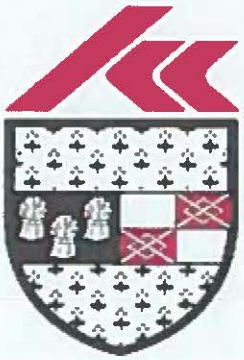

COMHAIRLE CHONTAE CHILL CHAINNIGH

KILKENNY COUNTY COUNCIL

Data Protection Breach Management Policy and Procedures

[Adopted by Management 26th Nov 2019]

Nov 2019

Contents

1.0 INTRODUCTION

Kilkenny County Council is obliged under the Data Protection Acts, 1988 to 2018/GDPR Regulation (the "Data Protection Acts") to keep personal data safe and secure and to respond promptly and appropriately to data security breaches (including reporting such breaches to the Data Protection Commissioner). It is vital to take prompt action in the event of any actual, potential or suspected breaches of data security or confidentiality to avoid the risk of harm to individuals, damage to operational service and severe financial, legal and reputational costs to the Kilkenny County Council.

2.0 PURPOSE

2.1 The purpose of these procedures is to provide a framework for reporting and managing data security breaches affecting personal or sensitive personal data (defined below) held by Kilkenny County Council. These procedures are a supplement to the Local Authority Data Protection Policy which affirms its commitment to protect the privacy rights of individuals in accordance with Data Protection legislation.

2.2 A personal data security breach is any event that has the potential to affect the confidentiality, integrity or availability of personal data held by Kilkenny County Council in any format.

2.3 Personal data security breaches can happen for a number of reasons, including:

- the disclosure of confidential data to unauthorised individuals or 3rd parties
- sharing personal data with the wrong person
- emails containing personal or sensitive information sent in error to the wrong recipient.
- loss or theft of data or equipment on which data is stored;
- loss or theft of paper records;
- confidential information left unlocked in accessible areas;
- breaches of physical security e.g. forcing of doors or windows into secure rooms or filing cabinets containing confidential information
- records altered or deleted without authorisation by the data "owner";
- inappropriate access controls allowing unauthorised use of information;
- leaving IT equipment unattended when logged-in to a user account without locking the screen to stop others accessing information;
- suspected breach of Kilkenny County Council's IT security;
- attempts to gain unauthorised access to computer systems, e.g. hacking;
- viruses or other security attacks on IT equipment systems or networks;

3. WHO DO THESE PROCEDURES APPLY TO?

These procedures apply to all processors of Kilkenny County Council's data, including:

- any person who is employed by the Kilkenny County Council or is engaged by Kilkenny County Council who has access to Kilkenny County Council data in the course of their employment or engagement for administrative, research, processing and/or any other purpose;

- individuals who are not directly employed by Kilkenny County Council, but who are employed as contractors (or subcontractors) and who have access to Kilkenny County Council data in the course of their duties for Kilkenny County Council.

4.0 WHAT TYPES OF DATA DO THESE PROCEDURES APPLY TO?

These procedures apply to:

4.1 all personal data created or received by Kilkenny County Council in any format (including paper records), whether used in the workplace, stored on portable devices and media, transported from the workplace physically or electronically or accessed remotely;

4.2 personal data held on all Kilkenny County Council IT systems managed centrally by the IT Department, and locally by individual / Departments/ Offices / Services;

4.3 any other IT systems on which Kilkenny County Council data is held or processed.

5.0 WHO IS RESPONSIBLE FOR MANAGING PERSONAL DATA SECURITY BREACHES?

5.1 Personal data security breaches are managed by the Data Protection Officer – Eamonn Tyrrell, in conjunction with the relevant Service Manager and Manager of IT Services *(where appropriate)*.

5.2 **In emergency situations**, Kilkenny County Council's Breach Management Team will take over responsibility for managing the incident.

6.0 PROCEDURE FOR REPORTING PERSONAL DATA SECURITY BREACHES

6.1 In the event of a breach of personal data security occurring, it is vital to ensure that it is dealt with immediately and appropriately to minimise the impact of the breach and prevent a recurrence.

6.2 If a processor becomes aware of an actual, potential or suspected breach of personal data security, he/she must report the incident to their Senior Supervisor /Head of Department/Director of Services immediately.

6.3 The Line Manager /Head of Department must then:

6.3.1 Report the incident immediately to the Data Protection Officer:
Eamonn Tyrrell, Corporate Section, Kilkenny County Council, County Hall, John Street, Kilkenny.

6.3.2 Complete the attached Data Security Breach Report Form and email it to dataprotection@kilkennycoco.ie as soon as possible.

This will enable all the relevant details of the incident to be recorded consistently and communicated on a need-to-know basis to relevant staff so that prompt and appropriate action can be taken to resolve the incident.

