1 - Supervisory Authority Contact Details*, above.

Data notification forms can be found in the document folder storage in the data protection forms library on the Shared Drive at HSQE- GDPR.

When notifying the Supervisory Authority there are a number of mandatory items. These have been prepopulated in the template documents, to help speed up the notification process. Listed below are the details that should be included for clarification;

- Organisation Details
  - Name of the organisation and is it the data controller in respect of the breach.
  - Who the Supervisory Authority should contact for further details and information
  - Data Controller registration number
- Details of the data breach
  - Description of the incident including as much detail as possible
  - When did the incident happen?
  - How did the incident happen?
  - If there has been a delay in reporting include the reasons for the delay
  - What measures did the Company have in place to prevent an incident of this type occurring?
  - Extracts of any policies and procedures relevant to the incident, explaining which were in existence at the time of the incident and the dates on which they were implemented
- Personal data placed at risk
  - What personal data has been placed at risk? Specify if this included any sensitive personal or financial data and the extend of the incident.
  - How many individuals have been affected?
  - Are the affected individuals aware of the incident?
  - What are the potential consequences and adverse effects to the individuals?
  - Have any affected individuals complained to the Company about the incident?
- Containment and Recovery
  - Has the Company taken any action to minimise or mitigate the effect on the affected individuals? If so, provide details.
  - Has the data placed at risk now been recovered? If so, provide details of how and when this occurred.

    - What steps has the Company taken to prevent a reoccurrence of the incident?
- **Training and guidance** (optional but will be included in the template document)
    - Does the Company provide its staff with training? If so provide any extracts relevant to this incident.
    - Please confirm training is mandatory for all staff. Had any staff members involved in this incident received training and if so when?
    - As a data controller, does the Company provide any detailed guidance to staff on the handling of personal data in relation to the incident reported? If so, please provide extracts relevant to the incident.
- Previous contact with the Supervisory Authority
    - Has the company reported and previous incidents in the last two years?
    - If the answer to the above is yes, please provide: brief details, the date when it was reported and if know the Supervisory Authority reference number.
- Miscellaneous
    - Have any other Supervisory Authorities (overseas) been contacted about this incident? If so provide details.
    - Have the Police been informed of the incident? If so provide details. Please include the force concerned and the crime reference number (if applicable).
    - Have any other regulatory bodies been informed of the incident (e.g. Banks, Solicitors Regulator Authority)? If so provide details.
    - Has there been any media coverage if the incident? If so provide details.

Sending in the notification

Send your completed form to casework@ico.org.uk, with 'DPA breach notification form' in the subject field, or by post to:

The Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF.

The ICO should, within 7 days, send you a case reference number and information about any next steps or clarification required.

Help with the Breach notification

Additional help with completing the Breach notification form in the UK can be obtained from the ICO helpline on **0303 123 1113** or **01625 545745** (09.00 – 17.00 Mon-Fri)

Personal Data Breach Notification Procedure – Data Processor

It is a requirement of the EU General Data Protection Regulations (GDPR), that a "Data Processor" must report without undue delay, any incidents which are likely to result in a risk to the rights and freedoms of data subjects, to the "Data Controller" for which it is processing the information. It remains the responsibility of the Data Controller to then notify the Supervisory Authority of the breach.

Many of the details need to be provided by the Data Processor are similar to those for the controller, this is so that the Data Controller is able to pass on the relevant information to the Supervisory Authority.

- Organisation Details
  - Name of the processor and contact details of the organisations data protection representative.
  - Data Processor registration number
- Details of the data breach
  - Description of the incident including as much detail as possible
  - When did the incident happen?
  - How did the incident happen?
  - If there has been a delay in reporting include the reasons for the delay
  - What measures did the Company have in place to prevent an incident of this type occurring?
  - Extracts of any policies and procedures relevant to the incident, explaining which were in existence at the time of the incident and the dates on which they were implemented
- Containment and Recovery
  - Has the Company taken any action to minimise or mitigate the effect on the affected individuals? If so, provide details.
  - Has the data placed at risk now been recovered? If so, provide details of how and when this occurred.
  - What steps has the Company taken to prevent a reoccurrence of the incident?
- **Training and guidance** (optional but will be included in the template document)
  - Does the Company provide its staff with training? If so provide any extracts relevant to this incident.

  - Please confirm training is mandatory for all staff. Had any staff members involved in this incident received training and if so when?
  - As a Data Processor, does the Company provide any detailed guidance to staff on the handling of personal data in relation to the incident reported? If so, please provide extracts relevant to the incident.
- Miscellaneous
  - Have the Police been informed of the incident? If so provide details. Please include the force concerned and the crime reference number (if applicable).
  - Have any other regulatory bodies been informed of the incident (e.g. Banks, Solicitors Regulator Authority)? If so provide details.
  - Has there been any media coverage if the incident? If so provide details.

Notification should be given via secure means to the body listed in *Table 1 - Supervisory Authority Contact Details*, above.

Data notification forms can be found in the SharePoint document folder storage in the data protection forms library.

Annex A.

