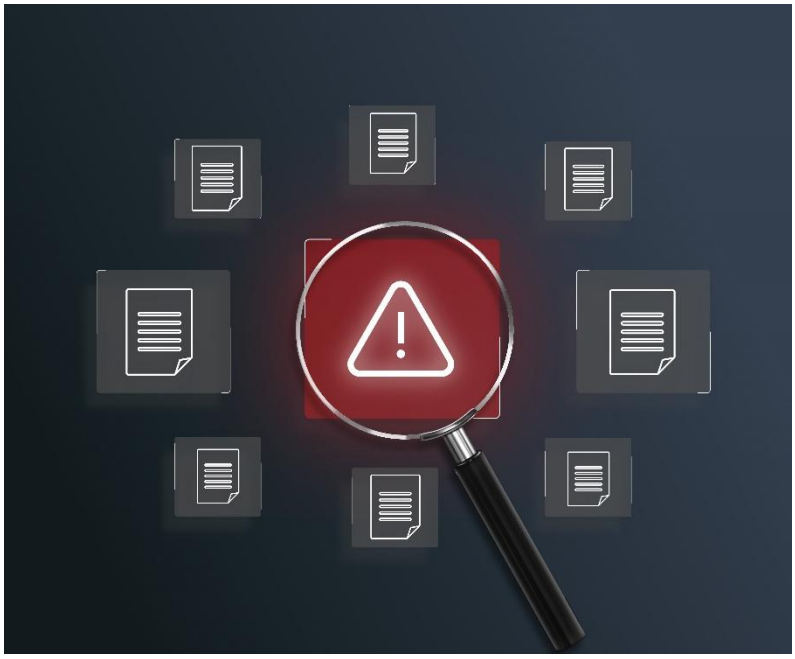
National Federation of Voluntary Service Providers
Pension & Life Assurance Scheme

Data Incident Response Procedure

July 2026



Oranmore Business Park, Oranmore, Galway, Ireland, H91 TP2W
+ 353 (0)91 792316 pensionadmin@fedvol.ie www.fedvol.ie

Pension Authority No: PB67866 Revenue Approval No: SF7346

National Federation of Voluntary Service Providers
Pension & Life Assurance Scheme

PURPOSE:

This Data Incident Response Procedure ("Procedure") outlines the procedures and responsibilities for effectively managing and mitigating the impact of data incidents, ensuring compliance with legal requirements and protecting sensitive information.

The Trustees are subject to obligations under the Data Protection Act 2018, the General Data Protection Regulation (EU) 2016/679, and related Irish and European Union data protection legislation governing the processing of personal data.

Pension Scheme data includes sensitive personal information such as financial details, health records, family circumstances, and employment history, which creates heightened risks in the event of a data breach and requires specialised response procedures.

The Trustees recognise that data breaches involving pension scheme information may result in significant harm to data subjects, regulatory sanctions, reputational damage, and financial liability, necessitating prompt and co-ordinated response measures.

This Procedure establishes a comprehensive framework for detecting, notifying, assessing, and reporting to personal data breaches affecting the Pension Scheme in compliance with legal obligations and industry best practices.

This Procedure applies to all actual or suspected personal data breaches involving Pension Scheme data processed by the Trustees in connection with the operation and administration of the Pension Scheme.

The Procedure covers all forms of Pension Scheme Data including, but not limited to:

(a) Member personal and financial information held in electronic or physical format.
(b) Beneficiary and dependant records, documentation and correspondence.
(c) Employer contribution data and payroll information.
(d) Benefit calculation records.
(e) Correspondence and communications relating to scheme members.

This Procedure is triggered immediately upon discovery or notification of any incident that may constitute a Personal Data Breach, regardless of whether the breach is subsequently confirmed or the extent of impact determined. The Trustees may have reporting requirements other than to the Data Protection Commission, depending on the nature of the incident. These may be to An Garda Síochána, Pensions Authority (competent authority for DORA incidents), Central Bank of Ireland, employers of members, other data controllers and insurers.

DEFINITIONS:

Personal data & data subjects:

Personal data means any information relating to an identified or identifiable natural person ('data subject'). An identifiable natural person is a person who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. Data can be either automated or manual, that is, it can be in electronic or in paper format.

