




EFFECTIVELY MANAGING DATA BREACHES

INSTITUTE OF CHARTERED SURVEYORS IRELAND

AISLING HENNESSY



WHILE EVERY EFFORT HAS BEEN TAKEN IN PRODUCTION OF THESE MATERIALS NO REPOSNSIBILITY IS TAKEN BY SETU, SOCIETY OF CHARTERED SURVEYORS IRELAND OR THE AUTHOR FOR ANY ERRORS OR OMMISSIONS. PROFFESIONAL ADVICE SHOULD BE TAKEN IN ALL CASES. COPYRIGHT AISLING HENNESSY.

ALL RIGHTS RESERVED



Relevant legislation

- Articles 33 and 34
- Recitals 75, 85, 86, 88
- Sections 141 – 143 of Data Protection Act 2018

What is a personal data breach?

- Breach of security leading to the **accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access** to, personal data transmitted, stored or otherwise processed.
- (Article 4 (12) of the GDPR)





Data breaches – Annual Report of DPC 2022

Total valid breach notifications received in 2022 was 5,828.

The highest category of data breaches notified to the DPC in 2022 related to **unauthorised disclosures, in cases affecting one or small numbers of individuals, accounting for 62% of the total notifications**

Most frequent cause of breaches reported to the DPC arose as a result of correspondence inadvertently being misdirected.

(Annual report of Data Protection Commission, 2022)

Data Breaches – Annual Report of DPC 2022

Annual Report 2022

Data Breach Notification by Category	Charity	Private	Public	Voluntary	Total
Disclosure unauthorised - Postal Material to incorrect recipient	18	1067	836	15	1936
Disclosure unauthorised - Email incorrect recipient	40	456	563	22	1081
Disclosure unauthorised - Other	24	294	229	24	571
Integrity - unintentional alteration (PD disclosed)		407	7		414
Unauthorised Access - Paper files/ Documents/Records	15	117	178	8	318
Paper Lost/Stolen - Official Documentation		9	236	3	248
Availability - accidental (Loss/destruction of PD)	6	47	189		242
Hacking	12	186	9	2	209
Paper Lost/Stolen	5	38	130	3	176
Processing error - (PD Disclosed)	8	87	47	6	148
Integrity - unauthorised alteration (PD disclosed)	1	80	3		84
Unauthorised Access - Online Account	1	37	22	2	62

Annual Report of Data Protection, 2022



Case study 50

- Complaint concerned a statutory body whose functions include the investigation of complaints concerning experts' professional conduct, training or competence.
- Letter concerning complaint was sent to incorrect email address. It was encrypted but password sent to same incorrect email address.
- Letter included special category data in relation to a number of data subjects.
- What could controller have done differently?



CASE STUDY 51

- Employee working from home reviewing applications from candidates for a job, disposed of applications in the domestic recycling bin – weather caused them to be dispersed.
- Employer had instructed employees working from home to minimise printing and destroy anything printed before disposing of it.
- More technical organisational measures required here. DPC made it clear that ensuring compliance with organisational measures a matter for employer.
- Provision of shredder?
- Policies and procedures (and training) need to be updated to take account of working from home.

Possible effect of data breach for data subjects

Loss of control over
personal data

Limitation of rights

Discrimination

Identity theft

Fraud

Financial loss

Unauthorised
reversal of
pseudonymisation

Damage to
reputation

Loss of
confidentiality
protected by
professional secrecy

Different Types of Breach

- Confidentiality breach
- Availability breach
- Integrity breach



Case study 39 – loss of paper files in transit

- Transfer by public body of hard copy files for legal proceedings – contained special category personal data.
- Hard copy files went missing in transit with no backups available.
- Did not have sufficient procedures in place for the secure removal and storage of hard-copy files that contained special-category personal data.



WHEN MUST THE DPC BE NOTIFIED OF A DATA BREACH?

Must notify the DPC that a personal data breach has occurred unless they are able to demonstrate that the personal data breach is ***“unlikely to result in a risk to the rights and freedoms of a data breach”***.

