Personal Data Breach Notification Procedure

Reference: UK GDPR DOC 2.5 Issue No: 2

Issue Date: 24TH May 2018

Amended: 5 May 2023

1. Definition of a personal data breach

Article 4 (12) defines a breach as "a breach of security leading to the accidental or lawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed."

Destruction of data:
This is where the data no longer exists, or no longer exists in a form that is of any use to Prospect.

Damage to data:
This is where personal data has been altered, corrupted or is no longer complete.

Loss of data:
This means the data may still exist, but Prospect has lost control or access to it, or no longer has it in its possession.

Unauthorised or unlawful processing of data:
This may include disclosure of personal data to (or access by) recipients who are not authorised to receive (or access) the data, or any other form of data that violates UK GDPR.

Data breaches can be categorised as:

1. **Confidentiality breach** - where there is an unauthorised or accidental disclosure of, or access to personal data.
2. **Integrity breach** - where there is unauthorised or accidental alteration of personal data.
3. **Availability breach** - where there is an accidental or unauthorised loss of access to, or destruction of, personal data.

Note: Examples of breach scenarios are in Appendix 1 to this document.

2. The scope of our Personal Data Breach Notification Procedure

This procedure applies in the event of a personal data breach under Article 33 of the UK GDPR – *Notification of a personal data breach to the supervisory authority* – and Article 34 – *Communication of a personal data breach to the data subject*.

The UK GDPR draw a distinction between a 'data controller' and a 'data processor' in order to recognise that not all organisations involved in the processing of personal data have the same degree of responsibility regarding personal data breaches. Each organisation must establish whether it is a data controller, or a data processor for the same data processing activity; or whether it is a joint controller. Under UK GDPR, if the processor becomes aware of a breach of personal data it is processing on behalf of the controller, it must notify the controller without undue delay.

Note: The processor does not need to first asses the likelihood of risk arising from a breach before notifying the controller; it is the controller that must make the assessment on becoming aware of the breach. The processor just needs to establish whether a breach has occurred and report it to the Controller.

3. Responsibility

3.1 All users whether employees, representatives, processors, contractors and third-party users of Prospect are required to be aware of, and to follow this procedure in the event of a personal data breach (reference Training Policy UK GDPR DOC 1.1).

3.2 All Employees, representatives, contractors, third party or temporary staff are responsible for reporting any personal data breach to the Data Protection Compliance Officer (DPCO) as soon as they become aware of a breach or potential breach.

4. Procedure – Breach Notification Data Processor to Data Controller

Note: The data processing contract between the controller and the processor should have the contact details and relevant procedures for reporting data breaches.

4.1 Prospect as the data processor will, once Prospect's DPCO has been given all the details, report any personal data breach or security incident to the Data

Controller without undue delay. Prospect's Data Controllers are listed on the Record of Processing Register. Details of a breach will be recorded in the Internal Breach Register held by the DPCO.

4.2 The breach notification to the Controller should be made by email and followed up with a phone call.

4.3 A confirmation of receipt of this information should also be by email and a follow-up phone call.

5. Procedure - Breach Notification - Data Controller to Supervisory Authority (ICO)

5.1 Prospect as the controller will, once the DPCO has been given all the incident details; establish if a personal data breach has occurred. The DPCO will liaise with the Director of Communications and Research, SMT and Head of IT to evaluate the risk. Prospect will report any personal data breach to the ICO without undue delay. Details of breach are recorded in the Internal Breach Register held by DPCO.

Notification to Information Commissioners Office (ICO)

5.2 Prospect will assess whether the personal data breach is likely to result in a **risk** to the rights and freedoms of the data subjects affected by the personal data breach and determine if the supervisory authority (ICO) needs to be notified in the event of a breach. The evaluation can be done by conducting a data protection impact assessment (DPIA) against the breach.

If there is **NO** risk – then there is no requirement to notify the ICO or individuals.

If **YES** and the breach is likely to result in a high risk to data subject (s), Prospect reports the personal data breach, by email and phone, to the supervisory authority, which is the ICO, without undue delay, and not later than 72 hours

If the breach affects individuals in more than one Member State, Prospect will notify their lead supervisory authority.

If the data breach notification to the supervisory authority is not made within **72 hours**, Prospects, DPCO submits details of the breach electronically with a justification for the delay.

