COMHAIRLE CHONTAE ROSCOMÁIN

ROSCOMMON COUNTY COUNCIL

Personal Data Breach

Policy and Procedures

February 2019

Contents

Appendix

1.0 Purpose

The General Data Protection Regulation (GDPR), which came into effect on 25th May 2018, and the Data Protection Act 2018 which gives further effect to this Regulation impose obligations on Roscommon County Council to safeguard all personal data under its control. These obligations include taking appropriate measures to protect against unauthorised access, unlawful processing and accidental loss, destruction of or damage to personal data. Roscommon County Council has implemented a range of security measures in order to meet these responsibilities. However, on rare occasions, a breach of personal data security may occur. The purpose of this document is to outline Roscommon County Council's policy and procedures for addressing instances where a personal data breach may occur.

2.0 Definitions

For the purposes of this policy and procedures document the following definitions apply:

- **Personal Data:** 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.

- **Personal Data Breach:** 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.

- **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.

- **Processor:** a natural or legal person, public authority, agency or other body which processes personal data on behalf of Roscommon County Council.

3.0 Scope

3.1 This scope of this document applies to all Roscommon County Council employees and the processors that it employs.

3.2 It covers all personal data held by Roscommon County Council) in physical or electronic format relating to members of the public, service users, suppliers and employees.

4.0 Roles and Responsibilities

4.1 Roles and Responsibilities of All Employees

4.1.1 Responsibility for data protection rests with all employees. This responsibility includes the protection of personal data held by Roscommon County Council and the systems employed in the processing of such data.

4.1.2 In the event of a personal data breach occurring all employees are required to comply with the provisions of this policy and procedures document and co-operate fully with all measures being taken to address a personal data breach.

4.2 Roles and Responsibilities of Line Managers

4.2.1 Line Managers are responsible for ensuring that all employees who report to them are fully briefed on their data protection responsibilities.

4.2.2 Line Managers are responsible for ensuring that all employees who report to them fully understand what constitutes a personal data breach and the appropriate response expected from employees in the event of a personal data breach occurring.

4.2 Roles and Responsibilities of Department Heads

4.2.1 Department Heads are responsible for ensuring that the provisions of this policy and procedures document are fully implemented within their respective Departments.

4.2.2 Department Heads are responsible for ensuring that the Data Protection Officer receives maximum co-operation and assistance with all measures being taken to address a personal data breach.

5.0 Policy

5.1 It is the policy of Roscommon County Council to ensure that in the event of a personal data breach occurring that appropriate measures exist to facilitate:

a) The identification of personal data breaches and their consequences;
b) The notification of personal data breaches;
c) Limiting and / or remedying the impact of personal data breaches;
d) Implementing controls to prevent a reoccurrence of the personal data breach.

5.2 The focus of such measures shall be on protecting the rights and interests of data subjects.

6.0 Procedures

6.1 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:

a) By employees to their line managers;
b) By line managers and/or processors to their relevant Department Head;
c) By the relevant Department Head to the Data Protection Officer using the report form prescribed in Appendix A.

6.2 Notifying the Data Protection Commission

6.2.1 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 Roscommon County Council becoming aware of the incident.

6.2.2 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.

6.2.3 In cases where a doubt exists as to whether a data beach 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.

6.2.4 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 Roscommon County Council to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects;
e) Contact details of Roscommon County Council's Data Protection Officer or other contact point where more information can be obtained.

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

6.2.6 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.

6.3 Notifying the Data Subject

6.3.1 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 Roscommon County Council to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects;
e) Contact details of Roscommon County Council 's Data Protection Officer or other contact point where more information can be obtained.

6.3.2 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.

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

a) Roscommon 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) Roscommon 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.

6.4 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.

6.5 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;
- Developing a Communications Strategy to support the response to the data breach.

7.0 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. Roscommon County Council shall fully co-operate with any such investigations.

8.0 Remedial Actions

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.

9.0 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.

10.0 Awareness

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

11.0 Monitoring and Review

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

12.0 Further Information

12.1 Further information and advice on the operation of this policy and procedures document is available from the Data Protection Officer, Roscommon County Council.

12.2 Contact details for the Roscommon County Council's Data Protection Officer are as follows:

Phone Number:	90 6637100
E-mail:	dataprotection@roscommoncoco.ie
Website:	www.roscommoncoco.ie
Postal Address:	Roscommon County council Áras an Chontae Roscommon F42 VR98.

Appendix A

Personal Data Breach Reporting Form

Personal Data Breach Reference Number: _____

(to be inserted by Data Protection Officer)

1. Name and Grade of Employee Reporting the Personal Data Breach

2. Location where the Personal Data Breach Occurred

3. Date and Time the Personal Data Breach Occurred

4. Date and Time the Personal Data Breach was Discovered

5. Description of Personal Data Breach which must include

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 any IT systems that may have been involved.

6. Description of the likely Consequences of the Personal Data Breach

7. Measures Required to address the Personal Data Breach and Eliminate/Mitigate its Effects

8. Any Additional Comments

Signed: _____

Grade: _____

Date: _____

For Breach Assessment Use (To be completed by the Data Protection Officer)

1. **Rate Severity of Breach**

   'No Risk' to rights and freedoms of data subjects Yes/No

   'Risk' to rights and freedoms of data subjects Yes/No

   'High Risk' to rights and freedoms of data subjects Yes/No

   Reason for Rating _____

2. **Data Subjects to be notified?** Yes/No

   Details _____

3. **Data Protection Commission to be notified?** Yes/No

   Details _____

4. **Other organisations to be notified e.g. Gardaí, Financial Institutions** Yes/No

   Details _____

   Signed: _____

   Date: _____