This information or data can be processed and held wholly or partly in an electronic format or non-electronic format. It does not matter what format the information is held in, if it contains data that identifies an individual, it is considered personal data. Personal data includes special categories of personal data.

Third-Party Providers:

The Trustees acknowledge that third-party providers appointed by the Trustees such as Irish Life and Cornmarket are independent Data Controllers.

1. DETECTING:

Categories of Data Breaches

The GDPR defines a "personal data breach" in Article 4(12) as: "a 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".

The European Data Protection Board (formerly the Data Protection Working Party under Article 29 (WP29)) outlines that security breaches can be categorised according to the following three information security principles:

- Confidentiality Breach: where there is an unauthorised or accidental disclosure of, or access to, personal data.
- Availability Breach: where there is an unauthorised or accidental loss of access to, or destruction of, personal data.
- Integrity Breach: where there is an unauthorised or accidental alteration of personal data.

A breach of confidentiality or integrity is relatively clear to identify; however, the occurrence of an availability breach may be less obvious. A breach is classified as an availability breach when there has been a permanent or temporary loss of, or destruction of, personal data e.g. a system is unavailable due to an electrical fault.

It should be noted that while these breaches may occur as separate incidents, depending on the circumstances a breach may consist of a combination of the above principles.

An individual may encounter information security incidents that may or may not involve a personal data breach. An individual is not expected to investigate and determine whether an information security event includes personal data. All information security incidents should be reported in line with this Procedure. In the remainder of this Procedure, the term "data breach" refers to both personal data breaches and information security incidents.

Examples of Data Breaches:

The following non-exhaustive list may be considered examples of data breaches where an individual is required to initiate the reporting process and begin documenting the breach:

- Sending an email to the wrong person.
- Sharing a document with an unintended recipient.

- Putting 2 member letters into one envelope.
- Loss or theft of personal data or equipment which stores personal data (E.g. loss of laptop, USB stick, iPad/tablet device, or paper records).
- Equipment theft or failure.
- Unauthorised use of, access to, or modification of personal data or information systems.
- Attempts (failed or successful) to gain unauthorised access to information or IT system(s).
- Unauthorised disclosure of personal data.
- Website defacement including social media accounts.
- Hacking attack.
- 'Blagging' offences where information is obtained by deceiving the organisation who holds it.
- Temporary loss of availability such as an electrical fault, fire or flood.

Third-Party Data Breaches:

The Scheme uses third parties to assist in fulfilling its role and to meet its legal obligations. Where the third party process personal data on behalf of the Scheme then they may act as either data controllers or data processors, depending on the nature of the work or service being provided. The Trustees have implemented appropriate written data processing or sharing agreements with these third parties.

Where the third party acts as a data processor for the Trustees, then the Trustees will retain overall responsibility for the protection of personal data, however, the processor is required to assist the Scheme in ensuring compliance with its obligations.

Third party data processors engaged by the Trustees are required to alert the Scheme's Data Protection Team, without undue delay, of all incidents (including suspected incidents) which give rise to the risk of unauthorised disclosure, loss, destruction or alteration of personal data, where the personal data compromised belongs to data subjects under the Scheme's control. The Data Protection Team will assess the incident as set out in this Procedure.

Third party data controllers are responsible for having appropriate policies and procedures for dealing with data breaches relating to personal data. Third party data controllers are not obliged to inform the Trustees of a data breach. The Trustees will not be obliged to assist the data controller in relation to the breach. However, mutual co-operation is in the best interests of members, and the Trustees and Data Protection Team should liaise with other data controllers as they deem necessary.

2. NOTIFYING

Who reports the data breach?

The person who first identifies the data breach is responsible for initiating the reporting of the breach incident to the Scheme's Data Protection Team. This applies even if they were not responsible for causing the breach incident and/or work in a different FedVol unit. You may pass your responsibility to another person but only on the clear understanding that they will report the data breach.

When to report the data breach?

The data breach must be reported immediately. The Trustees are permitted 72 hours to decide whether to report the data breach to the DPC. This is ordinary hours and not working hours e.g. if you become aware of a data breach incident at 10am on Friday then the Data Protection Team is obliged to investigate and determine if a report is necessary to the DPC by 10am on the following Monday.

