Il-Kalkara Local Council

Security Incident and Personal Data Breach Policy

CONTENTS

1 INTRODUCTION

The General Data Protection Regulation (GDPR) defines that all public authorities must adhere to the regulations thereof and Member State data protection legislation.

In terms of the Local Councils Act (CAP 363) of the Laws of Malta, the Il-Kalkara Local Council (hereafter referred to as the 'Local Council') is a statutory local government authority, hence a public authority under the GDPR, having a distinct legal personality and capable of entering into contracts, of suing and being sued, and of doing all such things and entering into such transactions as are incidental or conducive to the exercise and performance of its functions as are allowed under the Act. The full and updated version of the Act can be reviewed from:

http://www.justiceservices.gov.mt/DownloadDocument.aspx?app=lom&itemid=8833

This **Security Incident and Personal Data Breach Policy** sets out the Local Council's commitment to upholding the GDPR principles and managing the information it holds fairly and lawfully and puts into place a procedure for recording security incidents and dealing with any breaches of personal data which may occur.

2 COMPLIANCE

All staff, members and contractors or others with access to Local Council information must comply with this policy.

Anyone who is found to have breached this policy could be subject to Local Council's disciplinary and dismissal policy & procedures that might be in effect from time to time and serious breaches of this policy could be regarded as gross misconduct and would be reported to the relevant authorities for further investigation.

If you do not understand the implications of this or how it may apply to you, seek advice from the Data Protection Officer.

2.1 Advice and Training

If you do not understand anything in this policy or feel you need specific training to comply with it you should bring this to the attention of your superior. The Data Protection Officer is able to provide further advice in respect of this policy.

2.2 Equality and Diversity

Every policy must consider equality and identify any potential barriers or discrimination faced by people protected by equality legislation.

3 LEGAL CONSIDERATION

3.1 The Local Council has a duty under the General Data Protection Regulation (GDPR) to ensure that the personal data it processes is kept safely and securely. This policy details how the council will record security incidents and respond in the event of a personal data breach.

3.2 No matter how careful we are in trying to ensure that all the personal data the council processes is kept securely and used with security in mind, the potential for a security incident or personal data breach will always remain. We need to have a system in place to enable us to determine when a breach occurs and to ensure we deal with it as quickly and as efficiently as possible.

3.3 The following legislation and policies are in place to ensure compliance with the GDPR:

- Data Protection Act (CAP 586)
- Local Government Act (CAP 363)
- Data Protection Policy
- Surveillance Camera Policy, Procedures and Guidelines
- and the ICT Policy and Home and Remote Working Policy (from their effective date)

4 PURPOSE AND OBJECTIVES

4.1 This policy sets out the council's commitment to upholding the GDPR principles and managing the information it holds fairly and lawfully. It seeks to ensure that any personal or special category (sensitive) personal data the council has in its possession is kept safely and securely and that processes are in place to minimise or mitigate the impact of a personal data breach.

4.2 The policy puts into place a procedure for recording security incidents and dealing with any breaches of personal data which may occur, focussing on the steps to be taken once a breach has been discovered, and the processes staff should follow.

4.3 Instances of the loss of personal data are rare in the council; however, the consequences to the reputation of the organisation and the potential impacts on individual service users of the loss of personal data mean that we need to take swift and appropriate action in the event of a loss.

4.4 The Information and Data Protection Commissioner's Office (IDPC) has the ability to impose significant fines on data controllers for serious contraventions of the GDPR.

4.5 The IDPC also has the ability to serve an enforcement notice on a data controller if it considers taking positive steps is also necessary to bring about compliance. It is possible to receive a fine and an enforcement notice.

4.6 This policy aims to provide a consistent approach and follows guidance as provided or might be provided by the IDPC. However, dealing with incidents of breaches of data is complex; there are many potential variables and a balanced judgement needs to be taken on a case by case basis.

4.7 The GDPR requires that serious personal data breaches are reported to the IDPC within 72 hours, with the IDPC having the ability to impose fines for non-reporting. It is essential that all staff and Members are able to identify a breach and report all security incidents as soon as possible.

5 SECURITY INCIDENTS AND DATA BREACHES

5.1 A security incident can be defined as any event which has caused or has the potential to cause damage to the Council's information assets and will include, but is not limited to:

- Unauthorised persons gaining or seeking to gain access to council premises
- Unauthorised persons gaining or seeking to gain access to the council's information systems, whether operated by or on behalf of the council
- Loss, theft, misuse, damage or destruction of any council information asset or equipment
- Computer virus import or infection
- Loss or theft of hard copy documents containing personal information
- Unforeseen incidents such as flood or fire
- Hacking attacks
- Use of media in council IT systems that have not been virus checked
- Failure to make adequate arrangements for information backup
- Unauthorised copying, amendment or deletion of data or software
- Unauthorised copying or use of access security cards
- Unauthorised disclosure or use of passwords, data or software
- Alteration, falsification or tampering with audit records or evidence
- Unauthorised monitoring of information systems, employees, Members or business partners
- Use of the internet in contravention with national legislation and the council's ICT Policy
- 'Blagging' offences where information is obtained by deception
- Information being disclosed inappropriately, for example, to unintended recipients or published on a website.

