

SUBSIDIARY LEGISLATION 440.05

**DATA PROTECTION
(PROCESSING OF PERSONAL DATA IN THE POLICE
SECTOR) REGULATIONS**

30th September, 2004

LEGAL NOTICE 142 of 2004.

1. The title of these regulations is the Data Protection (Processing of Personal Data in the Police Sector) Regulations. Citation.

2. (1) In these regulations, unless the context otherwise requires: Interpretation.

"Act" means the Data Protection Act; Cap. 440.

"for Police Purposes" means all the tasks which the police (or other public entities, authorities or bodies exercising police powers) must perform for the prevention and suppression of criminal offences or the maintenance of public order;

"identifiable person" means a natural person who can be identified directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity. A natural person shall not be regarded as identifiable if identification requires an unreasonable amount of time, cost or manpower effort;

"controller" means the Commissioner of Police or his representative, or any other head of a public authority or body exercising police powers or his representative.

(2) The definitions contained in article 2 of the Act shall, unless the context otherwise requires and subject to the provisions of subregulation (1), apply to these regulations.

3. The Data Protection Act shall be extended to apply to public bodies exercising police powers to the extent as is provided in these regulations. Scope.
Cap. 440.

4. (1) Without prejudice to article 23 of the Act, the controller shall notify the Commissioner for Data Protection where in the exercise of his duty, the controller is required to process personal data for police purposes. Control and notification.

(2) The notification referred to in subregulation (1) must specify:

- (a) the name and address of the controller and of any other person authorised by him in that behalf, if any;
- (b) the purpose or purposes of processing;
- (c) a description of the category or categories of data subject and of the data or categories of data relating to him;

- (d) the recipient or categories of recipients to whom the data might be disclosed.

Collection of personal data.

5. (1) The collection of personal data for police purposes shall be such as is necessary for the prevention, suppression, investigation, detection and prosecution of specific criminal offences or for the prevention of real danger, or as specified in any law.

(2) Without prejudice to article 23 of the Act, where personal data has been processed without the knowledge of the person concerned, the data subject should only be informed, where practicable, that information is held about him, as soon as the object of police activities is no longer likely to be prejudiced, and if the data are not deleted.

(3) The collection of personal data by technical surveillance or other automated means can be performed for police purposes, or in accordance with any law.

(4) The processing of sensitive personal data is allowed if this is necessary for the purposes of a particular inquiry.

Requirements for processing.

6. (1) The processing of personal data for police purposes shall as far as possible, be limited to accurate data and to such data as are necessary to allow the public authority exercising police powers to perform their functions according to Law and to fulfil international obligations arising out of any convention, treaty or bilateral agreement relating to police matters to which Malta is a party.

(2) Collection of personal data for police purposes shall not be processed for any other purpose that is incompatible with such police purposes.

(3) Personal data processed for police purposes shall not be kept for a period longer than is necessary having regard to the police purposes for which they are processed.

(4) The controller shall take reasonable measures to complete, correct, block or erase personal data to the extent that such data is incomplete or incorrect having regard to the police purposes for which they are processed.

Processing for historical purposes, etc.

7. The processing of personal data for historical, statistical or scientific purposes shall not be regarded as incompatible with police purposes provided that the controller shall ensure that:

- (a) the appropriate safeguards are in place where personal data processed for historical, statistical or scientific purposes may be kept for a period longer than is necessary having regard to the purposes for which they are processed; or
- (b) personal data kept for historical, statistical or scientific purposes shall not be used for any decision concerning a data subject.

8. (1) The communication of personal data between different bodies exercising police powers shall only be permitted where there exists a legitimate interest for such communication within the framework of the legal powers of such bodies.

Communication of personal data.

(2) Communication of personal data from bodies exercising police powers, to other Government Departments or to bodies established by law, or to other private parties may only be made in accordance with regulation 10 if:

- (a) there exists a legal obligation or authorisation to communicate such data ; or
- (b) the Commissioner for Data Protection authorises such communication of data.

(3) In exceptional cases, communication of personal data from bodies exercising police powers, to other Government Departments or to bodies established by law, or to other private parties, may also be made if:

- (a) it is clearly in the interest of the data subject and either the data subject himself has consented to the communication or circumstances are such as to allow a clear presumption of such consent; or
- (b) it is necessary for the prevention of a serious and imminent danger.

(4) Bodies exercising police powers may also communicate personal data to other Government Departments or bodies established by law, if the data are necessary for the recipient to enable him to fulfil his lawful task and provided that the purpose of the processing to be performed by the recipient is not incompatible with the original processing or contrary to the legal obligations of the body exercising police powers.

9. (1) Without prejudice to the provisions of any law regarding the protection of the data subject, transfer of personal data to foreign authorities may only be made in accordance with regulation 10 and if the recipients of such data are bodies exercising police powers.