What information is required?

The first priority is to verbally report the data breach to the Data Protection Team. It is helpful if the reportee is able to assemble the information required in sections 1 to 12 of the Data Breach Incident Report Form in Appendix 1. Please be very clear that reporting should be prioritised over gathering this information.

How to report the data breach?

The person must report the data breach incident verbally to the Data Protection Team. The verbal report can be done in person or by telephoning the Data Protection Team. If the members of the Data Protection Team cannot be contacted, then the incident must be reported to any Trustee. See Section 3 below.

3. ASSESSING:

Responding to a data breach:

Once the Data Protection Team has been informed of a potential data breach, the priority is to secure the data and then an investigation and assessment will take place to determine the risks arising from the data breach.

The aim of this investigation is to determine the nature of the data breach, the consequences for the data subjects involved, whether the requirement for notification has been triggered, and the mitigating or remedial actions to be taken.

Data Protection Team:

In the event of a potential data breach, a member of the following team must be contacted in order to respond effectively to the breach and quickly coordinate the actions of the Trustees:

- Chairman & Professional Trustee: Mr James Skehan - 086 919 1007
- Pension Scheme Manager: Ms Maria McMahon - 091 792316 - 087 996 1104

If they cannot be contacted for any reason, then one of the other Trustees should be notified.

- Mr John McHugo
- Ms Pauline Brennan
- Mr Francis Coughlan
- Ms Deirdre Herlihy
- Mr Bernard O'Regan

Securing the Data:

The priority is to secure the data that may have been breached. How this is achieved depends on the nature of the breach, e.g.:

Type of incident	**Potential response**
Letter received by wrong recipient	Ask recipient to return the letter to the Pension Scheme Manager
Email sent to wrong recipient	Ask recipient to delete email from inbox **and** from their deleted items
Loss/theft of IT equipment	Report to Gardaí and FedVol IT unit to ensure equipment cannot be reconnected to network.
Unauthorised access to data on FedVol network	Contact FedVol IT unit to request access denial
Detection of malware	Shut-down equipment that is affected and contact FedVol IT unit

Speed is of the essence and contact should be made by the most appropriate method - telephone is often the best way to communicate.

The Data Protection Team will determine the most appropriate actions to secure the data breached. They will assign responsibility to people to complete these actions and report back.

A letter may be issued, if considered appropriate, to an unintended recipient to provide reassurance that the Trustees takes data protection seriously.

Data Breach Incident Form:
The Data Protection Team will request that the reportee and/or the person responsible for causing the incident will complete the Data Breach Incident Report Form, see Appendix 1. The reportee completes sections 1 to 12 of the form.

Breach Categories:
Personal Data Breaches shall be classified into the following categories:

(a) **None:** No risk to Data Subjects
(b) **Unlikely Breach:** A breach is unlikely to have any impact on affected Data Subjects.
(c) **Low Risk Breach**: A breach that is unlikely to have an impact on affected Data Subjects, or the impact is likely to be minimal in a risk to the rights and freedoms of affected Data Subjects.
(d) **Medium Risk Breach**: A breach that may result in some risk to affected Data Subjects, but the impact is unlikely to be substantial.
(e) **High Risk Breach**: A breach that is likely to result in a high risk to the rights and freedoms of affected Data Subjects, requiring immediate notification to both the DPC and affected Data Subjects.
(f) **Very High Risk Breach**: The breach may have a critical, extensive or dangerous impact on Data Subjects.

Risk Assessment:
Once a potential breach has been detected, a risk assessment will be undertaken by the Data Protection Team to determine the potential resulting 'high risk' to the rights and freedoms of data subjects.

A 'high risk' occurs where the breach may lead to physical, material or non-material damage for the data subject and may include instances of discrimination, identity theft or fraud, financial loss or damage to reputation. When the breach involves personal data that reveals racial or ethnic origin, political opinion, religion or philosophical beliefs, or trade union membership, or includes genetic data, data concerning health or data concerning sex life, or criminal convictions and offences or related security measures, such damage to reputation should be considered likely to occur.

