An Roinn Leanaí, Comhionannais, Míchumais, Lánpháirtíochta agus Óige
Department of Children, Equality, Disability, Integration and Youth

Department of Children, Equality, Disability, Integration and Youth

Personal Data Breach Management Policy

The purpose of this policy is to provide a clear outline of the procedures to be followed by all staff of the Department, and its processors, in the event of an actual or suspected personal data breach.

June 2019

Contents

Personal Data Breach Management Policy

1. Introduction

1.1. The Department of Children, Equality, Disability, Integration and Youth ('the Department') is committed to protecting the rights and privacy of individuals (also known as "data subjects") in accordance with both European Union (the General Data Protection Regulation [GDPR]) and Irish data protection legislation. We place high importance on the correct, lawful and fair handling of all personal data, respecting the legal rights, privacy and trust of all individuals with whom we deal.

1.2. A personal data breach is taken to mean a security incident leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

1.3. While we are committed to implementing technical and organisational measures to ensure the personal data we hold is secure, it is important that, in the event of a data breach, we have a responsive breach management plan in place.

1.4. Our main focus, in the event of a data breach, is to protect any affected individuals and to limit the impact of the breach.

1.5. This policy is a means to assist the Department in its role as a data controller.

2. Scope

2.1. This policy outlines the procedures that should be followed by all staff of the Department in the event of any incident comprising an actual or suspected personal data breach. It also identifies the responsibilities of processors – those who process personal data on our behalf – in the event of a breach.

2.2. It is important to note that not every information security incident is a personal data breach, **but** that every personal data breach is an information security incident. The circumstances of a security breach must be immediately ascertained. ***Ask yourself – has personal data been affected in any way?***

3. How personal data breaches can occur

3.1 The following are some examples of common personal data breaches:

- Human error;
- Loss or theft of paper documents;
- Loss or theft of equipment on which personal data is saved;
- Intentional or unintentional disclosure of confidential data to an unauthorised third party;
- Inappropriate access controls resulting in unauthorised access to confidential information;

- Hacking incidents;
- Emails containing personal or sensitive personal data being sent to the incorrect recipient(s);
- Personal data being left unattended in accessible areas;
- Premises breach (break-in, flood, fire, etc.);
- Inappropriate disposal of personal data (e.g. unsecured recycling).

3.2 Given that human error can be a significant contributing factor, staff (of the Department and our processors) need to exercise due caution when they are dealing with personal data.

3.3 The GDPR imposes a duty on the Department to report a data breach to the Data Protection Commission (DPC) within 72 hours of becoming aware of the breach. If the breach is likely to result in a high risk to the rights and freedoms of data subjects, the Department is also obliged to notify the affected individuals without undue delay.

4. Risks associated with a data breach

4.1 The risks to the individual associated with a data breach include:

- loss of control over personal data or identity;
- damage, interference, loss or distress to health or wellbeing;
- identity theft and fraud;
- impact on financial or economic status or circumstances;
- embarrassment or other negative outcomes, including reputational damage;
- loss of confidentiality of personal data protected by professional secrecy.

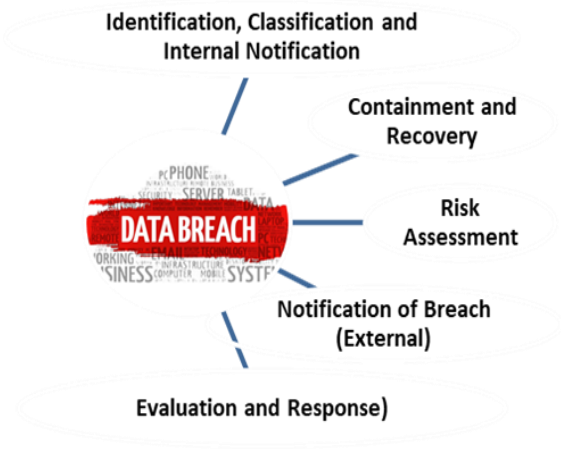
4.2 The risks to the Department include:

- Investigation, administrative fines, prosecution or other sanctions imposed by the DPC;
- Reputational damage as a result of the breach;
- Legal costs and/or compensation awards where claims are taken by an individual;
- Loss of public confidence in the services provided by the Department;
- Technical or organisational costs associated with correcting the circumstances that gave rise to the breach (e.g. amending or replacing systems, ICT fixes, review of scheme design or operation);
- Employee disciplinary action in the case of a wilful act resulting in a breach;

5. Personal Data Breach Management Plan

The Department's Breach Management Plan consists of five steps:

1. Identification, Classification and Internal Notification
2. Containment and Recovery
3. Risk Assessment
4. Notification of Breach (External)
5. Evaluation and Response



Step 1: Identification, Classification and Internal Notification

How might you know that a breach or potential breach has taken place?