How to assess the risk to the data subject

- Need to give sufficient weight to certain criteria ***when assessing the likelihood and gravity of any potential risk to data subjects*** (DPC Guidelines, 2019).
- Two separate assessments if first assessment determines that breach not unlikely to result in risk to rights and freedoms of data subject, then need to consider whether risk is such that controller must also notify breach to data subjects (DPC Guidelines, 2019).
- Keep record of how and when assessments carried out.

What to consider when assessing risk to rights of data subject

Type of breach (sensitive or special category personal data).

Nature, sensitivity and volume of personal data.

Circumstances of the data breach;

Was the personal data protected by appropriate technical protection measures such as encryption or pseudonymisation;

The ease of direct or indirect identification of the data subjects;

Likelihood of reversal of pseudonymization or loss of confidentiality;

Likelihood of fraud, financial loss, or other forms of misuse of the personal data;

Likelihood of personal data being used maliciously;

Likelihood that breach could result in and severity of physical, material or non-material damage to data subjects;

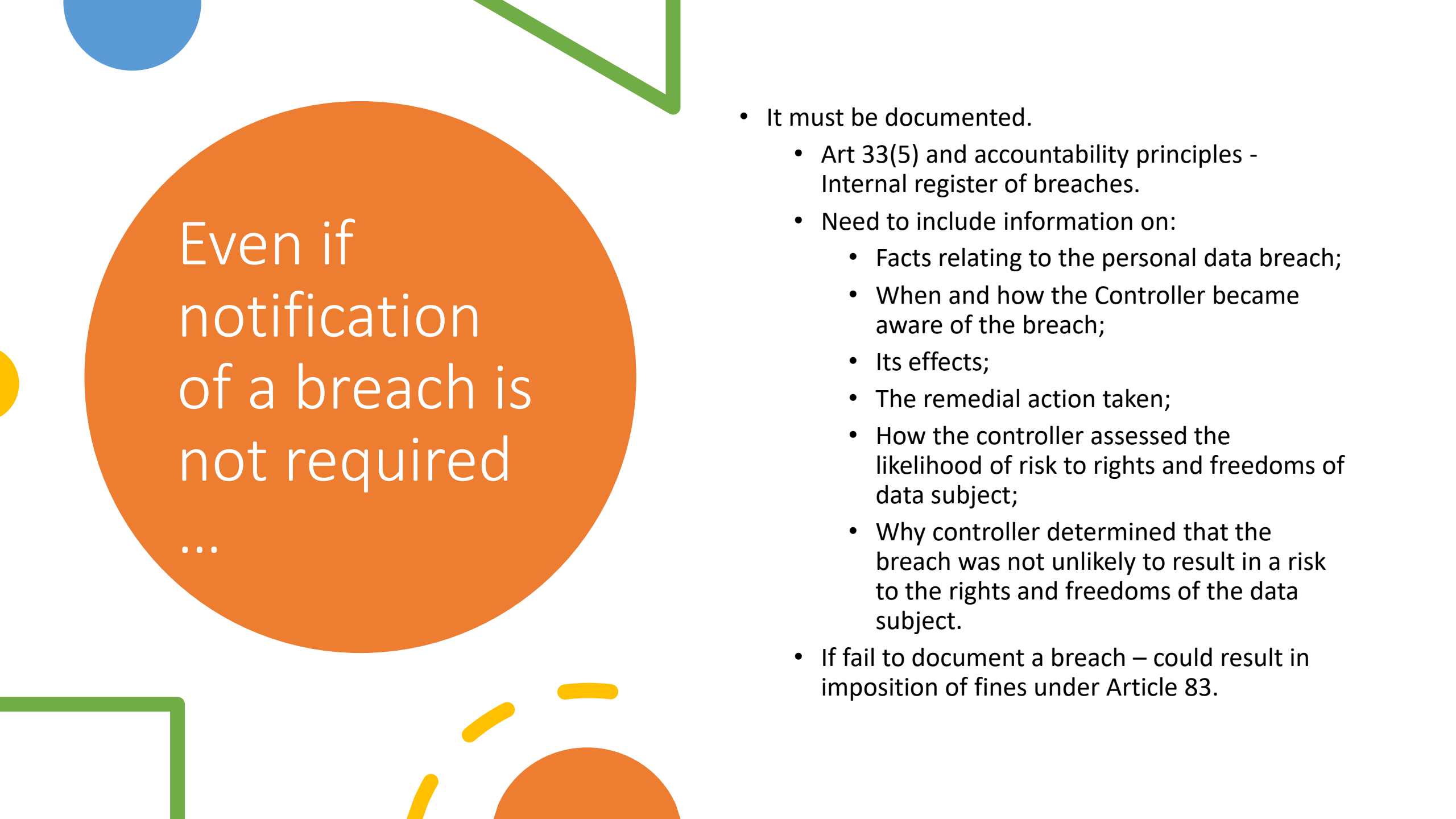
Whether breach could result in discrimination, damage to reputation or harm to data subjects or fundamental rights;