When assessing the risk, the Data Protection Team shall consider the specific circumstances of the data breach, including its severity and potential impact. The risk will also be evaluated on the basis of an objective assessment, considering the following criteria as recommended by the European Data Protection Board:

1. The type of data breach: the level of risk to the data subject will vary on whether the data breach is one of Confidentiality, Availability, or Integrity (See Section 1).
2. The nature, sensitivity and volume of personal data: consideration must be given to the type and special categories or sensitive nature of the data compromised (e.g. if a significant volume of sensitive financial data is compromised this would constitute a significant risk to the data subject).

3. Ease of identification of data subjects: consideration must be given as to how easy, or difficult, it would be to identify specific data subjects based on the compromised data.
4. Severity of consequences for data subjects: consideration must be given to the potential damage to data subjects, whether the recipient of the data is co-operating and may have malicious intentions, and the permanence of the consequences to the data subject.
5. Special characteristics of the data subject: consideration must be given to children or vulnerable data subjects who may be placed at a greater risk of danger due to the breach.
6. Number of affected data subjects: consideration must be given to the nature and context of the compromised data on the number of data subjects affected.
7. Special characteristics of the data controller: consideration must be given to the nature and activities of the Scheme, which may increase the level of risk to data subjects.
8. Should authorities become involved: the Trustees must consider the severity of the risk on the data subject and the likelihood of occurrence. Where doubt exists, the Trustees are to err on the side of caution and notify the Data Protection Commission and An Garda Siochána.

An assessment of such a breach may also be discerned from a Data Protection Impact Assessment (DPIA), if carried out previously, in relation to the processing activities affected by the data breach.

A detailed risk assessment methodology is set out in Appendix 2.

Additional guidance on evaluating risk can be found in the European Data Protection Board's (adopted from the Article 29 Data Protection Working Party) document entitled "Guidelines on Personal data breach notification under Regulation 2016/679" and in the European Union Agency for Network and Information Security (ENISA) document entitled "Recommendations for a methodology of the assessment of severity of personal data breaches".

4. REPORTING:

This section identifies the requirements, as outlined under Articles 33 and 34 of the GDPR, regarding the documentation and notification of data breaches to the DPC and to the data subject.

Breach Recording:

To demonstrate compliance and accountability, the Trustees shall maintain a brief record of each data breach. In circumstances where the DPC is not notified, an explanation of the basis of not doing so must also be retained. The purpose of this record is to allow the DPC to verify compliance with Article 33 (5) of the GDPR. This should be recorded on the Data Breaches & Incidents tab in the Scheme's Governance and Compliance Calendar.

In documenting the data breach, the Data Protection Team will record at least the following details:

- Cause of the data breach.
- Description of the data breach.
- Effects and consequences.
- Mitigating actions taken.
- Reasons behind the mitigating actions undertaken.
- Reasons for not reporting a data breach to the DPC, including reasons why the data breach was not considered likely to result in a risk to the data subject(s).

The Data Protection Team will also retain proof of communications to the data subject regarding data breaches to assist in demonstrating accountability and compliance.

Notification to the DPC:
Under Article 33 of the GDPR: "the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the DPC, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons."

Note: The European Data Protection Board states that a data controller is not considered to become 'aware' until they have a reasonable degree of certainty that a data breach incident has occurred which has resulted in personal data being compromised.

The personal data breach does not have to be notified where it is unlikely to result in a risk to the rights and freedoms of data subjects. Such a situation may arise where the personal data is encrypted.

Link to the DPC breach notification form.

The DPC has published guidance and other resources on breach notification, that can be found here.

Notification Delay:
Where the initial notification to the DPC is not made within 72 hours, it shall be accompanied by reasons for the delay.

Notification in Phases:
Where further investigation by the Data Protection Team is required, further information "may be provided in phases without undue further delay" accompanied by reasons for the delay, as outlined under Articles 33 of the GDPR.

When the Data Protection Team first notifies the DPC, it will outline whether it intends to supply more information at a later stage. If it transpires during the investigation that the incident was contained and there was no breach, the Data Protection Team will still notify the DPC to follow best practice.