7.0 PROCEDURE FOR MANAGING DATA SECURITY BREACHES

7.1 Notifying Line Managers, Department Heads and the Data Protection Officer

All incidents which give rise to a personal data breach should be immediately reported as follows:

7.1.1 By employees to their line managers;

7.1.2 By line managers and/or processors to their relevant Department Head;

7.1.3 By the relevant Department Head to the Data Protection Officer using the report form prescribed in Appendix A.

7.2 Notifying the Data Protection Commission

7.2.1 All data beaches that gives rise to a *'risk'* to the rights and freedoms of data subjects shall be reported, by the Data Protection Officer, to the Data Protection Commission without undue delay and, where feasible, within **72 hours** of Kilkenny County Council becoming aware of the incident.

7.2.2 A *'risk'* to the rights and freedoms of data subjects includes a broad range of situations, of varying likelihood and severity, which could lead to material and immaterial damage such as a loss of control over personal data, financial loss, identity theft and damage to reputation.

7.2.3 In cases where a doubt exists as to whether a data breach gives rise to a *'risk'* to the rights and freedoms of data subjects the Data Protection Officer shall report the incident to the Data Protection Commission.

7.2.4 The report to the Data Protection Commission shall include the following details:

a) A chronology of the events leading up to the personal data breach;

b) A description of the nature of the personal data breach including, where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records affected;

c) A description of the likely consequences of the data breach;

d) The measures being taken or proposed to be taken by Kilkenny County Council to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects;

e) Contact details of Kilkenny County Council's Data Protection Officer or other contact point where more information can be obtained.

7.2.5 If the report to the Data Protection Commission is not made within 72 hours, it shall be accompanied by reasons for the delay.

7.2.6 Where, and in so far as it is not possible to provide all the information required in the report at the same time, the information may be reported in phases without undue delay.

7.3 Notifying the Data Subject

7.3.1 The Data Protection Officer shall, without undue delay, inform data subjects affected by a breach if it is likely to give rise to *a 'high risk'* to their rights and freedoms. The following information should be communicated to data subjects:

a) A chronology of the events leading up to the personal data breach;

b) A description of the nature of the personal data breach in clear and plain language;

c) A description of the likely consequences of the personal data breach;

d) The measures being taken or proposed to be taken by Kilkenny County Council to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects;

e) Contact details of Kilkenny County Council's Data Protection Officer or other contact point where more information can be obtained.

7.3.2 In determining whether there is a *'high risk'* to the rights and freedoms of data subjects a qualitative and quantitative analysis is required of the nature and volume of the personal data that has been compromised. For instance, financial and sensitive personal data such as details of racial or ethnic origin, political opinions, religious beliefs, trade union membership, physical or mental health, and sexual habits, history or orientation are likely to be at the higher end of the risk scale whereas contact details may be at the lower end. In addition, generally the higher the volume of personal data affected, the higher the level of risk although this would require a qualitative analysis of the data involved.

7.3.3 There are circumstances whereby Kilkenny County Council is not required to notify data subjects of a personal data breach. These include circumstances whereby:

a) Kilkenny County Council has implemented appropriate technical and organisational protection measures, and those measures were applied to the data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it e.g. encryption;

b) Kilkenny County Council has taken steps to ensure that the *'high risk'* to the rights and freedoms of the data subjects is no longer likely to materialise;

c) The notification would involve disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby data subjects are informed in an equally effective manner.

7.4 Notifying Other Organisations

In appropriate cases the Data Protection Officer will notify organisations that may be in a position to assist in protecting data subjects including, where relevant, An Garda Síochána, financial institutions etc.

7.5 Cyber Security Breach – Additional Measures

It is recognised that data breaches arising from a cyber security incident could have very serious implications. An appropriate response in this instance will require close co-operation between the

Head of IS and the Data Protection Officer and additional measures may be required to appropriately address this situation. These measures could include the following:

- Establishing a Breach Management Response Team which shall consist of the following Personal; Chief Executive, IT Manager, Relevant Director of Services, Data Protection Officer, and any other person who may be of assistance with the incident.
- Developing a Communications Strategy to support the response to the data breach.

8.0 INVESTIGATIONS BY THE DATA PROTECTION COMMISSION

Depending on the nature of the incident, the Data Protection Commission may investigate the circumstances surrounding the personal data breach. Investigations may include on-site examination of systems and procedures. Kilkenny County Council shall fully co-operate with any such investigations.

9.0 REMEDIAL ACTION

The relevant Department Head shall, as soon as practical, shall arrange for appropriate measures to be taken to:

a) Identify the circumstances and events that caused the personal data to be compromised;
b) Identify the personal data that has been compromised;
c) Identify the likely consequences of the personal data breach
d) Secure and / or recover the personal data that has been compromised;
e) Limit and / or remedy the impact of the personal data breach;
f) Assist the Data Protection Officer to compile any notifications and reports that are required to be issued to the data subjects affected and the Data Protection Commission;
g) Implement controls to prevent a repetition of a similar incident.