The following is a list of examples and the actions that should be taken to help assist data controllers decide whether they need to notify a breach to the Supervisory Authority

Example	Notify the supervisory authority?	Notify the data subject?	Notes/recommendations
i. A controller stored a backup of an archive of personal data encrypted on a CD. The CD is stolen during a break-in.	No	No	As long as the data was encrypted with a state of the art algorithm (FIPs140-2), backups of the data exist, and the unique key is not compromised, this may not be a reportable breach. However, if it is later compromised, notification is required.
ii. Personal data of individuals are ex-filtrated from a secure website managed by the controller during a cyber-attack. The controller has customers in a single Member State.	Yes, report to competent supervisory authority if there are potential consequences to individuals.	Yes, report to individuals depending on the nature of the personal data affected and if the severity of the potential consequences to individuals is high.	If the risk is not high, we recommend the controller to notify the data subject, depending on the circumstances of the case. For example, notification may not be required if there is a confidentiality breach for a newsletter related to a TV show, but notification may be required if this newsletter can lead to political point of view of the data subject being disclosed
iii. A brief power outage lasting several minutes at a controller's call centre meaning	No	No	This is not a notifiable personal data breach, but still a recordable incident. Appropriate records should be

customers are unable to call the controller and access their records.			maintained by the controller.
iv. A controller suffers a ransomware attack which results in all data being encrypted. No back-ups are available and the data cannot be restored. On investigation, it becomes clear that the ransomware's only functionality was to encrypt the data, and that there was no other malware present in the system.	Yes, report to the competent supervisory authority, if there are potential consequences to individuals as this is a loss of availability.	Yes, report to individuals, depending on the nature of the personal data affected and the possible effect of the lack of availability of the data, as well as other likely consequences.	If there was a backup available and data could be restored in good time, this would not need to be reported to the supervisory authority or to individuals as there would have been no permanent loss of availability or confidentiality. However, the supervisory authority may consider an investigation to assess compliance with the broader security requirements.
v. An individual phones a bank's call centre to report a data breach. The individual has received a monthly statement for someone else. The controller undertakes a short investigation (i.e. completed within 24 hours) and establishes with	Yes	Only the individuals affected are notified if there is high risk and it is clear that others were not affected.	If, after further investigation, it is identified that more individuals are affected, an update to the supervisory authority must be made and the controller takes the additional step of notifying other individuals if there is high risk to them.

a reasonable confidence that a personal data breach has occurred and if it is a systemic flaw so that other individuals are or might be affected.			
vi. A multi-national online marketplace suffers a cyber-attack and usernames, passwords and purchase history are published online by the attacker.	Yes, report to lead supervisory authority if involves cross border processing.	Yes, as could lead to high risk	The controller should take action, e.g. by forcing password resets of the affected accounts, as well as other steps to mitigate the risk.
vii. A website hosting company (a data processor) identifies an error in the code which controls user authorisation. The effect of the flaw means that any user can access the account details of any other user.	As the processor, the website hosting company must notify its affected clients (the controllers) without undue delay. Assuming that the website hosting company has conducted its own investigation, the affected controllers should be reasonably confident as to whether each has suffered a breach and therefore is likely to be considered as having "become	If there is likely no high risk to the individuals they do not need to be notified.	The website hosting company (processor) must consider any other notification obligations (e.g. under the NIS Directive). If there is no evidence of this vulnerability being exploited with this particular controller a notifiable breach may not have occurred but is likely to be recordable or be a matter of noncompliance under Article 32.

	aware" once they have been notified by the hosting company (the processor). The controller then must notify the supervisory authority.		
viii. Medical records in a hospital are unavailable for the period of 30 hours due to a cyber-attack.	Yes, the hospital is obliged to notify as high-risk to patient's well-being and privacy may occur.	Yes, report to the affected individuals.	
ix. Personal data of 5000 students are mistakenly sent to the wrong mailing list with 1000+ recipients.	Yes, report to supervisory authority	Yes, report to individuals depending on the scope and type of personal data involved and the severity of possible consequences.	
x. A direct marketing e-mail is sent to recipients in "to:" or "cc:" field, thereby enabling each recipient to see the email address of other recipients.	Yes, notifying the supervisory authority may be obligatory if a large number of individuals are affected, if sensitive data are revealed (e.g. a mailing list of a psychotherapist) or if other factors present high risks (e.g. the mail contains the initial passwords).	Yes, report to individuals depending on the scope and type of personal data involved and the severity of possible consequences.	Notification may not be necessary if no sensitive data is revealed and if only a minor number of email addresses are revealed.

Data Breach Procedure – January 2025

Document Revision

This is a controlled document and any revisions, amendments or changes must be agreed by the Information Security Group. At a minimum, this document will be reviewed annually with any amendments record in the document revision history below.

Revision Date	Sections Revised	Signed	Name
01/05/19	Revision for GDPR	L. Amoah	Lawrence Amoah
04/01/2020	Annual review and update	L. Amoah	Lawrence Amoah
07/01/2021	Annual review and update	L. Amoah	Lawrence Amoah
06/01/2022	Annual review and update	L. Amoah	Lawrence Amoah
04/01/2023	Annual review and update	L. Amoah	Lawrence Amoah
05/01/2024	Annual review and update	L. Amoah	Lawrence Amoah
04/01/2025	Annual review and update	L. Amoah	Lawrence Amoah