Article 34 – Notification to the Data Subject:
Article 34 of the GDPR states that where a personal data breach is likely to result in a 'high risk' to the rights and freedoms of data subjects, the controller must communicate the personal data breach to the data subjects "without undue delay".

Assessing the risks to data subjects:
1. The Data Protection Team shall carry out an assessment as to whether the personal data breach results in a "high risk" to the rights and freedoms of a data subject.
2. In assessing whether a high risk occurs, the European Data Protection Board states the Data Protection Team must conduct their assessment considering, but not limited to, the following criteria:
   (a) The type of breach.
   (b) The nature, sensitivity and volume of personal data.
   (c) Ease of identification of data subjects.
   (d) Severity of consequences for data subjects.
   (e) Special characteristics of the data subject, especially vulnerable data subjects.
   (f) Number of affected data subjects.

(g) Special characteristics of the data controller.
(h) Should law enforcement be involved.

3. The assessment must be documented.

Where it is determined that a 'high risk' results, the Data Protection Team must communicate the breach to the data subjects in accordance with 4.3 of this Procedure.

The Data Protection Team will provide the data subject with specific information on steps to take to protect themselves. The exact information will depend on the nature of the incident.

Contacting the Data Subject:
The Data Protection Team will aim to contact the data subject directly unless it would involve a 'disproportionate effort' in line with Article 34(3) of the GDPR. Where this is the case, a public communication or similar approach will be taken.

This communication will be a dedicated message and sent separately to other information, such as newsletters or updates. The Data Protection Team will choose a means of communication that maximises the chance of properly communicating information to individual data subjects. The Trustees prefer if the initial contact is made either in person or by telephone. This allows for a more natural interaction and answering of specific questions. It is the policy of the Trustees to initiate contact between Monday to Thursday, avoiding initial contact on a Friday or any day before a public holiday unless no other option is available.

Information to be provided:
As outlined under Article 34 (2) of the GDPR, the breach notification to be supplied to the data subject by the Data Protection Team shall:

(1) Be in clear and plain language; and
(2) Include at least the following information:
   (a) Description of the nature of the breach.
   (b) The contact details of the Data Protection Team or other contact point where more information can be obtained.
   (c) Description of the likely consequences of the personal data breach.
   (d) Description of the measures taken by the Trustees to address the personal data breach, including measures to mitigate the breach's adverse effects.

Conditions Where Notification is not Required:
Under Article 34(3), the GDPR provides three conditions where a notification to a data subject is not required in the event of a personal data breach:

(a) Technical and Organisational Measures: the Trustees have applied appropriate technical and organisational measures to protect personal data prior to the breach, in particular those measures that render personal data unintelligible to any person who is not authorised to access it (e.g. encryption). However, even where data is encrypted, a loss of data may have negative consequences for data subjects where the Trustees retained no backups. In this regard, a notification to the data subject would be required as the breach affects the Trustees' ability to "restore the availability and access" to personal data.
(b) Subsequent Measures: the Trustees have taken subsequent measures which ensure that the high risk to the rights of the data subject are no longer likely to materialise.

(c) Disproportionate Effort: communication to the data subjects would involve disproportionate effort. In such an instance, as outlined above, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.

5. DATA BREACH INCIDENT REVIEW:

Following completion of the steps in sections 1 to 4 above, the Data Protection Team will conduct a full review of the cause of the data breach, the subsequent actions taken, and the existing controls to determine whether further actions are required to prevent the incident from occurring again. These actions may include reviewing systems or implementing policies and procedures.

6. AWARENESS AND TRAINING

All Trustees and relevant FedVol staff are aware of their responsibility to promptly report data breaches incidents. They must be aware of the procedure for reporting data breaches and the point of contact to which the data breaches are required to be reported.

All new Trustees and relevant FedVol staff will receive training on the Trustees' data protection policies and procedures as part of their induction program. This will include coverage of their responsibilities under this Procedure.

All Trustees and the Pension Scheme Manager have been trained on how to respond to data breaches in line with this Procedure. Please contact the Data Protection Team in the first instance.