5.2 A data breach can be defined as the loss, disclosure or inappropriate access to personal information as a result of a security incident.

5.3 Once a security incident has been discovered and reported, it will be determined whether a personal data breach has resulted from the incident.

6 ENSURING BREACHES DO NOT HAPPEN

6.1 The effects of personal data losses are not only felt by the individuals concerned, but also affect the efficiency of the service and the reputation of the council as a whole.

6.2 It is important that all staff are aware of their responsibilities for handling personal information, keeping it secure and not disclosing it without proper cause. The Executive Secretary should ensure that all staff within their responsibility are familiar with the appropriate policies and procedures.

6.3 All data controllers have a responsibility to ensure appropriate and proportionate security of the personal data they hold. This is covered by the 6th principle of the GDPR as detailed below:

> *"Personal data should be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality')"*

6.4 The council is the data controller in relation to personal data of its staff, Elected Members and customers. Elected Members are data controllers in respect of the personal data of their constituents.

6.5 To prevent the council from being in breach of the requirements of the GDPR all elected Members, officers (whether permanent or temporary) and all third parties acting on its behalf must be aware of their corporate and personal responsibilities set out under the provisions of the GDPR.

6.6 Breaches may involve either criminal or civil liability, or both, depending on the circumstances, and may include both individual and corporate responsibility.

7 DEALING WITH AN INCIDENT

7.1 As soon as an incident has been identified, the officer concerned must report the incident immediately to the Executive Secretary, who becomes the 'incident owner'.

7.2 The councils' IT consultant/contractor or member of staff responsible for IT must be informed if the incident relates to the security of the council's IT equipment or systems, including the loss of any council issued mobile phone, laptop or tablet.

7.3 The Data Protection Officer must be informed immediately if the incident involves any personal data.

7.4 Elected Members who identify an incident relating to their role within the council (not as a representative of their political party) should initially contact the Executive Secretary.

7.5 It should be remembered that if a breach of personal data occurs where the Local Council is considered as a data processor (acting on behalf of any Government authority or agency), then the authority or agency concerned must be notified immediately. Similarly, should a breach of personal data originate from an authority or agency, the effects of the breach on the council should be assessed and the use of this policy should be considered to protect the interests of the council, its customers and stakeholders.

7.6 If an incident is suspected to have taken place the following information will be required in order to assess the seriousness of the breach:

- The type of data involved
- How sensitive the data is

- If the data has been lost or stolen, whether there are any protections in place e.g. encryption
- What has happened to the data
- What could the data tell a third party about an individual
- The volume of data i.e. how many individuals' personal data are affected by the breach
- Who are the individuals whose data has been breached
- What harm can come to those individuals
- Are there wider consequences to consider e.g. loss of public confidence, negative publicity, financial implications

7.7 If after the initial assessment a personal data breach has been clearly identified, then an incident response team should be co-ordinated by the Data Protection Officer. This should include the key officers involved in the breach.

7.8 The key officers involved should be proportionate to the type of incident. For instance, a minor personal data breach may require the following:

- Executive Secretary (breach owner)
- Data Protection Officer
- IT Consultant/Contractor/Member of Staff (if the incident is IT related)

7.9 A serious breach, whether in terms of size of breach, or sensitivity of information, may comprise part or all of the Local Council's operations.

7.10 The Executive Secretary, should liaise with the Data Protection Officer to consider the action to be taken to:

- Protect the interests of the customer;
- Ensure the continuing delivery of the service;
- Protect the interests of the Local Council;
- Meet the requirements of the GDPR in terms of informing the IDPC

7.11 Incidents will require not just an initial response to investigate and contain the situation but also a recovery plan including, where necessary:

- damage limitation;

- establishing who needs to be made aware of the incident and informing them of what they are expected to do to assist in the containment exercise. This could be isolating or closing a compromised section of the network, finding a lost piece of equipment, or simply changing access codes;

- establishing whether losses can be recovered and damage can be limited;

- fully assessing the risk in terms of the potential adverse consequences for individuals. How serious or substantial are the consequences, how likely are they to happen and what needs to be put in place to provide protection to those affected by the incident.

8 NOTIFYING THE IDPC

8.1 The GDPR places a duty on all organisations to report certain types of personal data breach to the Information and Data Protection Commissioner's Office.

