



Malta Police Force

Data Protection Policy

Policy Document

Applicable To: General Application

Classification: Unrestricted

Authorisation: Data Protection Officer

Publication Date: 20/09/2026

Current Version Number: 2.0

Review Date: 20/09/2026

Reference Number: POL-DPP

Document and Version Control

This document is maintained by the MPF. Suggestions for improvement and comments relating to the accuracy and currency of the document should be forwarded to the Data Protection Officer.

This document sets out the policy for the principles and standards of protection of personal data. It outlines the steps we take to ensure that personal data is protected and describes the rights individuals have in relation to the data we process. Specific policies governing particular processing activities shall supplement this Policy.

The version number is allocated when it has been approved. Any major revisions will be designated by the next whole number (e.g. version 2.0, 3.0, 4.0). Minor revisions shall be identified by an incremental decimal version number (e.g. 2.1, 2.2, 2.3). The current version number will appear on the front cover, footer and Table 1 of this Policy.

Table 1 – Version Control

Version Number	Approval Date	Changelog
Version 2.0	20/09/2026	Comprehensive Review And Consolidation Of The Policy Provisions.
Version 1.1	31/01/2021	Various Updates To References To Laws And Other Content.
Version 1.0	18/11/2016	First Release

Acronyms, Terminology & Definitions

- i. **CLEP** – Criminal Law Enforcement Purposes
- ii. **DPO** – Data Protection Officer
- iii. **GDPR** – General Data Protection Regulation
- iv. **IDPC** – Information and Data Protection Commissioner
- v. **MPF** – Malta Police Force

- 01. **Criminal Law Enforcement Purposes** – Means the prevention, investigation, detection or prosecution of criminal offences, the execution of criminal penalties, or safeguarding against and preventing threats to public security.
- 02. **Data Controller** – Means a person who alone or jointly with others determines the purposes and means of the processing of personal data. For the purpose of this document, and unless the context indicates otherwise, it is the Malta Police Force.
- 03. **Data Subject** – Means an identified or identifiable living natural person to whom personal data relates.
- 04. **General Data Protection Regulation** – Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 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.
- 05. **Personal Data** – Means any information relating to an identified or identifiable living natural person.
- 06. **Personal Data Breach** – Means a breach of security resulting in the accidental or unlawful destruction, loss, alteration or disclosure of, or access to, personal data.
- 07. **Processing** – Means any operation performed on personal data, including its collection, recording, organisation, storage, alteration, retrieval, use, sharing, restriction, erasure or destruction.
- 08. **Processor** – Means a person or entity which processes personal data on behalf of the controller.

09. **Profiling** – Means automated processing used to evaluate or predict personal aspects relating to a person.
10. **S.L. 586.08** – Means the Data Protection (Processing of Personal Data by Competent Authorities for the Purposes of the Prevention, Investigation, Detection or Prosecution of Criminal Offences or the Execution of Criminal Penalties) Regulations.
11. **Special Categories Of Personal Data** – Means the categories of personal data identified as such under applicable data protection law and described in section 9 of this Policy.

Table of Contents

Document and Version Control	1
Table 1 – Version Control.....	1
Acronyms, Terminology & Definitions	2
Part I: Preliminary Provisions	6
1. Policy Statement	6
2. Scope & Application	6
3. Controller	7
Part II: Policy Provisions	7
4. Objectives And Functions Of The MPF.....	7
5. Purposes And Applicable Data Protection Regimes	8
5.1 Processing For Criminal Law Enforcement Purposes (CLEP).....	9
5.2 Other Purposes.....	9
5.3 New Or Different Purposes	9
6. Legal Bases For Processing.....	10
7. Data Protection Principles	10
8. Categories of Personal Data.....	11
9. Special Categories And Criminal Offence Data	13
9.1 Special Categories Of Personal Data	13
9.2 Criminal Offence Data	13
10. Children And Vulnerable Persons	14
11. Sources of Personal Data.....	14
12. Access, Sharing And Recipients	15
13. International Transfers	16
14. Accuracy And Quality Of Information.....	16
15. Security And Personal Data Breaches.....	17
16. Data Protection By Design And By Default.....	18
17. Automated Processing And Profiling.....	18
18. Transparency And Information.....	18
19. Rights Of Data Subjects	19
20. Restrictions On Rights.....	20
21. Exercise Of Rights	20
22. Retention And Disposal	21
Part III: Governance & Administration.....	22
23. Processors AND Service Providers.....	22

24.	Records And Accountability.....	22
25.	Data Protection Officer.....	22
26.	Responsibilities Of Members And Employees.....	23
27.	Relationship With Other MPF Instruments	24
28.	Complaints And Remedies.....	24
29.	Contact Details	26

Part I: Preliminary Provisions

1. Policy Statement

The Malta Police Force is committed to protecting personal data and respecting the fundamental rights and freedoms of every person whose personal data it processes.