Approval and Next Review Date of this Procedure:

This document was approved and came into effect as follows:

Document Control	
Approved By:	Mr. James Skehan Scheme Chairman & Professional Trustee, National Federation of Voluntary Service Providers' Pension & Life Assurance Scheme
Approved By:	Mr. John McHugo Scheme Vice Chairman, National Federation of Voluntary Service Providers' Pension & Life Assurance Scheme
Date approved:	30th July, 2026
Next review date	30th October, 2029
Previous versions	30th October, 2025

Signed: _____ **Date: 30th July, 2026**

James Skehan,

Chairman & Professional Trustee.

Signed: _____ **Date: 30th July, 2026**

John McHugo,

Vice Chairman.

APPENDIX 1: DATA BREACH INCIDENT REPORT FORM

The Data Incident Report should be completed by the Pension Scheme Manager and reviewed by the Professional Trustee before presenting to the Trustee Board for review and final decision.

Incident Name	
Completed by	Pension Scheme Manager
Employer	
Date	

#	Question	Response
1	Actual or approximate date on which the breach occurred	
2	Is the breach ongoing?	
3	Date the breach ended	
4	Date the breach became known	
5	Has there been a delay in notifying the DPC of a personal data breach? (i.e. more than 72 hours after the breach became known)	
6	Reason for the delay	
7	How were you made aware of the breach?	
8	Type of breach	
9	Nature of the breach	
10	How did the breach occur	
11	Cause of the breach	
12	Types of data affected by the breach	
13	Special categories of data	
14	Did the breached data include personal data related to criminal convictions or offences	
15	Any other type(s) of personal data involved (if relevant)	
16	Actual or approximate number of data records	
17	Actual or approximate number of affected members	
18	Vulnerable individuals affected	
19	Type of consequences	
20	Severity of the risk to the rights and freedoms of affected individuals caused by this breach	

#	Question	Response
21	Details of any technical or organisational data security measures relevant to this breach which were in place prior to the incident occurring	
22	Deficiencies in these measures identified as a result of this breach	
23	Has the breached date been secured/retrieved/restored?	
24	Details of any measures put in place in order to mitigate the impact of this personal data breach on the rights and freedoms of affected data subjects?	
25	Details of any technical or organisational measures which have been put in place following this breach in order to ensure the appropriate security of personal data against such a personal data breach reoccurring	
26	Has the incident been communicated to the affected members?	
27	Any other relevant information?	
28	Incident risk assessment and recommendation	

Trustee Review:	
Reviewed by:	
Risk assessment:	
Decision to report to DPC or not:	
Date:	
GDPR Breaches log no:	

APPENDIX 2: RISK ASSESSMENT

Calculation of the Severity:

In determining the severity of the risk from the Data Breach for the affected Data Subjects, the Data Protection Team must take into account the impact the Data Breach could potentially have on Data Subjects whose data has been exposed.

In assessing this potential impact, the following should be considered:

(a) The circumstances of the Data Breach (CB) including
- the nature of the Data Breach,
- the cause of the Data Breach,

(b) The context of the data processing, (CDP) including
- the type of data exposed,
- mitigating factors in place
- whether the personal data of vulnerable Data Subjects has been exposed. The DPC has defined a vulnerable person as being a child or a person who, by reason of physical or mental incapacity, is unable to act on their own behalf.

(c) The ease of identification (EI) of the Data Subjects involved.

The overall severity (SE) is calculated by the following formula: SE = CB + (CDP x EI). How to evaluate these are set out in detail on the following pages.

The next step is to evaluate the likelihood of the risk (LI).

The final risk score (RS) is to multiply the severity by the likelihood: SE x LI - RS

The result of such equation will allow to determine the severity of the breach; which in accordance with the criteria used by:

	Risk Grade Severity		Action
RS = 0	None	the breach has no impact on Data Subjects	No obligation to report to the Data Protection Commission Or The Data Subject Unless there are other factors
RS <1	Unlikely	the breach is unlikely to have any impact on Data Subjects	
RS <2	Low	the breach is unlikely to have an impact on Data Subjects, or the impact is like to be minimal	
2 ≤ RS < 3	Medium	the breach may have an impact on Data Subjects, but the impact is unlikely to be substantial	
3 ≤ RS < 4	High	the breach may have a considerable impact on affected Data Subjects	Report to the Data Protection Commission And Report to the Data Subject(s)
4 ≤ RS	Very high	The breach may have a critical, extensive or dangerous impact on affected individuals.	

