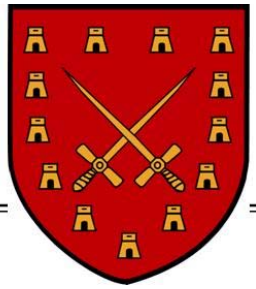
Kunsill Lokali Pembroke
Triq Alamein
Pembroke, PBK 1776,
Malta.
Tel : (+356) 2137 2111 **Fax** : (+356) 2137 2555
Web page : www.pembroke.gov.mt
e-mail : pembroke.lc@gov.mt



Pembroke Local Council
Alamein Road
Pembroke, PBK 1776,
Malta.
Tel : (+356) 2137 2111 **Fax** : (+356) 2137 2555
Web page : www.pembroke.gov.mt
e-mail : pembroke.lc@gov.mt

DATA PROTECTION POLICY

Introduction

Pembroke Local Council (the "Council") needs to gather and use certain information about third parties who come into contact with the Council. These can be residents, service providers, members of the general public, employees and other individuals whom the Council has a relationship with or may need to contact.

This policy describes how this personal data must be collected, handled and stored to meet the Council's data protection standards, and for the Council to comply with applicable laws on privacy and the protection of data.

Why this policy exists

This data protection policy ensures that the Council:

- Complies with data protection laws and follows good practice.
- Protects the rights of employees, residents and other third parties that make use of the services of the Council or are otherwise in contact with the Council ("data subjects").
- Is open about how it collects, stores and processes individuals' data.
- Protects itself from the risks of a data breach.

General Data Protection Regulation

The Regulation on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (Data Protection Directive) describes how organizations must process personal information.

These rules apply regardless of whether data is stored electronically on paper or on other materials. To comply with the law personal information must be collected and used fairly, stored safely and not disclosed unlawfully.

Personal data must:

1. Be processed fairly and lawfully.
2. Be obtained only for specific, lawful purposes.
3. Be adequate, relevant and not excessive.
4. Be accurate and kept up to-date.
5. Not be held for longer than necessary.
6. Processed in accordance with the rights of data subjects.
7. Be protected in appropriate ways.
8. Not be transferred outside the European Economic Area (EEA), unless that country or territory also ensures an adequate level of protection.

Lawful purposes

1. All data processed by the Council must be justified under one of the following lawful basis:

    i. with the consent of the data subject; or
    ii. is necessary for the performance of a contract to which the data subject is a party (ex. if a resident requires the council to provide it with a particular service, or if a third party registers to participate in an activity organised by the Council); or
    iii. to comply with a legal obligation to which the Council is subject (ex. in the field of employment); or
    iv. in order to protect the vital interest of the data subject or of another person (ex. in a medical emergency);
    v. in the performance of the Council's tasks in the public interest or in the exercise of official authority (ex. when the Council is empowered by law to process data);
    vi. to safeguard its legitimate interests (in the case of any processing which is not directly related to the performance of its tasks, ex. the Council has a legitimate interest to install CCTV cameras).

2. The Council, with the assistance of its Data Protection Officer, shall note the appropriate lawful basis in the Council's policies and procedures on the processing of data and shall assess the lawfulness of any processing operation before commencing with such processing.

3. Where consent is relied upon as a lawful basis for processing data, evidence of opt-in consent shall be kept with the personal data.

4. Where communications are sent to individuals based on their consent, the option for the individual to revoke their consent should be clearly available and systems should be in place to ensure such revocation is reflected accurately in the policies and procedures.

Data Controller

The entity responsible for the processing of personal data is:

Data Protection Officer
Ms Alison Grixti
Pembroke Local Council
Triq Alamein
Pembroke, PBK 1776.
Telephone: 2137 2111
Email: pembroke.lc@gov.mt

Data Controller
Mr Kevin Borg (Executive Secretary)
Pembroke Local Council
Triq Alamein
Pembroke, PBK 1776.
Telephone: 2137 2111
Email: pembroke.lc@gov.mt

The Information and Data Protection Commissioner
The Information and Data Protection Commissioner may be contacted at:
Level 2, Airways House,
High Street,
Sliema SLM 1549
Telephone: 23287100
Email: idpc.info@gov.mt

People, risks and responsibilities

Policy scope
This policy helps to protect the Council from security risks, including:

- **Breaches of confidentiality**. For instance, information being given out inappropriately.
- **Failing to offer choice**. For instance, all individuals should be free to choose how the Council uses data relating to them.
- **Reputational damage**. For instance, the Council could suffer if hackers successfully gained access to personal data.

Responsibilities

Everyone who works for or with the Council has some responsibility for ensuring data is processed appropriately.

Each member of staff that handles personal data must ensure that it is handled and processed in line with this policy and data protection principles.

However, the following have key areas of responsibility:

- The Mayor, Executive Secretary and Council Members are collectively ultimately responsible for ensuring that the Council meets its legal obligations.