Personal data shall be processed lawfully and fairly and only where necessary for the achievement of the objectives of the MPF, the performance of its functions and duties, the exercise of its lawful powers or compliance with an obligation imposed by law.

The MPF shall apply appropriate measures to protect personal data and comply with applicable data protection law.

Nothing in this Policy shall limit or override any obligation, safeguard, restriction or right established by law.

2. Scope & Application

This Policy applies to all personal data processed by or on behalf of the MPF, regardless of the purpose, format, source, system or organisational unit involved.

It applies to all members and civilian employees of the MPF and, where relevant, to contractors, processors, service providers and other persons processing personal data on its behalf.

Specific legislation, policies, standard operating procedures, privacy notices and other applicable instruments may establish additional requirements and shall be read together with this Policy.

3. Controller

The Malta Police Force is the controller of personal data processed by or on its behalf, unless otherwise provided by law.

Where another authority is the controller, or responsibility is shared with another authority, this shall be identified in the relevant privacy notice or other applicable documentation.

Part II: Policy Provisions

4. Objectives And Functions Of The MPF

The processing of personal data by the MPF shall primarily be oriented towards the objectives assigned to the Force by article 4 of the Police Act. These include preserving public order and peace, preventing offences, enforcing the law, protecting rights and property, responding to requests for assistance, supporting peaceful coexistence, protecting the environment and performing all duties assigned to the Force by law.

The MPF processes personal data where necessary for the performance of its lawful functions. These include:

- a) preventing, detecting, investigating and prosecuting criminal offences;
- b) safeguarding public security and preserving public order;
- c) protecting life, physical integrity, property and the environment;
- d) responding to incidents, reports, complaints, emergencies and requests for Police assistance;
- e) collecting, preserving, analysing and presenting information, intelligence and evidence;

- f) executing warrants, judicial decisions, criminal penalties and other lawful measures;
- g) managing custody and assisting victims, witnesses, children, vulnerable persons and persons requiring protection;
- h) performing traffic, immigration, border, passenger-information and related functions;
- i) maintaining criminal records and providing certificates, vetting information and other information authorised by law;
- j) cooperating and exchanging information with national, European Union and international authorities and organisations;
- k) administering licences, permits, approvals, registrations and regulatory requirements assigned by law;
- l) receiving and managing lost, found, abandoned, seized, confiscated and other property;
- m) handling complaints, disciplinary matters, legal proceedings, audits and oversight;
- n) managing personnel, procurement, finance, contracts, premises, systems, equipment and other administrative matters; and
- o) performing any other function, duty or responsibility assigned by law.

A connection with an MPF objective or function does not remove the requirement for processing to have an applicable legal basis and to be necessary, proportionate and compliant with data protection law.

5. Purposes And Applicable Data Protection Regimes

The applicable data protection regime shall be determined principally by the purpose for which personal data is processed at the relevant time. The same information may be processed for different

purposes, provided that each processing operation is authorised by law and complies with the requirements applicable to that purpose.

5.1 Processing For Criminal Law Enforcement Purposes (CLEP)

Processing is undertaken for CLEP where the MPF acts as a competent authority for:

- a) the prevention, investigation, detection or prosecution of criminal offences;
- b) the execution of criminal penalties; or
- c) safeguarding against and preventing threats to public security.

Such processing is governed principally by S.L. 586.08 and the legislation authorising the relevant function, including the Police Act, the Criminal Code and other applicable national or European Union law.

5.2 Other Purposes

Where processing is carried out for a purpose outside criminal law enforcement, it is governed principally by the GDPR, the Data Protection Act and other applicable legislation.

This includes processing for personnel administration, salaries, pensions, occupational health, disciplinary and grievance procedures, procurement, finance, contracts, licensing, regulatory functions, civil or administrative reports, found property, legal claims, audits, research, statistics and general administration.

5.3 New Or Different Purposes

Before personal data is used for a new or different purpose, the MPF shall determine whether that purpose is authorised by law, necessary and proportionate, and which data protection regime and safeguards apply.