Scoring of the criteria:

Circumstances of the Data Breach (CB):

Circumstances of the Data Breach quantifies the specific circumstances that may be present or not in a particular situation. The elements that are considered the nature and cause of the Breach and any malicious intent detected.

Circumstances	Examples	Score
Confidentiality – no evidence that illegal processing has occurred **Integrity** – data altered but without any identified incorrect or illegal use **Availability** – data recovered without any difficulty	• Device lost/stolen encrypted • Data entry mistake • Database records are wrongly updated or corrupted but are recovered before any processing occurs • Unauthorised disclosure (internal) • File/database overwritten but recoverable from backup • Documentation filed in another person's file	**0**
Confidentiality – data disposed to a number of known recipients **Integrity** – data altered and possible used in an incorrect or illegal way but with possibility to recover **Availability** – data temporarily unavailable	• Email/letter sent to unintended recipients • Inappropriate disposal of paper • Network security breach (staff) • Unauthorised disclosure (external) • File server offline • File/database corrupted but can be reconstructed • File lost/corrupted but can be recovered from the Data Subject	**+0.25**
Confidentiality – data disposed to a number of unknown recipients **Integrity** – data altered and possible used in an incorrect or illegal way without possibility to recover **Availability** – data cannot be recovered M**alicious Intent** – breach was due to an intentional action	• Device lost/stolen unencrypted • Paper lost/stolen • Hacking • Malware • Phishing • Unintended publishing online • Network security compromise • Website security breach	**+0.5**

The context of the data processing (CDP):

In order to define the score for the context of the data processing, the Data Protection Team should follow the next steps:

Step 1: Definition and classification of the types of Personal Data

(a) Define the types of the Personal Data involved in the Data Breach.

(b) Classify the Personal Data in at least one of the four categories: simple, behavioural, financial, and special data (these categories are explained in detail in the table below). In this way a preliminary basic CDP score is obtained.

The list of data types described under the four categories is not exhaustive; however most data involved in real cases can be matched to at least one of the categories. Login credentials are not considered as a specific data category and should be handled based on the type of data processed by the systems where they provide access to.

Data Processing Context		Score
Simple data e.g. name, contact, family life, educational data, professional data etc	**Preliminary basic score**: when the breach involves ''simple data'' and the controller is not aware of any aggravating factors.	1
	Volume of data allows profiling of the Data Subjects	2
	Data could lead to assumptions about Data Subject's health status, sexual preferences, political or religious beliefs	3
	Data relates to vulnerable groups (e.g., children) or the Personal Data impacts safety or physical/psychological conditions	4
Behavioural data e.g. address, location, personal preferences and habits	**Preliminary basic score**:	2
	If nature of data does not provide any substantial insight to the Data Subject's behavioural information or can be collected easily through publicly available sources	1
	If volume of Personal Data or knowledge of the controller could lead to a profile of the person being created, exposing detailed information about his/her everyday life and habits	3
	If a profile based on the Data Subject's sensitive data can be created	4
Financial data e.g. salary, benefits, financial transactions, bank statements, investments, credit cards, invoices, PPSN or other national tax identifier	**Preliminary basic score**:	3
	If nature of data does not provide any substantial insight to the Data Subject's financial information e.g. the person is a customer/member	1
	If nature of data does not provide specific insight into the Data Subject's financial status/situation e.g. bank account numbers, PPSN	2
	If nature or volume of data would allow fraud or detailed social/financial profile to be created e.g. credit card details	4
Special categories of data e.g. any type of special categories of Personal Data, race or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, sex life data, health data, genetic data or biometric data	**Preliminary basic score**:	4
	If nature of data does not reveal any substantial insight to the Data Subject's behavioural information or any data can be collected easily through publicly available sources. If data has been shared with a party with a duty of confidentiality e.g. doctor, dentist, pharmacist, Gardai, accountant, lawyer, actuary or similar.	1
	If nature of data can only lead to general assumptions	2

Step 2: Adjustment by contextual factors related to the data processing:

(a) Assess the occurrence of certain factors that could increase or decrease the basic score (data volume, special characteristics of the controllers or the Data Subjects, invalidity/inaccuracy of data, public availability (before the breach), nature of data).