- The Data Protection Officer is responsible for:
    - Keeping the Council updated about data protection responsibilities, risks and issues.
    - Reviewing all data protection procedures and related policies, in line with an agreed schedule.
    - To monitor compliance of the Council with applicable laws.
    - Arranging data protection guidance and advice for the members of staff covered by this policy.
    - Handling data protection questions from members of staff and other individuals covered by this policy.
    - Dealing with requests from individuals requesting what data the Council holds about them, or objecting to the processing of their data, or in any other manner enquiring about the processing of their data by the Council ("data subject requests").
    - Checking and approving any contracts or agreements with third parties that may handle the Council's personal data.
    - Where necessary, working with other staff to ensure that initiatives comply with data protection principles.
    - To act as the point of reference of the Council with the Office of the Information and Data Protection Commissioner and cooperate with same on any matter concerning data protection.

- The Council is to ensure that in engages the appropriate competent persons in the field of IT who shall be responsible for:
    - Ensuring all systems, services and equipment used for storing data meet acceptable security standards.
    - Performing regular checks and scans to ensure security hardware and software is functioning properly.
    - Evaluating any third-party services the Council is considering using to store or process data.

General staff guidelines

- The only people able to access data covered by this policy should be those who need it in the carrying out of their duties.
- Data should not be shared informally. When access to confidential information is required, employees can request it from their superior.
- The Council will provide training to all employees to help them understand their responsibilities when handling data.
- Employees should keep all data secure, by taking sensible precautions and following the guidelines below.
- In particular, strong passwords must be used and they should never be shared.
- Personal data should not be disclosed to unauthorised people, whether within the Council or externally.
- Data should be regularly reviewed and updated if it is found to be out of date. If no longer required, it should be deleted and disposed of.
- Employees should request help from the data protection officer if they are unsure about any aspect of data protection.

Data minimisation

The Council shall ensure that personal data is adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.

Data storage

These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to the data protection officer who in turn shall consult the Council's IT service provider as may be required.

When data is ***stored on paper***, it should be kept in a secure place where unauthorised people cannot see it.

These guidelines also apply to data that is usually stored electronically but is printed out for some reason:

- When not required, the paper or files should be kept ***in a locked drawer or filing cabinet***
- Employees should make sure paper and printouts are ***not left where unauthorized people can see them***, like on a printer.
- Data printouts should be shredded and disposed of securely when no longer required.

When data is stored electronically, it must be protected from unauthorised access, accidental deletion and malicious hacking attempts:

- Data should be protected by strong passwords that are changed regularly and never shared between employees.
- If data is stored on removable media (like CD, DVD or pen drive), these should be kept locked away securely when not being used.
- Data should only be stored on designated drives and servers and should only be uploaded on approved computing systems.
- Servers containing personal data should be located in a secure location.
- Data should be backed up frequently. Those backups should be tested regularly, in line with the Council's standard backup procedures.
- Data should never be saved directly to mobile devices like tablets or smart phones.
- All servers and computers containing data should be protected by approved security software and a firewall.

Data use

Personal data is of no value to the Council unless the Council can make use of it. However, it is when personal data is accessed and used that it can be at the greatest risk or loss, corruption or theft:

- When working with personal data, employees should ensure the screens of their computers are always locked when left unattended.
- Personal data should not be shared informally. In particular, it should never be sent by email, as this form of communication is not secure.
- Data should be encrypted when being transferred electronically.
- Employees should not save copies of personal data to their own personal computers. Always access and update the central copy of any data.

Data accuracy

The law requires the Council to take reasonable steps to ensure data is kept accurate and up to date.

It is the responsibility of all employees who handle personal data to take reasonable steps to ensure it is kept as accurate and up to date as possible.

- Data will be held in as few places as necessary. Staff should not create any unnecessary additional data sets.
- Staff should take every opportunity to ensure data is updated. For instance, by confirming a resident's details when they call.
- The Council shall endeavour to assist data subjects in updating the information the Council holds about them. For instance, this could be done via the Council website.

- Data should be updated as inaccuracies are discovered. For instance, if a resident can no longer be reached on their stored telephone number, it should be removed from the database.

Data subject requests
All individuals who are subject of personal data held by the Council are entitled to:

- Ask what information the Council holds about them and why.
- Ask how to gain access to it.
- Be informed how to keep it up to date.
- Request the erasure of their data ("the right to be forgotten")
- Request the restriction of processing of their personal data
- Object to the processing of their data
- Receive their personal data in electronic format and to transmit the data to another controller.
- Object to being subject to a decision based solely on automated processing.
- Be informed how the Council is meeting its data protection obligations.

If an individual contacts the Council requesting this information, they should be directed to communicate with the Council's Data Protection Officer. Data subject requests from individuals should be made by email, addressed to the data protection officer.

The data protection officer should reply to the subject access request within 14 days.

The data protection officer should always verify the identity of anyone making a subject access request handing over any information.

Disclosing data for other reasons
In certain circumstances, the GDPR allows personal data to be disclosed to law enforcement agencies without the consent of the data subject.

Under these circumstances, the Council will disclose such requested data. However the data controller will ensure the request is legitimate, seeking assistance from the board and from the Council's legal advisers where necessary.

Providing information
The Council aims to ensure that individuals are aware that their data is being processed and that they understand, *inter alia*:

- How the data is being used.
- How to exercise their rights.
- The purpose for processing their personal data.
- The retention periods.
- Who the personal information will be shared with.

To these ends, the Council has a Privacy Policy, setting out how data relating to individuals is used by the Council. A version of this statement is also available on the Council's website.