6. Legal Bases For Processing

The MPF shall process personal data only where the processing has a lawful basis under the applicable data protection regime.

For CLEP, processing shall be based on law and necessary for the performance of a task carried out by the MPF as a competent authority.

For processing governed by the GDPR, the MPF shall rely on an applicable legal basis. Processing connected with its statutory functions will ordinarily be based on compliance with a legal obligation or the performance of a task carried out in the public interest or in the exercise of official authority.

Consent, contractual necessity, vital interests or legitimate interests shall be relied upon only where legally available and appropriate. Consent shall not be relied upon where the person has no genuine freedom to refuse or withdraw it.

The legal basis applicable to each processing activity shall be documented where required.

7. Data Protection Principles

The MPF shall ensure that personal data is:

- a) processed lawfully and fairly;
- b) collected for specified, explicit and legitimate purposes and not further processed in a manner incompatible with those purposes, unless the further processing is authorised by law;
- c) adequate, relevant, limited to what is necessary and, for CLEP, not excessive in relation to the purposes for which it is processed;

- d) accurate and, where necessary, kept up to date, having regard to the nature and purpose of the processing;
- e) corrected, completed, erased or restricted without undue delay where it is inaccurate or is processed unlawfully, subject to applicable legal, operational and evidential requirements;
- f) retained in a form permitting identification of data subjects for no longer than is necessary for the applicable purpose, subject to any lawful retention, preservation or archival requirement;
- g) protected by appropriate technical and organisational measures; and
- h) processed in a manner that enables compliance to be demonstrated.

For CLEP, the MPF shall, as far as possible, distinguish facts from personal assessments and distinguish between the different categories of persons concerned, including suspects, convicted persons, victims, witnesses, complainants, informants and other relevant persons.

8. Categories of Personal Data

Depending on the purpose and applicable legal authority, the MPF may process:

- a) identification, biographical and contact information;
- b) family, social, domestic and personal circumstances;
- c) reports, complaints, allegations, statements, incidents and operational information;
- d) intelligence, assessments, alerts and information concerning relevant persons, places, objects, vehicles and activities;
- e) criminal investigations, proceedings, offences, convictions, penalties, warrants, custody, evidence and criminal records;

- f) correspondence, communications, electronic data, device information, online identifiers, system records and location information;
- g) photographs, CCTV, body-worn camera footage, audio, video and other recordings;
- h) travel, passenger, immigration, border, vehicle, driving and traffic information;
- i) financial, employment, professional, business, property and payment information;
- j) licensing, regulatory, inspection and compliance information;
- k) personnel, recruitment, payroll, pension, attendance, training, welfare, performance and disciplinary information;
- l) procurement, contractor and service-provider information;
- m) biometric, genetic, health, forensic and other special categories of personal data; and
- n) any other personal data necessary for a lawful MPF function.

The inclusion of a category in this section does not mean that it is processed in every case. The categories processed shall be limited to what is necessary and proportionate for the relevant purpose.

More detailed descriptions of the principal records held by the MPF, together with their retention periods or review arrangements, are established in the *Malta Police Force Data Retention Schedule Policy* (POL-DRS). Additional information may be provided through specific privacy notices and other applicable instruments.

9. Special Categories And Criminal Offence Data

9.1 Special Categories Of Personal Data

Special categories include personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership, and genetic data, biometric data used for unique identification, health information and information concerning a person's sex life or sexual orientation.

For CLEP, such data shall be processed only where strictly necessary, authorised under the applicable legal framework and subject to appropriate safeguards.

For purposes governed by the GDPR, such data shall be processed only where an applicable condition under data protection law is satisfied.

The MPF shall not collect or use special categories of personal data merely because they are available or potentially useful.

9.2 Criminal Offence Data

Personal data relating to criminal allegations, suspected or established offences, investigations, prosecutions, convictions, criminal penalties and related measures is not, solely for that reason, a special category of personal data.

When processed for CLEP, such data shall be subject to the general requirements of S.L. 586.08. When processed for a purpose governed by the GDPR, it shall be processed under official authority or where otherwise authorised by law, subject to appropriate safeguards.

Access to special-category and criminal-offence data shall be restricted to authorised persons who require it for their duties. Additional safeguards shall be applied according to the nature, purpose and risks of the processing.

10. Children And Vulnerable Persons

The MPF shall take particular care when processing personal data concerning children or vulnerable persons, having regard to their age, capacity, circumstances, safety, rights and interests.