Special characteristics of the individual;

Special characteristics of the controller;

Number of affected individuals;

(DPC Guidelines, 2019 and EDPB Guidelines, 2023)



Even if
notification
of a breach is
not required

...

- It must be documented.
 - Art 33(5) and accountability principles - Internal register of breaches.
 - Need to include information on:
 - Facts relating to the personal data breach;
 - When and how the Controller became aware of the breach;
 - Its effects;
 - The remedial action taken;
 - How the controller assessed the likelihood of risk to rights and freedoms of data subject;
 - Why controller determined that the breach was not unlikely to result in a risk to the rights and freedoms of the data subject.
- If fail to document a breach – could result in imposition of fines under Article 83.

Becoming aware of a breach

- In the event of a notifiable personal data breach, data controllers must notify the supervisory authority **without undue delay or as soon as possible** and, where feasible, not later than 72 hours after having **become aware of it**.
- Deemed to have become aware of security breach where “controller has a reasonable degree of certainty that a security incident has occurred that has lead to personal data being compromised”.





Becoming aware of a breach

- To comply with principle of accountability, Controller should be able to demonstrate to the DPC (1) **when** and (2) **how** they became aware of a personal data breach.
- DPC recommends that controllers “as part of their internal breach procedures, have a system in place for recording how and when they became aware of a data breach”

Becoming aware of a breach

“It should be ascertained whether all appropriate technological protection and organisational measures have been implemented to establish immediately whether a personal data breach has taken place and to inform promptly the supervisory authority and the data subject”

(Article 87)





Becoming aware of a data breach

- Must have appropriate technical knowledge available to enable controller to enable them to identify without undue delay;
 - That they have been the victim of a security incident such as a cyber-attack;
 - The measures and actions which should be taken immediately after a breach has occurred and
 - Appropriate safeguards which should have been employed to reduce the risk of incidents of this nature occurring.

(DPC Guidelines, 2019)

72-hour period

- If breach notification made outside this period – must provide reason for delay with notification.
- Will be in breach of its obligation “unless reason given is sufficient to justify the delay”. (DPC Guidelines)
- If Controller does not have the required information can notify in phases and can provide further information in due course.

Information to be included in notification to supervisory authority (Article 33)

- A notification to the authority must “**at least**”:
- (a) describe the nature of the personal data breach, including the number and categories of data subjects and personal data records affected;
- (b) provide the data protection officer’s contact information;
- (c) describe the likely consequences of the personal data breach; and
- (d) describe how the controller proposes to address the breach, including any mitigation efforts.

Additional
information
Controller
should be able
to provide to
DPC to assist in
reviewing
notification

- Detailed description of how the breach occurred;
- Detailed description of the source of the breach;
- Information on how and when Controller became aware of breach notification.
- What immediate steps were undertaken upon discovery of the breach;
- Any further plans/steps to be taken and the time frame of their introduction;
- Whether all relevant records, such as audit logs, have been retained;
- A record of processing;
- Relevant policy and procedures documentation; and
- **Explanation for any delay (if applicable).**

(DPC Guidelines, 2019)



Notification of a personal data breach to data subjects (Article 34)