- *An email is returned to you, indicating that the recipient details are incorrect.*
- *An individual contacts you to say that they received correspondence/email that was meant for someone else.*
- *A customer/client did not receive something they were due to receive (e.g. financial supports).*
- *An individual contacts the Department to advise they have been contacted by someone who has indicated they received the individual's personal data from the Department or one of its processors.*
- *One of the Department's data processors informs you of a breach.*
- *Official laptop/tablet/phone/papers have been lost or mislaid.*

Breach Classification:

Breaches can be classified according to the following three information security principles:

Confidentiality breach	where there is an unauthorised or accidental disclosure of, or access to, personal data (e.g. by an entity not entitled to such access)
Integrity breach	where there is an unauthorised or accidental alteration of personal data, (e.g. an inappropriate modification of personal data)
Availability breach	where there is an accidental or unauthorised loss of access to, or destruction of, personal data (e.g. loss of control of access to personal data, or inappropriate deletion of personal data)

Responding to notification or identification

Given the very strict breach reporting timelines, a staff member who discovers that a suspected or actual breach has occurred should report this to their Head of Unit (PO equivalent) **immediately**. The Head of Unit will decide which staff member to designate to looking after the breach notification.

Person receiving/identifying a potential or real breach	Report immediately to the Head of Unit (PO)
Head of Unit	Nominate a member of staff to look after the breach report: • formal reporting • liaison with the DPO, and • liaison with the processor (where required).
Nominated officer	• Completes Internal Personal Data Breach Form[1] (including an assessment of the level of risk associated with the breach) • Liaises with the data processor (where required). Ensures the processor completes and submits an Internal Personal Data Breach Form. Agrees the risk level with the processor (amending it if necessary). • Advises the DPO of situation and submits Internal Personal Data Breach Form

Step 2: Containment and Recovery

Incident Response Team

Depending on the extent and assessed level of risk of the data breach, the DPO may recommend that an Incident Response Team (IRT) be convened ***immediately*** (note - the 72 hour notification period is inclusive of weekend days) to assist with further investigation of, and response to the breach.

The IRT is a group of people who, given the risk associated with the data breach, prepare for and respond to the breach in order to protect the rights of the data subject and ensure the Department's response is adequate and timely. The IRT will consist of some or all of the following representatives:

i. Relevant Head of Unit and any other relevant member of senior management (to the level of Management Board if required);
ii. Data Protection Officer;
iii. Communications/Press Officer (or representative);
iv. Head of ICT (or representative);

[1] All breaches, regardless of whether they are ultimately notified to the DPC or to affected individuals, should be recorded (by the reporting Unit) on the Internal form. The Department - through the Data Protection Unit - has record-keeping obligations in respect of all breaches, including those where it is determined there is no risk to affected individuals following a breach. A 'Personal Data Breach Report' is maintained, which is completed using information from the Internal forms. In cases of no risk, the Breach Report must include the details, the means for deciding there was no risk, who decided there was no risk and the risk rating that was recorded. The Data Protection Commission can request sight of records at any time.

v. Representatives of the processor (*if the breach is at processor level*);
vi. Head of Legal (or representative);

In addition to the above and depending on the complexity of the breach, third party assistance may be required to establish the full extent of, and help contain the breach. The IRT will be chaired by the most senior member of staff attending for the particular incident and will, among other things:

- Decide on actions required to contain the breach (e.g. isolating/closing a compromised section of the network, finding a lost piece of equipment, changing access codes on doors, etc.);
- Decide on actions required to recover any losses and limit the damage the breach can cause (e.g. physical recovery of equipment/records, the use of back-up to restore lost/damaged data);
- Decide on actions required to report the breach to the Minister and Management Board;
- Identify whether it is appropriate to inform the Data Protection Commission;
- Identify if it is appropriate to notify affected individuals immediately (e.g. where it has been determined that there is a high level of risk of serious harm to individuals);
- Identify the best methodology to contact individuals affected (e.g. the number of individuals may warrant the issue of a press release, rather than individual letters);
- Identify if it is appropriate to inform An Garda Síochána (e.g. in cases involving theft or other suspected criminal activity).

It is essential that there is a full understanding by relevant staff of the requirement to participate in an IRT, in the context of the very strict timeframes around reporting the data breach to the DPC. All papers relating to the IRT deliberations will be retained by the DCEDIY DPO.

Step 3: Risk Assessment

The assessment of the level of risk involved will be reviewed by the DPO in consultation with the Head of Unit, and a final risk assessment will be formally agreed. This will inform our reporting obligations.