Information shall, where appropriate, be provided in a clear and understandable form. Personal data shall be accessed, used, shared and retained only to the extent necessary for the relevant purpose and subject to appropriate safeguards.

A parent, guardian, representative or other responsible person may be involved where appropriate and permitted by law. Such involvement shall not take place where it may place the person at risk, prejudice an investigation or proceeding, or conflict with their rights or interests.

11. Sources of Personal Data

The MPF may obtain personal data directly from the person concerned or from other lawful sources, including:

- a) victims, witnesses, complainants, suspects, accused persons, convicted persons, informants and other persons;
- b) courts, judicial authorities, public authorities, regulatory bodies and official registers;
- c) other national or foreign competent authorities;
- d) European Union institutions, agencies, information systems and cooperation channels;
- e) international organisations and international police cooperation channels;
- f) employers, service providers, financial institutions, transport operators and other private entities;

- g) publicly accessible sources, including online sources;
- h) Police records, systems, reports, databases and operational activities;
- i) documents, devices, communications, objects, vehicles, premises or property lawfully accessed, obtained or examined; and
- j) authorized recording, surveillance, forensic, investigative or technical means.

Personal data shall be obtained only by lawful means and limited to what is necessary and proportionate. Public availability does not remove the requirement for its collection and use to be lawful.

The source, accuracy and reliability of information shall be assessed and recorded where appropriate. Information shall not be treated as verified fact merely because it is held in an MPF record or system.

12. Access, Sharing And Recipients

Personal data held by the MPF shall be accessed internally only by authorised persons who require it for their duties. Access to an MPF system, unit or record does not by itself authorise access to all personal data held within it.

The MPF may share personal data with courts, judicial and prosecuting authorities, public authorities, regulatory and oversight bodies, national or foreign competent authorities, European Union institutions and agencies, international organisations, parties in legal proceedings, processors, service providers and other authorised recipients.

Personal data shall be shared only where authorised or required by law and necessary for the relevant purpose. The MPF shall limit disclosure to what is required, consider the accuracy and context of the information and apply any relevant conditions or restrictions.

Regular or systematic sharing shall be governed by an appropriate legal instrument, agreement, procedure or other documented arrangement.

Access and sharing shall comply with applicable MPF procedures and any instructions or guidelines issued or approved by the DPO. The DPO shall be consulted where the lawfulness or conditions of a proposed disclosure are unclear.

13. International Transfers

Personal data may be transferred to a third country or international organisation where authorised by applicable law, necessary for a lawful MPF purpose and subject to the required safeguards.

The MPF shall use authorised cooperation channels and take reasonable steps to ensure that the recipient is authorised, the information is limited to what is necessary, appropriate security measures are used and any restrictions on use, disclosure, onward transfer or retention are communicated.

Transfers for CLEP shall comply with S.L. 586.08 and any specific legislation or instrument governing the relevant cooperation mechanism. Transfers for other purposes shall comply with the GDPR and other applicable law.

International transfers shall be carried out in accordance with applicable MPF procedures and any instructions or guidelines issued or approved by the DPO.

14. Accuracy And Quality Of Information

The MPF shall take reasonable steps to ensure that personal data is accurate, sufficiently complete, up to date and reliable for the purpose for which it is processed.

The level of verification required shall depend on the nature, source, intended use and possible consequences of the information. Where appropriate, the MPF shall indicate whether information consists of verified fact, allegation, intelligence, opinion or personal assessment.

Where personal data is found to be inaccurate, incomplete or misleading, it shall be corrected, updated, annotated, restricted or erased as appropriate. Original reports, statements and evidential records may be preserved where necessary, provided that any correction, clarification or dispute is clearly recorded.

Recipients of inaccurate personal data shall be informed where required by law and reasonably practicable.

15. Security And Personal Data Breaches

The MPF shall implement technical and organisational measures appropriate to the nature, purpose and risks of the processing. These may include physical and electronic access controls, authentication, logging, encryption, secure communications, information classification, backup and recovery, secure management of devices and media, and confidentiality and training requirements.

Access shall be limited to authorised persons who require the information for their duties and shall be reviewed when responsibilities change.

Any actual or suspected personal data breach shall be reported and handled in accordance with applicable MPF procedures. The MPF shall take appropriate steps to contain and assess the breach, mitigate its effects, restore security and implement any necessary corrective measures.