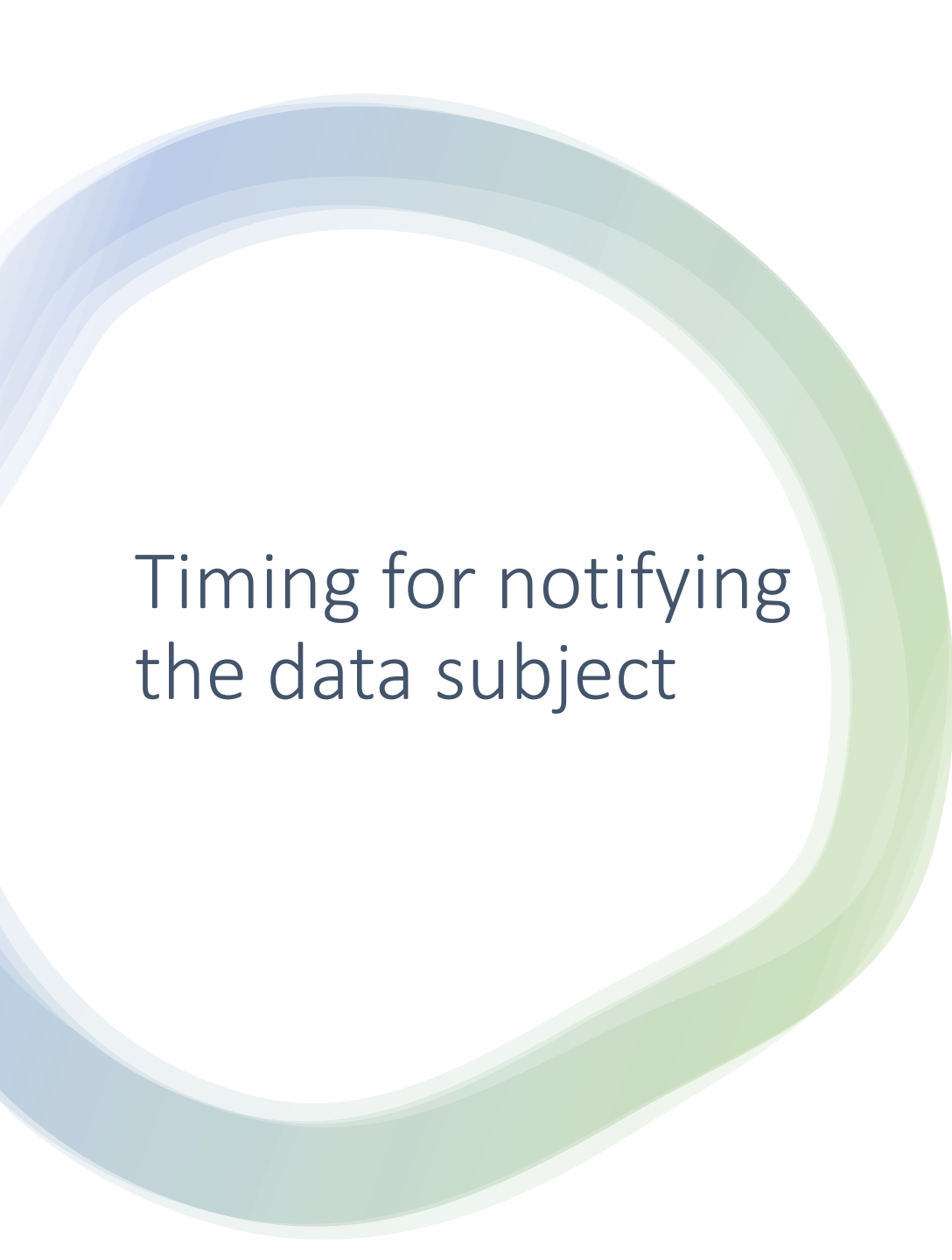
- If the controller has determined that the personal data breach “**is likely to result in a high risk to the rights and freedoms of individuals,**” it must communicate information regarding the personal data breach to the affected data subjects.
- Higher test than notification to supervisory authority.

No duty to notify data subjects where:-

(a) the controller has “implemented appropriate technical and organizational protection measures” that “render the data unintelligible to any person who is not authorized to access it, such as encryption”;

(b) the controller takes actions subsequent to the personal data breach to “ensure that the high risk for the rights and freedoms of data subjects” is unlikely to materialize; or

(c) when notification to each data subject would “involve disproportionate effort,” in which case alternative communication measures may be used – e.g. public notices.