When assessing the risk caused by the breach, primary consideration should be given to the extent of the damage that the breach could potentially cause to individual(s). To inform the assessment, the following should be considered:

- Type and cause of the breach;
- Nature of personal data involved;
- Sensitivity of the data;
- What the data could convey about the individual to a third party;
- Any special characteristics of the individual (e.g. child, vulnerable adult, etc.) or the controller (e.g. treatment facility, hospital, etc.);
- Any security mechanisms in place (e.g. password, encryption);
- Whether the Department is using a trusted recipient (e.g. an organisation with whom it has on-going contractual arrangements or a long-standing relationship).

All personal data breaches must be reported to the DPC, unless it has been determined that there is ***no risk*** associated with the breach.

If the personal data breach is deemed ***likely to result in a high risk*** to the rights and freedoms of individuals, the breach should be reported to the individuals affected.

Some further guidance on reporting requirements can be found in **Appendix 2**.

Step 4: Notification of Breach (External)

Notification to the DPC

All personal data breaches must be reported to the DPC, unless it has been assessed that there is ***no risk*** associated with the breach

The Department must notify the DPC of the personal data breach without undue delay, but not later than 72 hours after becoming aware of it, unless the breach is unlikely to result in a risk to the rights and freedoms of individuals. The Department will be regarded as having become 'aware' when it has a reasonable degree of certainty that a security incident has occurred, leading to personal data being compromised.

In many cases it will be evident that a breach has taken place, however if there is a degree of uncertainty the Department can undertake a short period of investigation in order to establish whether or not a breach has in fact occurred. It is presumed during this period that that Department is not considered 'aware'. Once the breach is verified, we are 'aware' of it.

The Data Protection Officer is usually responsible for notifying the DPC within the specified time frame.

Notification to third parties

Based on the circumstances and the evaluation of the risk, it may be necessary to also notify a third party such as An Garda Síochána at this stage. This may need to be discussed at more senior levels of management (see establishment of Incident Response Team above).

Notification to Individuals

Where a personal data breach is likely to result in a ***high risk*** to the rights and freedom of individuals, the Department ***must notify*** such individuals of the data breach without undue delay and in a clear and transparent manner.

Notification to individuals is subject to some limited exceptions:

- The Department has protected the data such that it would be unintelligible to any person not authorised to access it (e.g. encryption).
- Subsequent measures taken by the Department following the breach have ensured that the risk to the rights and freedom of the data subject is no longer likely to materialise.
- It would involve a disproportionate effort to contact each individual and hence a public communication or similar measure is adopted in order to notify those involved.

In circumstances where a breach must be notified to individuals, it is reasonable that we concentrate on those individuals in the immediate aftermath of the incident (e.g. to notify them to change their passwords). The DPC can be contacted in 72 hours, whereas immediate notification to individuals can have a positive impact on mitigating the risks to them. **However, no individuals should be notified in advance of the reporting of the breach to the DPO in the Department.**

While there is no statutory obligation on the Department to notify individuals of a data breach where there is no assessed high risk involved, each case should be considered on its own merit as to whether a notification to any individual should issue.

Step 5: Evaluation and Response

Following a personal data breach, a review of the circumstances surrounding the breach and the actions taken will be carried out by the DPO. The following should be considered:

- How the breach occurred and what action is required to reduce the risk of similar future breaches and minimise their impact?
- Were the policies and procedures in place in respect of data protection and breach management effective?
- Were employees aware of their responsibilities in respect of data protection and breach identification & management?
- What lessons were learned from the incident?
- Whether the Risk Register needs to be revisited and amended?

Where it is identified that significant changes to policy or operations are required, these changes must be approved at Management Board level and notice of changes will be issued to relevant staff.

A breach should be monitored to ensure that the circumstances do not escalate, which may result in the breach becoming reportable where initially it may not have been. It is important to note that while some impacts may have already happened at the time the breach is detected, some may only become material at a later time (e.g. if credentials are stolen, some may already have been used, others may be used later).

6. Responsibility of staff

6.1 Staff should familiarise themselves with this policy and pay particular attention to what constitutes a breach of personal data and the formal Departmental response required.

6.3 Staff found to have performed an intentional act resulting in a breach of personal data may be subject to disciplinary procedures under the Civil Service Disciplinary Code.

7. Responsibility of data processors

7.1 The GDPR imposes a requirement on processors to notify the controller (DCEDIY) without undue delay after becoming aware of a personal data breach, at which point they should provide all the relevant details to the relevant Departmental line Unit. Detailed engagement with the line

Unit will be required, and the processor must complete the requisite Internal Personal Data Breach form. At all times the processor's own DPO should be kept informed of developments.