Communication of data to foreign authorities.

(2) Subject to subregulation (1), such transfer of data shall only be permissible if there exists a legal obligation under any law, or an international obligation under a treaty, convention or international agreement on mutual assistance, to which Malta is a party.

(3) In the absence of a provision as referred to in subregulation (2), transfer of data to foreign authorities may also be made if such communication is necessary for the prevention of a serious and imminent danger, or is necessary for the suppression of a serious criminal offence.

10. (1) Requests for communication of personal data shall be submitted in writing to the body exercising police powers, and shall include an indication of the person or body making the request and of the reason and purpose for which the request is made unless any other law or any international agreement to which Malta is a party, provides otherwise.

Requests for communication.

(2) The body exercising police powers shall reply in writing informing the body making the request of the decision taken as to whether the request can be met or not.

(3) The body exercising police powers shall keep a record of all personal data communicated, indicating the following:

- (a) the details of the body making the request;
- (b) the purpose and reason for the request;
- (c) the date of transmission of data.

(4) Personal data communicated from bodies exercising police powers, to other Government Departments or to bodies established by law, or to other private parties, or to foreign authorities, shall not be used for purposes other than those specified in the request for communication of data.

(5) When it is necessary that personal data referred to in subregulation (4) be used for purposes other than those for which it was requested, the recipient shall submit a new request to the body exercising police powers in accordance with subregulation (1), and that data shall not be used by the recipient for purposes other than those included in the original request unless there is written agreement to the new request.

Safeguards for communications.

11. In the communication of personal data the following rules shall, as far as possible, be adhered to:

- (a) the accuracy of the data shall be verified no later than at the time when the data are first disclosed;
- (b) data based on opinions or personal assessments shall be checked at source prior to its disclosure and its degree of reliability or accuracy shall be indicated;
- (c) data consisting of judicial decisions or decisions not to prosecute should be clearly indicated as such;
- (d) data that are no longer accurate or up to date shall not be communicated and in the event that it is discovered that data which have been communicated are no longer accurate and up to date, the recipients of the data shall be informed unless the granting of such information would involve a disproportionate effort.

Access to other files.

12. Without prejudice to the provisions of these regulations, the body exercising police powers may, in the course of executing their duties for the prevention, suppression, investigation, detection and prosecution of criminal offences, have access to a personal data filing system held for purposes other than police purposes, in accordance with the law provided that the communicating body or the Commissioner for Data Protection has authorised such access.

Rights of access, rectification and appeal.

13. (1) The data subject may request in writing the following from the controller:

- (a) whether personal data is being processed about him for a stated purpose,
- (b) rectification, blocking or erasure of data that has not

been processed in accordance with these regulations.

(2) Without prejudice to article 23 of the Act, the controller shall provide the data subject with information in accordance with article 21(2) of the Act and rectify, block or erase personal data subject to article 22 of the Act and without excessive delay and without expense.

Provided that:

- (a) the rights of access, rectification and blocking are not restricted or refused in accordance with subregulation 3, or
- (b) in the interest of the data subject, there is no other law excluding the provision of information.

(3) The exercise of the rights of access, rectification and blocking or erasure by the data subject, shall only be restricted or refused insofar as the restriction or refusal is justified for the purpose of the suppression of criminal offences, or is necessary for the protection of the data subject or the rights and freedom of others.

(4) The data subject shall be informed in writing of the decision imposing a restriction or refusal to the exercise of the rights mentioned in subregulation (3) and shall include reasons for the restriction or refusal:

Provided that it shall be lawful not to communicate the said reasons if such restriction or refusal to communicate reasons is necessary for the performance of a legal task of the police or is necessary for the protection of the rights and freedom of others.

(5) Where access, rectification or erasure are refused or restricted, the data subject shall be entitled to appeal to the Commissioner for Data Protection within thirty days from when the data subject is informed, or may reasonably be deemed to have known, of the decision.

(6) In considering the appeal the Commissioner for Data Protection shall review the decision and shall satisfy himself that the refusal or restriction is reasonable and well founded.

14. (1) The controller shall implement appropriate technical and organisational measures to protect the personal data that are processed against accidental destruction or loss or unlawful forms of processing thereby providing an adequate level of security that gives regard to the:

Security measures relating to processing.

- (a) technical possibilities available;
- (b) cost of implementing the security measures;
- (c) special risks that exist in the processing of personal data;
- (d) sensitivity of the personal data being processed.

(2) Where the controller engages a processor, the controller shall ensure that the processor:

- (a) can implement the security measures that must be

taken;

(b) actually takes the measures so identified by the controller.

English text to prevail.

15. In the case of conflict between the Maltese and English texts of these regulations, the English text shall prevail.