Timing for notifying the data subject

- Should be made “without undue delay *in close cooperation with DPC.*” (DPC Guidelines, 2019)
- “When there is a need to mitigate an immediate risk to data subjects, prompt communication with data subjects will be necessary”. (DPC, 2019)
- Can still notify data breach to data subjects even if not required to.
- In certain circumstances where justified and on advice of law-enforcement the controller may delay communicating the breach to affected individuals until such time as would not prejudice investigations. (Recital 88 and EDPB Guidelines, 2023)

What must be included in notification to data subjects (Article 34)

- Communication to data subject must be in clear language and contain at least the following information:-
 - Description of nature of the breach;
 - Name and contact details of the DPO or other contact point;
 - Description of the likely consequences of the breach; and
 - Description of measures taken or proposed to be taken by the controller to address breach including where appropriate measures to mitigate possible adverse effects.
 - Specific advice on protecting themselves from adverse consequences.

Controller/Processor relationship

Contract should specify that the processor ***shall assist the controller in ensuring compliance with the obligations pursuant to Articles 32 – 36 taking into account the nature of processing and the information available to the processor*** (Article 28(3)(f) of the GDPR).

Processor must notify the Controller “without undue delay”.

Responsibility for assessing the likelihood of risk arising from the breach and notification of the breach remains with the Controller.

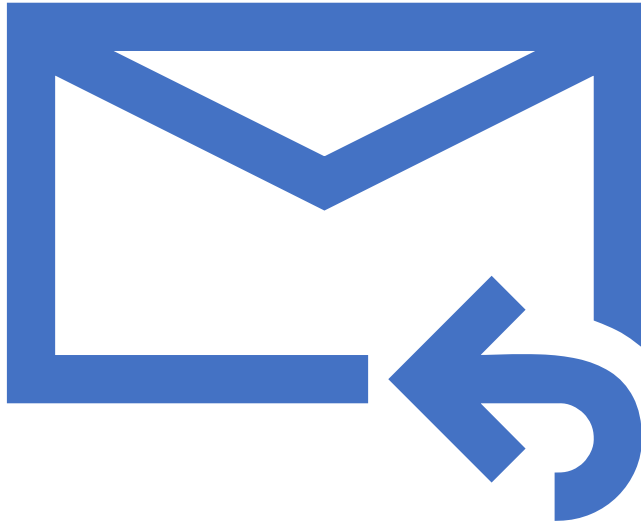
Controller should be considered “aware” once Controller makes them aware of the breach.

Contract with processor must include procedures for notifying a breach to the Controller “without due delay”.

Being prepared ..

- Policies and Procedures in dealing with personal data breaches:
 - Have system in place for recording how and when Controller becomes aware of personal data breaches;
 - Information concerning all security-related incidents should be directed towards a responsible person(s) with the task of addressing (i) addressing incidents (ii) establishing the existence of a breach and (iii) assessing the risk.
 - Risk to individual should be assessed (no risk, risk, high risk) and relevant departments within the organisation informed.
 - Notify DPC and if relevant the data subjects;
 - At same time Controller should be able to contain and recover the breach.
 - Document the breach as it develops.
- (DPC Guidelines, 2019 and EDPB Guidelines, 2023)

Case study 52



- Charity supporting people with intellectual disabilities send an email to a number of people.
- Email addresses were included in the carbon copy (cc) rather than blind carbon copy (bb) field.
- Poor awareness of personal data awareness found in the organisation.

Actions to take
where data
breach due to
emails sent in
error to wrong
address

“It is incumbent on the data controller to take all reasonable steps to remedy such a breach.

- *recalling the email from the sender,*
- *Asking the unintended recipient to confirm they have deleted the email, and thereafter putting in place measures to prevent a recurrence.”*

P.26 Annual Report of the DPC, 25 May
2018 – 31 December 2018

Resources

- Practical Guide to Personal Data Breach Notifications under the GDPR (Data Protection Commission, October 2019)
- Guidelines 9/2002 on personal data breach notification under GDPR version 2 (European Data Protection Board, Adopted 28 March 2023)
- DPC case studies booklet 2018 – 2023