7.2 **The obligation to report a data breach to the DPC usually rests with the controller**. However, some contractual arrangements could include Departmental authorisation to the processor to make notifications ***directly*** to the DPC. Such notifications should be made by staff designated by the processor for this purpose. In such circumstances the processor remains obliged to keep the relevant Departmental line Unit informed, and to complete the Incident Form. The line Unit should in turn keep the Data Protection Unit informed, which will allow it to ensure its Incident Log is up to date.

7.3 The particulars of the breach response and notification obligations of each processor should be set out in the relevant contract with the Department.

Note: A processor's obligations to the Department are only in respect of personal data that is ultimately under the Department's control, and processed as part of the contract. It is often the case that a data processor is also a data controller in its own right (e.g. in respect of the personal data of its employees), and subject to all the obligations - including breach reporting obligations where a breach occurs - that apply to that controller role.

8. Review and Update

This policy may be reviewed from time to time in order to take into account any changes in the organisational structure of the Department, business practices and/or changes in legislation.

Appendix 1

Internal Personal Data Breach Form

You should use this form if you are:

a. A member of staff of the Department of Children, Equality, Disability, Integration and Youth; or
b. A processor who processes data on behalf of the Department.

This form replicates the content from the Data Protection Commission's Breach Notification form. It is an important element in recording personal data breaches by DCEDIY and its processors. It should be completed to report a personal data breach that has occurred, or you think may have occurred in the Department (or in a processor used by the Department), irrespective of any additional reporting requirements.

A personal data breach occurs where the data is accessed, disclosed, altered, lost or destroyed in contravention of the Department's obligation to keep personal data in its possession safe and secure. This is an obligation which extends to processors used by the Department.

NB - When completing this form, please do not include any of the actual personal data involved in the breach. For example, do not include the names of individuals impacted by the breach.

You should notify your Head of Unit of the actual or suspected breach immediately upon discovery of the breach, and complete this form. Certain personal data breaches are required to be notified to the Data Protection Commission within 72 hours of becoming aware of the breach, therefore it is important that actual or suspected breaches are reported immediately.

About You (Controller) *(This part should be completed by the person designated by the Head of DCEDIY Unit to deal with the data breach, including where the breach has occurred in a processor)*	
Full Name	
DCEDIY Role	
Phone number	
Email address	
About You (Processor) *(This part should be completed by the person designated by the Head of Processor Unit to deal with the data breach)*	
Full Name	
Name of Organisation	
Role	
Phone number	
Email address	

Part One - Introductory Questions	
Q1 A. Are you notifying a personal data breach?	☐a) Yes, I am notifying a personal data breach to the DPC as a data controller / on behalf of a data controller. ☐b) Yes, I am notifying a personal data breach to the DPC as a data processor / on behalf of a data processor. ☐c) No, I am an individual concerned about the processing of my personal data or the personal data of another.
Q1 B. Type of notification	☐a) This is a new notification ☐b) I have already notified a personal data breach and I wish to provide an update
Q1 C. Is the personal data breach likely to result in a risk to the rights and freedoms of individuals?	☐Yes ☐No
Q1 D. Does this personal data breach notification relate to the processing of personal data for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, within the meaning of section 70 of the Data Protection Act 2018?	☐Yes ☐No
Are you completing this form as:	☐An employee of the Department ☐An employee of a data processor.
If you are a data processor, do you have an agreement with the Department which allows you to report a breach directly to the DPC?	☐Yes ☐No
If you are a processor, have you notified the Department of the breach in advance of completing this form?	☐Yes ☐No
If you have not notified the Department immediately upon becoming aware of the breach, please outline the reasons why?	

Part Two – Your Supervisory Authority	
Q2. Are you notifying a breach that concerns cross-border processing of personal data?	☐a) I am notifying a personal data breach which only affects data subjects in Ireland and which only relates to my organisation's activities in Ireland. ☐b) I am notifying a personal data breach on behalf of an organisation which does not have an establishment in the European Union. ☐c) I am notifying a personal data breach which affects data subjects in more than one EU/EEA state or relates to data processing activities in more than one EU/EEA state
	If Q2(a) selected finish this section *If Q2(b) selected continue to Q3(a)* *If Q2(c) selected continue to Q4*
Q3 A. Please confirm if the organisation making this notification has designated in writing a representative in the EU as per Article 27 of the GDPR	☐Yes ☐No
	If Q3a (YES) selected continue to Q3b *If Q3a (NO) selected show NEXT button*
Q3 B. Please confirm the name, contact details and geographical location of the EU/EEA representative	
Q4. You are notifying a breach that concerns cross-border processing of personal data. Which of the following two options applies?	☐a) I am notifying a breach which concerns the processing of personal data which takes place in the context of the activities of establishments of a controller or a processor in more than one EU/EEA state ☐b) I am notifying a breach which concerns the processing of personal data which takes place in the context of the activities of a single establishment of a controller or a processor in the Union but which substantially affects or is likely to substantially affect individuals in more than one EU/EEA state.
	If Q4 (a) selected continue to Q5,6 and 9 *If Q4 (b) selected continue to Q7,8 and 9*
Q5. Please provide details of all of your establishments in the EU/EEA relating to this incident	