The DPO shall coordinate the assessment of whether notification to the Information and Data Protection Commissioner or communication to affected persons is required. Personal data breaches shall be documented as required by law. Detailed arrangements are established in *Data Protection Procedures Standard Operating Procedure (SOP-DPP)*.

16. Data Protection By Design And By Default

The MPF shall consider data protection requirements when developing, procuring, introducing or materially changing any process, system, technology, service or arrangement involving personal data.

Appropriate measures shall be applied to ensure that, by default, personal data is collected, accessed, used, shared and retained only to the extent necessary for the relevant purpose.

The measures applied shall take account of the nature, purpose and risks of the processing. The DPO shall be consulted where the processing or change is likely to involve material data protection risks or where consultation is required under applicable MPF procedures.

17. Automated Processing And Profiling

Automated processing and profiling may be used only where authorised, necessary and proportionate for a lawful MPF purpose and subject to appropriate safeguards.

A decision producing an adverse legal or similarly significant effect shall not be based solely on automated processing unless expressly authorised by law and accompanied by the required safeguards.

Automated results shall not be treated as necessarily accurate or conclusive. Where human review is required, the responsible person shall consider the relevance, reliability and limitations of the information before acting upon it.

18. Transparency And Information

The MPF shall provide clear and accessible information about its processing of personal data, subject to any restriction permitted by law.

This Policy provides general information about processing carried out by the MPF. More specific information may be provided through privacy notices, forms, correspondence, signage, websites, recorded messages or other appropriate means.

Information may be delayed, restricted or omitted where authorised by law and necessary and proportionate to protect an investigation, proceedings, public or national security, the rights and freedoms of others or another legally protected interest.

19. Rights Of Data Subjects

Subject to applicable law and any lawful restriction, a data subject may have the right to:

- a) receive information about the processing of their personal data;
- b) obtain access to their personal data;
- c) request the correction or completion of inaccurate or incomplete personal data;
- d) request erasure or restriction of processing;
- e) object to processing or request data portability where those rights apply under the GDPR;
- f) obtain the safeguards applicable to certain automated decisions;
- g) request verification of the lawfulness of processing through the Information and Data Protection Commissioner;
- h) lodge a complaint with the Information and Data Protection Commissioner; and
- i) seek an effective judicial remedy.

The rights available depend on the purpose of the processing and the applicable legal framework. Not every right applies to every processing operation or circumstance.

Data protection rights do not create a general right of access to Police reports, evidence, intelligence, court records, criminal-procedure material or official documents. Access concerns the requester's personal data and not necessarily the document in which it is contained.

The MPF may provide a clear and intelligible summary or extract of the personal data unless a copy of the relevant record is required by law or necessary for the effective exercise of the requester's rights.

Personal data concerning third parties, their identities and confidential sources may be withheld or redacted where disclosure is not authorised or would prejudice their rights, confidentiality, an investigation, proceedings, public or national security or another protected interest.

20. Restrictions On Rights

The exercise of a data protection right may be delayed, restricted or refused only where authorised by law and necessary and proportionate to protect an inquiry, investigation or proceeding, criminal law enforcement, public or national security, the rights and freedoms of others or another interest protected by law.

Any restriction shall be limited to what is necessary and documented where required. The data subject shall be informed of the restriction, the reasons for it and the available remedies unless providing that information would prejudice the protected purpose or is otherwise prohibited by law.

21. Exercise Of Rights

Requests concerning personal data may be submitted directly to the DPO or at any Police station, branch, unit or office.

The officer or employee receiving the request shall verify the requester's identity and, where applicable, the authority of any representative, in accordance with applicable MPF procedures. The request shall then be securely forwarded to the DPO without undue delay.

The requester shall provide sufficient information to identify the processing or information concerned and enable the MPF to locate and assess the relevant personal data.

Requests shall be coordinated by the DPO and handled within the period and in the manner required by applicable law. Where another authority is responsible for the processing, the requester may be directed to that authority.

22. Retention And Disposal

Personal data shall be retained for no longer than necessary for the purpose for which it is processed, subject to any retention, preservation or archival requirement established by law.

The *Malta Police Force Data Retention Schedule Policy* (POL-DRS) establishes the descriptions of the principal categories of records held by the MPF, their retention periods or review arrangements and the action to be taken when those periods expire. A retention period prescribed by national or European Union law shall prevail.

Where a record or processing activity is not covered by the *Malta Police Force Data Retention Schedule Policy* (POL-DRS) or another applicable instrument, an appropriate retention period or review arrangement shall be established and documented.