(b) In case such factors exist, accordingly increase/decrease the basic score. The table provides the adjustment scales per category of data, together with example cases that could lead to lower/higher scores.

Where more than one category of Personal Data has to be assessed, the value to be used for the overall calculation of the severity will be the highest score reached.

The ease of identification (EI):

Ease of identification (EI) evaluates how easy it will be for a party who has access to the set of data to match them to a certain person.

Score	Circumstances	Examples
0.25	Negligible	Full name - Many people have the same full name ID Card/passport/social security number – no other information was provided Telephone number/home address – no country public register Email address – does not reveal any other data e.g. name not used as primary address on internet sites Picture – unclear or vague Unique ID/Aliases – cannot be linked to other Personal Data
0.5	Limited	Full name - Few or no people have the same full name in a country Telephone number/home address – no city public register Picture – unclear or vague but has other information that may allow identification
0.75	Significant	Full name – few or no people share the name in a city ID Card/passport/social security number – identifier reveals identification information e.g. date of birth and other data i.e. email address Email address – primary address on internet sites Picture – clear but no other identification information Unique ID/Aliases – reveals some data about the Data Subject e.g. name and is linked to other data e.g. email
1.0	Maximum	Full name – identifiable from their name ID Card/passport/social security number – information from the reference database is also available e.g. full name and photo Telephone number/home address – number is included in publicly available register Email address – reveals Data Subject's name and is used as primary address on internet sites e.g. john.murphy@xyz.com Picture – clear and linked to other identification information e.g. home address Unique ID/Aliases – ID/alias reveals Data Subject's full name

The Likelihood:

Likelihood	Description	Example	Level
IMPOSSIBLE	We have evidence which assures us that individuals will not be impacted	• there was no data compromised • any systems impacted were restored with no impact to individuals • data at risk was encrypted and keys are still in our control • data was otherwise unintelligible	0
UNLIKELY	We have some evidence that leads us to believe that individuals will not be impacted	• data was accidentally disclosed and we have evidence of its disposal or retrieval • data (or device) was lost and basic protections in place (e.g password) • only simple data and the number of individuals and/or records impacted was low	0.25
POSSIBLE	We have no evidence to assure us that individuals will not be impacted	• this was a denial of service attack that has stopped • data was exfiltrated but would be complex to reconstruct to be meaningful • data was compromised but we have recovered the data • this was a ransomware attack and system availability has been restored	0.5
LIKELY	We assume that individuals may be impacted	• we have been threatened with data exposures • we cannot evidence that the data is secure or destroyed • we have not recovered the data and this was a malicious attack	0.75
CERTAIN	We know that individuals will be impacted	• we have evidence of data in the wild • or we have reports from data subjects or third parties of data being used • or we have a credible threat or evidence of future exposure	1

Example data breach risk assessment

Circumstances – Irish Life sent a spreadsheet of 16 member's data to another client of theirs. The file was password protected but Irish Life shared the password. The file contained PPSN, name and surname. The client payroll contact realised that it was the wrong file on opening. The contact confirmed that they had deleted the file

CB = Confidentiality breach – A file containing the data or 16 members was shared with a third party, a known client of Irish Life's. Data disposed to a known recipient = +0.25

CDP = the file contained the name, surname & ppsn for 16 patients. As it contains PPSN, this is Financial Data. The preliminary basic score is = +3. However, reduced to 2 as per the CDP guidelines "If nature of data does not provide specific insights". Therefore the score can be reduced to 2.

EI = includes PPSN = maximum = 1

Score CB + CDP x EI
= 0.25 + (2 X 1) = 2.25

Severity = 2.25 = Medium = Medium risk

Other factors =
Recipient realised immediately and confirmed deletion.

Conclusion = the scoring indicates that this is medium risk and there is mitigation in that the recipient confirmed deletion. Therefore no requirement to report to the DPC. No requirement to inform data subjects.

End