Q6. If data subjects in other EU/EEA States are affected, please indicate the EU/EEA states concerned	
Q7. Please indicate the EU Member States in which individuals are substantially affected or likely to be substantially affected	
Q8. Please indicate how individuals in other EU/EEA states are substantially affected or are likely to be substantially affected by the personal data breach	
Q9. As you are notifying a cross-border breach, is the Data Protection Commission competent to deal with your notification?	☐a) I am notifying on behalf of a data controller or processor whose main or single establishment in the EU/EEA is in Ireland ☐b) I have notified another EU/EEA data protection supervisory authority as my lead supervisory authority, but I also wish to inform the Data Protection Commission ☐c) Neither of the above
	If Q9 (a) selected continue to Q10 and finish this section *If Q9 (b) selected, finish this section* *If Q9 (c) selected, finish this section*
Q10 Please provide an explanation of why you consider that your organisation's main or single establishment in the EU/EEA is in Ireland, including whether this establishment is in your organisation's central administration/headquarters in the EU/EEA and is the place where decisions on the purposes and means of processing of personal data are taken	

Part Three – Details of the Data Controller	
Q11. Name of organisation	
Q12. Address of organisation	
Q13. Please provide the name and location of any other EU/EEA establishments that your organisation has	
Q14. Which sector does your organisation operate in?	☐a) public sector ☐b) private sector ☐c) voluntary sector ☐d) charity
Q15. Sub-sector **Explanatory note: for an explanation of the industry sectors, please see page 325+ here** (Statistical classification of economic activities in the European Community)	☐Agriculture ☐Mining and quarrying ☐Manufacturing ☐Electricity, gas, steam and air conditioning supply ☐Water supply, sewerage, waste management and remediation activities ☐Construction ☐Wholesale and retail trade repair of motor vehicles and motorcycles ☐Transportation and storage ☐Accommodation and food service activities ☐Information and communication ☐Insurance activities ☐Financial activities ☐Real estate activities ☐Professional, scientific and technical activities ☐Administrative and support service activities ☐Public administration and defence; compulsory social security ☐Education ☐Human health and social work activities ☐Arts, entertainment and recreation ☐Other service activities ☐Activities of households as employers; undifferentiated goods and services producing activities of households for own use ☐Activities of extraterritorial organisations and bodies
Q16. Internal reference number assigned by your organisation to this incident	

Part Four – Details of the Data Processor	
Q17. Name of processor organisation	
Q18. Address of processor organisation	
Q19 A. Name of processor contact person	
Q19 B. Email address of process contact person	

Part Five – Contact Point	
Q19_2. Are you the DPO?	☐a) Yes ☐b) No
	If Q19_2(a) selected continue to Q20-22 only and finish this section *If Q19_2(b) selected continue to Q20-28 and finish this section*
Q20. DPO Name	
Q21. DPO Email address	
Q22. DPO Phone number	
Q23. Name of person notifying	
Q24. Email address of person notifying	
Q25. Phone number of person notifying	
Q26. Function	
Q27. I am contacting the DPC as a processor that has an agreement from a data controller to report a breach on its behalf	☐a) Yes ☐b) No
Q28. I am the designated contact in relation to this personal data breach	☐a) Yes ☐b) No – Contact the DPO

Part Six – Timeline of the incident	
Q29. Do you know the date on which the breach initially occurred?	☐Yes ☐No
Q30. Actual or approximate date on which the breach occurred	
Q31. Is the breach on-going?	
Q32. Please enter the date on which the breach ended	
Q33. When did you become aware of the breach?	
Q34. If you are notifying the DPC of a personal data breach more than 72 hours after having becoming aware of it, please provide reasons for that delay	
Q35. How was the data controller made aware of the breach?	