10.0 RECORDING INCIDENTS OF DATA BREACHES

The Data Protection Officer shall maintain a summary record of each incident of a personal data breach. The record should include a brief description of the nature of the personal data breach, its effects and remedial actions taken. Where relevant, an explanation as to why it was not considered necessary to inform the Data Protection Commission should be included. Such records will be provided to the Data Protection Commission upon request.

11.0 AWARENESS & RELATED POLICIES AND PROCEDURES

Kilkenny County Council shall implement appropriate measures to make its employees and processors aware of the contents of this policy and procedures document.

These procedures underpin the following Kilkenny County Council's policies and procedures:

- Data Protection Policy
- Data Protection Guidelines for Staff
- Records Retention Schedule
- CCTV Policy 2018
- How to Make a Subject Access Request

Kilkenny County Council's staff should ensure compliance with the above policies and procedures in addition to the Data Breach Management Procedures.

12.0 MONITORING & REVIEW

Provisions contained in this policy and procedures document shall be subject to on-going monitoring and review.

13.0 FURTHER HELP & ADVICE

For further information and advice about this procedure and about data protection matters, please contact:

Name: Eamonn Tyrrell
Phone: (Direct)353-56-7794277
E-mail: dataprotection@kilkennycoco.ie
Website: www.kilkennycoco.ie
Postal Address: Kilkenny County Council, County Hall, John Street, Kilkenny R95 A39T

14.0 DISCLAIMER

The Kilkenny County Council reserves the right to amend or revoke these procedures at any time without notice and in any manner in which the Kilkenny County Council sees fit at the absolute discretion of the Kilkenny County Council

PERSONAL DATA SECURITY BREACH REPORT FORM

Please act promptly to report any data security breaches. If you discover a data security breach, please notify your Line Manager immediately. Heads of Department to complete Section 1 of this form and email it to the Data Protection Officer at dataprotection@kilkennycoco.ie.

SECTION 1: Notification of Data Security Breach	To be Completed By Head of Department/Person Reporting Incident
Date Incident was Discovered	
Date(s) of Incident	
Place of Incident	
Name of Person Reporting Incident	
Contact Details of Person Reporting Incident *[Email Address, Telephone Number]*	
Brief Description of Incident or details of the Information Lost	
Number of Data Subjects affected, if known	
Has any personal data been placed at risk? If so, please provide details.	
Brief description of any action taken at the time of discovery	

FOR LOCAL AUTHORITY USE	
Received By:	
On [date]	
Forwarded For Action To:	
On [date]:	

SECTION 2: ASSESSMENT OF SEVERITY	To be completed by Data Protection Officer in consultation with Head of Area affected by the Breach
Details of the IT Systems, equipment, devices, records involved in the security breach.	
Details of Information Loss	
What is the nature of the information lost?	
How much data has been lost? *If laptop lost/stolen how recently was the laptop backed up onto central IT systems?*	
Is the information unique? *Will its loss have adverse operational, financial, legal liability or reputational consequences for the Local Authority or Third Parties?*	
How many Data Subjects are affected?	
Is the data bound by any contractual security arrangements?	
What is the nature of the sensitivity of the data? *Please provide details of any types of information that fall into any of the following categories*	
HIGH RISK Personal Data ▪ **Sensitive Personal Data** *[as defined in the Data Protection Acts]* relating to a living, identifiable individual's (a) racial or ethnic origin; (b) political opinions or religious or philosophical beliefs; (c) membership of a Trade Union; (d) physical or mental health or condition or sexual life; (e) commission or alleged commission of any offence, or (f) proceedings for an offence committed or alleged to have been committed by the data subject, the disposal of such proceedings or the sentence of any court in such proceedings.	
▪ Information that could be used to commit identify fraud such as personal bank account and other financial information and national identifiers, such as Personal Public Service Numbers [PPSNs] and copies of passports and visas.	
▪ Personal Information relating to vulnerable adults and children.	

SECTION 3: ACTION TAKEN	To Be Completed by Data Protection Officer
Incident Number *[e.g. KCC/2018/001]*	
Report Received By	
On [date]	
Action Taken by Responsible Officer[s]	
Was Incident Reported to Gardaí?	Yes ☐ No ☐ *If Yes, notified on:* _____ ***Details:***
Follow up action required/recommended.	
Reported to Data Protection Officer on *[date]*	
Reported to other Internal Stakeholders *[details, dates]*	
Reported to other External Stakeholders *[details, dates]*	

For Use of Data Protection Officer	
Notification to Data Protection Commissioner	Yes ☐ No ☐ *If Yes, notified on:* _____ ***Details:***
Notification to Data Subjects	Yes ☐ No ☐ *If Yes, notified on:* _____ ***Details:***
Notification to Other External Stakeholder	Yes ☐ No ☐ *If Yes, notified on:* _____ ***Details:***