Notification to individual (data subject)

5.3 Prospect will evaluate if the breach is likely to result in a high risk to individual rights and freedoms and determine if they need to be notified in the event of a breach.

If there is **NO** risk – then there is no requirement to notify the induvial.

If **YES** – and the breach is likely to result in a high risk to data subject (s), Prospect notifies the affected **individual** by phone and email and, where required, provides them with information on steps they can take to protect themselves from consequences of the breach without undue delay.

5.4 If it is not possible to provide all of the necessary information at the same time, Prospect will provide the information in phases without undue further delay.

5.5 The following information needs to be provided to the supervisory authority

- A description of the nature of the breach.
- The categories of personal data affected.
- Approximate number of data subjects affected.
- Approximate number of personal data records affected.
- Name and contact details of the DPCO.
- Consequences of the breach, including consequences that have already occurred and those that are likely to occur.
- Any measures taken to address the breach.
- Any information relating to the data breach. This may be submitted in phases, if necessary.

5.6 The DPCO notifies the supervisory authority, the ICO. Contact details for the ICO are recorded in the Schedule of authorities and key supplier list held by the DPCO.

5.7 In the event the supervisory authority assigns a specific contact in relation to a breach, these details are recorded in the Internal Breach Register held by the DCPO.

5.8 The breach notification is made by email and telephone call.

5.9 A confirmation of receipt of this information is made by email and telephone call.

6. Procedure - Breach Notification Data Controller to Data Subject

6.1 Prospect evaluates if the personal data breach is likely to result in **high risk** to the rights and freedoms of the data subject and determines if they need to be notified.

If there is **NO** risk – then there is no requirement to notify the individual.

If **YES –** and the breach is likely to result in a high risk to data subject (s) , Prospect notifies the affected individual by phone and email immediately, where required, provides them with information on steps they can take to protect themselves from consequences of the breach without undue delay.

6.2 The notification to the data subject describes the breach in clear and plain language, in addition to the information specified in clause 4.6 above.

6.3 Prospect takes measures to render the personal data unusable to any person who is not authorised to access it.

6.4 Prospect takes subsequent measures to ensure that any risks to the rights and freedoms of the data subjects are no longer likely to occur as soon as practicable.

6.5 If the breach affects a high volume of data subjects and personal data records, Prospect will make a decision based on an assessment of the amount of effort involved in notifying each data subject individually, and whether it will hinder Prospect's ability to appropriately provide the notification within the specified time frame. In such a scenario a public communication or similar measure will inform those affected in an equally effective manner.

6.6 If Prospect has not notified the data subject(s), and the ICO considers the likelihood of a data breach will result in a high risk, Prospect will communicate the data breach to the data subject as soon as practicable.

6.7 Prospect records any personal data breaches, incorporating the facts relating to the personal data breach, its effects and the remedial actions taken. This will be held in the Internal Breach Register.

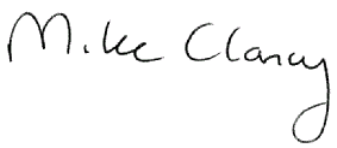
Document Control

The Data Protection Compliance Officer is the owner of this document and is responsible for ensuring that this procedure is reviewed in line with the review requirements of the UK GDPR.

A current version of this document is available to all members of staff on Prospects intranet and is published in the Library.

This procedure was approved by the General Secretary (GS) on 24th May and is issued on a version-controlled basis under their signature.

Signature: Date: 24/05/2018



Mike Clancy
GENERAL SECRETARY

Change History Record

Issue	Description of Change	Approval	Date of Issue
1	Initial issue	DPCO	24/05/2018
2	Amended in line with changes to legislation	DPCO	18/05/2023

Personal Data Breach Notification Procedure

Reference: UK GDPR DOC 2.5 Issue No: 2

Issue Date: 24TH May 2018

Amended: 5 May 2023

APPENDIX 1 – FOR STAFF USE ONLY
Examples of Breach Scenarios and who to notify

The following non-exhaustive examples, information will assist Prospect in determining whether we need to notify in different personal data scenarios. These examples may also help to distinguish between risk and high risk to the rights and freedoms of individuals.