Part Seven – Type of Breach	
Q36. Please specify the type of breach	☐a) Confidentiality breach (i.e. unauthorised disclosure of or access to personal data) ☐b) Integrity breach (i.e. alteration of data) ☐c) Availability breach (i.e. loss or destruction of data)
Q37. Please specify the nature of the breach	☐i) Accidental or deliberate loss or destruction of personal data ☐ii) Loss or theft of an encrypted device ☐iii) Loss or theft of an unencrypted device ☐iv) Loss or theft of paper ☐v) Unauthorised disclosure of/access to personal data – CCTV images ☐vi) Unauthorised disclosure of/access to personal data – email correspondence ☐vii) Unauthorised disclosure of/access to personal data – online portal or account ☐viii) Unauthorised disclosure of/access to personal data – messaging platform ☐ix) Unauthorised disclosure of/access to personal data – social media ☐x) Unauthorised disclosure of/access to personal data – postal correspondence ☐xi) Unauthorised access to personal data – electronic devices/assets ☐xii) Unauthorised access to personal data – paper files/documents/records ☐xiii) Verbal/in person disclosure of personal data ☐xiv) e-Waste (personal data held on an obsolete device) ☐xv) Hacking (e.g. credential stuffing, malware, DDoS, ransomware etc.) ☐xvi) Social engineering (e.g. phishing, spear phishing, smishing or vishing) ☐xvii) Inappropriate disposal of equipment/assets ☐xviii) Inappropriate disposal of paper ☐xix) Deliberate unauthorised alteration of personal data ☐xx) Unintentional alteration of personal data ☐xxi) Deliberate online publication ☐xxii) Unintentional online publication ☐xxiii)Processing error ☐xxiv) System maintenance ☐xxv) Other

Q38. Please describe how the breach occurred	
Q39. Please specify the cause of the breach	☐i) Employee error or omission ☐ii) Employee intentional act ☐iii) Contractor error or omission ☐iv) Contractor intentional act ☐v) External intentional act ☐vi) External unintentional act ☐vii) Former employee error or omission ☐viii) Former employee intentional act ☐ix) Unknown

Part Eight – About the breached data	
Q40. Types of data affected by the breach	☐i) Name, surname and/or date of birth ☐ii) Contact details (phone number, email address, address, postal code/eircode) ☐iii) Official identification data (PPS number/national identification number/passport number) ☐iv) Identification or access information (username, password, reference number) ☐v) Social media profile ☐vi) Economic and financial data ☐vii) Official documents (orginials) ☐viii) Official documents (copies) ☐ix) Location data, such as GPS location information, but excluding addresses/contact details ☐x) Photo, video or audio recordings or records of such ☐xi) Information relating to personal activities or family life ☐xii) Information relating to professional activities ☐xiii) Communication data ☐xii) Pseudonymised data ☐xii) Unknown
Q41. Special categories of data	☐i) Data revealing racial or ethnic origin ☐ii) Data revealing political opinions ☐iii) Data revealing religious or philosophical beliefs ☐iv) Data revealing trade union membership ☐v) Data concerning an individual's sex-life or sexual orientation ☐vi) Data concerning health ☐vii) Genetic or biometric data ☐viii) No special category data has been breached
Q42. Did the breached data include personal data related to criminal convictions or offences	☐Yes ☐No
Q43. Please describe any other type(s) of personal data involved (if relevant)	
Q44. Actual or approximate number of data records	☐i) 1-10 ☐ii) 11-100 ☐iii) 101-1000 ☐iv) 1001-10000 ☐v) 10001-100000 ☐vi) 100001-1000000 ☐viii) 1000000 or greater ☐viii) Actual or approximate number unknown at this time

Part Nine – About the data subjects	
Q45. Actual or approximate number of affected data subjects	☐i) 1-10 ☐ii) 11-100 ☐iii) 101-1000 ☐iv) 1001-10000 ☐v) 10001-100000 ☐vi) 100001-1000000 ☐viii) 1000000 or greater ☐viii) Actual or approximate number unknown at this time
Q46. Were vulnerable individuals affected?	☐Yes ☐No ☐Unknown

Part Ten – Consequences of the breach	
Q47. Type of consequence	☐i) Loss of control over their personal data ☐ii) Limitation of their rights ☐iii) Discrimination ☐iv) Identity theft ☐v) Fraud ☐vi) Financial loss ☐vii) Unauthorised reversal of pseudonymisation ☐viii) Damage to reputation ☐ix) Loss of confidentiality of personal data protected by professional secrecy ☐x) Other
Q48. How severe is the risk to the rights and freedoms of affected individuals caused by this breach? ("Self-declaration?")	☐i) No Risk ☐ii) Low risk ☐iii) Medium risk ☐iv) High risk ☐iv) Severe risk

Part Eleven – Action taken	
Q49. Please provide details of any technical or organisational data security measures relevant to this breach which were in place prior to the incident occurring	
[Identify what technical / organisational measures were in place prior to the breach – such as ICT arrangements, clean desk policy, etc. You may find these listed on your Unit's Record of Processing Activities (ROPA)]	
Q50. What deficiencies in these measures have you identified as a result of this breach?	
Mitigation measures **Q51. Have you secured/retrieved/restored the breached data?**	☐Yes ☐No
Q52. Please provide details of any measures you have put in place in order to mitigate the impact of this personal data breach on the rights and freedoms of affected data subjects?	
[*These may be identified on your Unit's Risk Register*]	
Q53. Please provide details of any measures which will be put in place in order to mitigate the impact of this personal data breach on the rights and responsibilities of affected data subjects, and the expected implementation date	
Technical and organisational measures put in place following the breach **Q54. Please provide details of any technical or organisational measures which you have put in place following this breach in order to ensure the appropriate security of personal data against such a personal data breach reoccurring**	