Personal data shall not be erased or destroyed while subject to a lawful preservation requirement, legal hold, investigation, complaint, proceeding, audit or archival obligation. When no longer required, records shall be securely destroyed, erased, anonymised or transferred to the National Archives or another authorised repository, as applicable.

Part III: Governance & Administration

23. Processors AND Service Providers

The MPF may engage processors and service providers to process personal data on its behalf only where they provide sufficient guarantees concerning data protection, confidentiality and security.

Processing shall be governed by an appropriate contract or other binding instrument requiring personal data to be processed only on the documented instructions of the MPF, unless otherwise required by law.

Processors and service providers shall not use MPF personal data for their own purposes or appoint another processor without the required authorisation.

24. Records And Accountability

The MPF shall maintain records and other documentation necessary to demonstrate compliance with applicable data protection law and this Policy.

Units shall provide the DPO with the information reasonably required to maintain such records and shall notify the DPO of material changes to their processing activities.

25. Data Protection Officer

The Commissioner shall designate a DPO in accordance with applicable data protection law.

The DPO shall advise the MPF on its obligations, monitor compliance, provide guidance, promote awareness and training, cooperate with the Information and Data Protection Commissioner and coordinate the handling of data-subject requests and personal data breaches.

The DPO shall be involved in a timely manner in matters concerning personal data, act independently and report directly to the Commissioner.

Responsibility for compliance and decisions concerning processing remains with the MPF and the unit or person responsible for the relevant activity.

26. Responsibilities Of Members And Employees

Every member and employee shall:

- a) process personal data only for authorised official purposes;
- b) access only the personal data required for their duties;
- c) comply with applicable law, this Policy and relevant MPF policies, procedures, instructions and guidelines;
- d) protect personal data, systems, devices and access credentials;
- e) take reasonable steps to maintain the accuracy and quality of information;
- f) prevent unauthorised access, use, disclosure, alteration, loss or destruction;
- g) immediately report actual or suspected personal data breaches or security incidents;
- h) promptly refer data-subject requests, complaints and other data protection matters to the DPO as required;
- i) cooperate with the DPO and authorised oversight bodies; and
- j) maintain confidentiality during and after their service or employment.

Unauthorised access, use, disclosure, alteration, concealment or destruction of personal data may result in disciplinary, civil or criminal consequences.

27. Relationship With Other MPF Instruments

This Policy shall be read together with the *Malta Police Force Data Retention Schedule Policy* (POL-DRS), the *Malta Police Force Data Protection Procedures Standard Operating Procedure* (SOP-DPP), the *Malta Police Force CCTV Policy* (POL-CTV), applicable privacy notices, information-security and records-management procedures, data-sharing and processing agreements, system-specific documentation and other relevant MPF instruments.

Processing through CCTV, body-worn cameras, recorded telephone systems and other audio-visual recording systems shall also be governed by the *Malta Police Force CCTV Policy* (POL-CTV), applicable procedures, the *Malta Police Force Data Retention Schedule Policy* (POL-DRS) and any system-specific notices or instructions.

Detailed operational requirements shall normally be established in the relevant policy, standard operating procedure, guideline or instruction.

Applicable law shall prevail over any inconsistency. Any material uncertainty or inconsistency shall be referred to the DPO.

28. Complaints And Remedies

A person who considers that their personal data has been processed unlawfully or that their data protection rights have not been respected may contact the DPO.

Where the complaint also concerns the conduct of a member or employee, including alleged unauthorised access, use, disclosure or misuse of personal data, it may also be submitted to the Professional Standards Office.

The person may also lodge a complaint with the Information and Data Protection Commissioner or seek a judicial remedy in accordance with applicable law.

Submitting a complaint to the DPO or the Professional Standards Office does not prevent the person from approaching the Information and Data Protection Commissioner, a court or another competent authority.

29. Contact Details

Data protection enquiries, requests and complaints may be addressed to:

Data Protection Officer
Legal and Data Protection Unit
Malta Police Force
Police General Headquarters
St Calcedonius Square
Floriana FRN 1530
Malta

Email: dpu.police@gov.mt

Telephone: +356 21224001

Website: www.pulizija.gov.mt

Requests may also be submitted at any Police station, branch, unit or office for verification of identity and referral to the DPO.

Complaints concerning the conduct of a member or employee may also be submitted to the Professional Standards Office through the contact channels published by the MPF or through any Police station, branch, unit or office.