Item	Example	Is it breach?	Notify the ICO	Notify the data subject?	Notes/Recommendations	Remedial

USB Stick Encrypted	A controller stored a backup of an archive of personal data encrypted on a USB stick. The key is stolen during a break in.	Yes Article 4 (12)	No	No	As long as the data are encrypted with a state of the art algorithm, backups of data exist, the unique key is not compromised, and the data can be restored in good time, this may not be a reportable breach. However, if it is later compromised, notification is required.	Article 32 (1) & (2) - assess processes and appropriate organisational and technical measures in place to protect Personal Data, especially staff training.
USB Stick Non-Encrypted	A Prospect employee loses a USB stick on a train containing all member contact details.	Yes Article 4 (12)	Yes - if the risk to individuals is identified. Article 33(1)	Depends on whether stick was encrypted and what details were on it-if not and details sensitive – then yes notify the individual.	In the case of a loss of a USB stick with unencrypted personal data, it is often not possible to ascertain whether unauthorised persons gained access to that data. Nevertheless, even though Prospect may not be able to establish if a confidential breach has taken place, such a case has to be notified as there is a reasonable degree of certainty that an availability breach has occurred, Prospect would become aware when it released the USB stick had been lost.	Article 32 (1) & (2) - assess processes and appropriate organisational and technical measures in place to protect personal data, especially staff training.

Power Outage – a short period	A brief power outage lasting several minutes at Prospects member contact centre meaning members are unable to call Prospect and access their records.	Yes	No	No	This is not a notifiable breach, but still a recordable accident under article 33 (5). Appropriate records should be maintained by Prospect.	
Power Outage – a long period	The member contact centre suffers a power cut due to workmen drilling through a cable. The member database is unavailable to staff for twenty minutes during which time they cannot help a member with their queries.	Yes Article 4(12)	No - data not accessible by staff but not at risk	No - Article 34 (3) c may apply but carry out risk-assessment	This is not a notifiable breach, but still a recordable accident under article 33 (5).	Article 32 (1) & (2) - assess processes and appropriate organisational and technical measures in place to protect Personal Data, especially back-up/disaster recovery issues.
Mailing List	Special Category Data of a large number of members are mistakenly sent to the wrong mailing list with 1000+ recipients.	Yes - Prospect has clear evidence that a breach has occurred	Yes, report to ICO	Yes, report to individuals depending on the scope and type of the personal data involved and the severity of possible consequences.		Article 32 (1) & (2) - assess processes and appropriate organisational and technical measures in place to protect Personal Data, especially staff

						training.
Direct Marketing e-mails	Direct Marketing e-mails are sent to recipients in the "to" or "cc" fields, thereby enabling each recipient to see the email address of other recipients.	Yes - Prospect has clear evidence that a breach	Yes, notifying the ICO may be obligatory of a large number of individuals are affected, if sensitive data are revealed (e.g. a mailing list of members) or if other factors present high risks (e.g. the mail contains initial passwords).	Yes, report to individuals depending on scope and type of personal data involved and the severity of possible consequences.	The notification may not be necessary if no sensitive data is revealed and if only minor number of email addresses are revealed.	Article 32 (1) & (2) - assess processes and appropriate organisational and technical measures in place to protect Personal Data, especially staff training.
Ransomware Attack	Ransomware Attack which results in all data being encrypted. No back-ups are available and the data cannot be stored. On investigation, it becomes clear that the ransomewares only functionality was to encrypt the data, and that there was no other malware present in the system.	Yes Article 4(12). Prospect has clear evidence that a breach.	Yes, report to the ICO if there is likely to consequences to individuals as this is 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 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 ICO or to individuals as there would have been no permanent loss of availability or confidentiality. However, if the ICO became aware of the incident by other means, it may consider an investigation to assess compliance with the broader security requirements of article 32.	
Mobile Phone	A Prospect employee loses a work-issued mobile phone, which contains high-value	Yes Article 4(12). Prospect	No - risk mitigated by encryption. Article 32 (1) a	Assess the risk		Article 32 (1) & (2) - assess processes and appropriate organisational and

	members' account details. The phone is password protected and encrypted.	has clear evidence that a breach.				technical measures in place to protect Personal Data, especially staff training
Post	An envelope containing credit card slips was mistakenly thrown into a waste bin rather than securely destroyed. The waste bin was emptied to a large bin left outside Prospect premises for waste collection. When the mistake was discovered the envelope was retrieved. It had not been opened.	Yes - technical	No - personal data recovered	No-personal data recovered		More of an incident than a breach, but Article 32 (1) & Article 4(12) (2) - assess processes and appropriate organisational and technical measures in place to protect personal data especially disposal of confidential material.