Part Twelve – Communication to data subjects ***(NB Notification only required in High/Severe risk cases)***	
Q55. Have you communicated the incident to affected data subjects?	☐a) The incident has been communicated to affected data subjects ☐b) The incident has not yet been communicated to affected data subjects, but this communication is planned. ☐c) The incident has not/will not be communicated to affected data subjects (choose reasons)
	If Q55(a) selected continue to Q56 and Q57 and Q68 *If Q55 (b) selected continue to Q59* *If Q55 (c) selected continue to Q60*
Q56. What medium was used to communicate the incident to affected data subjects?	☐1) Letter ☐2) Email ☐3) Telephone call ☐4) In person ☐5) Other
Q57. Please describe the content of the communication to data subjects, including advice given to data subjects to mitigate any adverse consequences of the personal data breach	
Q58. If your communication that has been was in the form of the public communication, please explain why it would involve disproportionate effort to notify affected data subjects and provide a link to the public communication.	
Q59. When will affected data subjects be notified?	

Q60. Please outline your reasons for not communication the incident to data subjects	☐1) The personal data breach is not likely to result in a high risk to the rights and freedoms of individuals ☐2) The data controller has implemented appropriate technical and organisation protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the data unintelligible to any person who is not authorised to access it, such as encryption ☐3) The data controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects is no longer likely to materialise ☐4) Other

Part Thirteen – Declaration		
Reporting Officer		
Print Name	**Signature**	**Date**
Head of Division		
Print Name	**Signature**	**Date**
Data Protection Officer		
Print Name	**Signature**	**Date**

Breach Notification Form Guidance

Where do I send this form?
Send your completed form to DPOContact@equality.gov.ie

What do I include in the email subject line?

- **For new breach notifications** – 'new', divisional name, risk rating (e.g. 'New Breach Notification, Early Years, High Risk)
- **For updates to an existing notification** – 'updated breach notification, divisional name, reference number [if one has been provided] (e.g. 'Updated Breach Notification, Early Years, [reference no.])

Further guidance on specific questions provided below:

How serious is the breach for affected individuals?	In determining how serious you consider the breach to be for affected individuals, you should take into account the impact the breach could potentially have on individuals whose data has been exposed. In assessing this potential impact you should consider the nature of the breach, the cause of the breach, the type of data exposed, mitigating factors in place and whether the personal data of vulnerable individuals has been exposed. The levels of risk are further defined below: • **Low:** The breach is unlikely to have an impact on individuals, or the impact is likely to be minimal. • **Medium**: The breach may have an impact on individuals, but the impact is unlikely to be substantial. • **High:** The breach may have a considerable impact on affected individuals • **Severe:** The breach may have a critical, extensive or dangerous impact on affected individuals. Further guidance is available in the DPC Guidance Note entitled 'A Practical Guide to Personal Data Breach Notifications under the GDPR' (Page 8 – Assessing Risk)
Were vulnerable individuals affected?	A vulnerable individual is a child or a person who, by reason of physical or mental incapacity, is unable to act on their own behalf.
Does the breach involve personal data maintained for the prevention, detection, investigation, prosecution of criminal offences or the execution of criminal penalties in the State?	The EU Law Enforcement Directive (LED) provides for the free flow of personal data between competent authorities within the EU for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security, and the transfer of such personal data to third countries and international organisations. Personal data processed for the purposes listed above will be subject to the provisions of the LED.

Appendix 2

DCEDIY & PROCESSORS - FURTHER INFORMATION
DATA BREACH REPORTING REQUIREMENTS

Reporting Requirements (subject to determined level of risk):

Level of Risk	Risk Description	Report to… Internally	Report to… Externally
NONE	No impact on individuals.	• Head of Unit (PO level) + • Data Protection Unit [Internal Personal Data Breach form - for records purposes].	• No Requirement
LOW:	The breach is unlikely to have an impact on individuals, or the impact is likely to be minimal.	• Head of Unit (PO level) + • Data Protection Unit [Internal Personal Data Breach form - for records purposes].	• Data Protection Commission [online Breach Notification form]
MEDIUM	The breach may have an impact on individuals, but the impact is unlikely to be Substantial.	• Head of Unit (PO level) + • Data Protection Unit [Internal Personal Data Breach form - for records purposes].	• Data Protection Commission [online Breach Notification form]
HIGH	The breach may have a considerable impact on affected individuals.	• Head of Unit (PO level) + • Asst. Secretary + • Data Protection Unit [Internal Personal Data Breach form - for records purposes].	• Data Protection Commission [online Breach Notification form] + • Affected Individuals/data subjects.
SEVERE	The breach may have a critical, extensive or dangerous impact on affected individuals.	• Head of Unit (PO level) + • Asst. Secretary + • Secretary General + • Data Protection Unit [Internal Personal Data Breach form - for records purposes].	• Data Protection Commission [online Breach Notification form] + • Affected Individuals/data subjects.