8.2 The GDPR states that a personal data breach should be reported to the IDPC if the breach is likely to result in a risk to the rights and freedoms of the individuals concerned. By this it means discrimination, damage to reputation, financial loss, loss of confidentiality or any other significant economic or social disadvantage. It also requires that this is done on a case by case basis. If there is no risk to the rights and freedoms, the IDPC does not need to be notified.

8.3 In the case of a notifiable personal data breach the council shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the IDPC, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of individuals. Where the notification to the IDPC is not made within 72 hours, it shall be accompanied by reasons for the delay. Notification to the IDPC will:

a) Describe 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 concerned

b) Communicate the name and contact details of the Data Protection Officer or other contact point where more information can be obtained

c) Describe the likely consequences of the personal data breach

d) Describe the measures taken or proposed to be taken by the council to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects

8.4 Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.

8.5 The Local Council shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable the IDPC to verify compliance with the GDPR.

8.6 Failing to notify a breach when required to do so can result in a significant fine at the discretion of the IDPC.

8.7 After carrying out a full assessment of the risk, the decision as to whether or not to inform the IDPC would normally rest with the Data Protection Officer.

8.8 If the decision is to notify the IDPC, the Data Protection Officer will act as liaison with the IDPC. The Data Protection Officer will also ensure that the Chief Executive and Deputy Chief Executive are informed of all reported breaches.

8.9 The Executive Secretary will also need to consider whether any officer concerned with the incident will be subject to disciplinary procedures and if so, a report is to be drawn and reverted for a formal decision.

9 COMMUNICATION OF A PERSONAL DATA BREACH TO THE DATA SUBJECT

9.1 When the personal data breach is likely to result in a high risk to the rights and freedoms of individuals, the council shall communicate the breach to the data subject(s) without delay. This risk exists when the breach may lead to physical, material or non-material damage for the individuals whose data have been breached. Examples of such damage are:

- Discrimination
- Identity theft or fraud
- Financial loss
- Damage to reputation

9.2 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 should be considered likely to occur.

9.3 Further information regarding the methodology of assessing the risk to the data subject can be found in the Article 29 Guidelines on Personal data breach notification under Regulation 2016/679 Section IV.

9.4 The communication to the data subject shall describe in clear and plain language the nature of the breach and contain at least the information and the recommendations provided for in points (b), (c) and (d) of paragraph 7.3.

9.5 The communication to the data subject shall not be required if any of the following conditions are met:

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

b) The Local Council has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects is no longer likely to materialise;

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

9.6 The Executive Secretary and the Data Protection Officer should consider consulting the IDPC to seek advice about informing data subjects about a breach and on the appropriate messages to be sent to, and the most appropriate way to contact, individuals.

9.7 Consideration also needs to be given to any prospective equality issues that may arise from a breach e.g. the vulnerability of an individual affected by the breach.

10 POST BREACH EVALUATION

10.1 Once the immediate breach response actions have been completed it is important not only to investigate the causes of the breach, but to also evaluate the effectiveness of the response. Carrying on 'business as usual' may not be acceptable if systems, policies or allocation of responsibilities was found to be at fault. Improvements should be instigated as soon as possible and should be communicated to staff and/or Members and recorded so the Local Council can be seen to have reacted in a responsible manner.

10.2 Those investigations into the cause of the loss of data should consider any staff capability or training issues that may be indicated and where appropriate, action may be considered under the Local Council's disciplinary procedure.

10.3 If the breach was caused, even in part, by systemic and ongoing problems, then action will need to be taken and procedures in place to prevent any recurrence in the future.

11 QUERIES ABOUT DATA PROTECTION

Members of the public and members of staff who wish to request more information about data protection in the Local Council should contact:

Data Protection Officer
c/o Il-Kalkara Local Council
1, Binja tas-Salvatur,
Triq Luigi Pisani,
Il-Kalkara, KKR1330
Telephone: +356 7957 3417
Email: DPO@boomconsultancy.eu

Data Controller
The Executive Secretary
Il-Kalkara Local Council
1, Binja tas-Salvatur,
Triq Luigi Pisani,
Il-Kalkara, KKR1330
Telephone: +356 21 66 55 00
Email: kalkara.lc@gov.mt

The Information and Data Protection Commissioner

Level 2, Airways House,

High Street,

Sliema, SLM 1549

Telephone: +356 2328 7100

Email: idpc.info@idpc.org.mt

12 APPROVALS AND SIGN OFFS

This policy comes into effect on 15 September 2019.

Document Control	
Approved By	**Executive Secretary**
Date approved	**9 September 2019**
Next review date	**8 September 2020**

This policy will be reviewed on an ongoing basis. The DPO is responsible for initiating each review.

13 VERSION CONTROL

Version	Date	Changes made by	Details
1.0	5th August, 2019	DPO	Draft Security, Incident and Personal Data Breach Policy