Useful Contacts

Department of Children, Equality, Disability, Integration and Youth	**Data Protection Commission**
Data Protection Officer, Department of Children, Equality, Disability, Integration and Youth, Block 1 – Miesian Plaza, 50-58 Lower Baggot Street, Dublin 2, D02 XW14.	(i) 21 Fitzwilliam Square Dublin 2 D02 RD28 (ii) Canal House, Station Road Portarlington Co Laois R32 AP23 www.dataprotection.ie www.gdprandyou.ie
Phone: +353 1 647 3183 Email: dpocontact@equality.gov.ie Subject Access Requests: sar@equality.gov.ie	Phone: +353 57 868 4800 +353 (0) 761 104 800 Lo-call No: 1890 252 231 Fax: +353 57 868 4757 Email: info@dataprotection.ie

Glossary of Terms

Accountability	**'Accountability'** means being able to demonstrate compliance with GDPR principles. The Department must have appropriate technical and organisational measures in place to be able to demonstrate compliance.
Automated data	**'Automated data'** means any information on computer, or information recorded with the intention of putting it on a computer. It includes not only structured databases but also emails, office documents or CCTV images.
Consent	**'Consent'** is any "freely given, specific, informed and unambiguous" indication of the individual's wishes by which the data subject, either by a statement or by a clear affirmative action, signifies agreement to personal data relating to them being processed for one or more specific purposes. The affirmative action, or a positive opt-in, means that the consent cannot be inferred from silence, pre-ticked boxes, or inactivity. It should also be separate from terms and conditions, and have a simple way to withdraw it. Public authorities and employers will need to pay special attention to ensure that consent is freely given.
Data Controller	'**Data controller'** means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by law.
Data Processor	'**Data Processor'** means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller but does not include an employee of the data controller who processes such data in the course of his/her employment. In the context of the Department, this would include the National Shared Services Office (Peoplepoint & the Payroll Shared Services Centre), Financial Shared Services and Pobal.
Data Protection Officer	A **'Data Protection Officer'** must be appointed in accordance with the regulations where either (a) processing is carried out by a public authority; or (b) the "core activities" of a data controller / data processor either require "the regular and systematic monitoring of data subjects on a large scale," or consist of processing of special categories of data or data about criminal convictions "on a large scale."
Data Subject	A natural person (individual) who is the subject of the personal data.
Joint Controller	Joint Controllers as defined in Article 26 of the GDPR jointly determine the purposes and means of processing of personal data.
Personal Data	**'Personal data'** means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one 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.
Processing	**'Processing'** means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
Profiling	**'Profiling'** is any form of automated processing of personal data intended to evaluate certain personal aspects relating to an individual, or to analyse or predict in particular that person's performance at work, economic situation, location, health, personal preferences, reliability, or behaviour.
Sensitive personal data	See **'Special Categories of Personal Data'**
Special Categories of Personal Data	**'Special categories of data'** include information about an individual's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership (or non-membership), physical or mental health or condition, criminal offences, or related proceedings, and genetic and biometric information — any use of special categories of personal data should be strictly controlled in accordance with this policy.
Subject access	'**Subject access'** is the data subject's right to obtain from the data controller, on request, certain information relating to the processing of his/her personal data.
Supervisory Authority	The **'Supervisory Authority'** is the national body responsible for data protection. The supervisory authority for the Department of Children, Equality, Disability, Integration and Youth is the Data Protection Commission. See www.dataprotection.ie
Territorial scope	**'Territorial scope'** of the GDPR includes the European Economic Area (EEA – all 28 EU member states), Iceland, Lichtenstein, and Norway, and does not include Switzerland.
Third party	A **'third party'** is any natural or legal person, public authority, agency, or any other body other than the data subject, the controller, the processor, and the persons who, under the direct authority of the controller or the processor, are authorized to process the data.
Transfer	The **'transfer'** of personal data to countries outside the EEA or to international organizations is subject to restrictions. Data does not need to be physically transported to be transferred, for example viewing data hosted in another location would amount to a transfer for GDPR purposes.