Ministry for Health

Financial Management and Control Unit

Data Protection and Retention Policy

SCOPE

1. This Policy is aimed at regulating the retention, maintenance and disposal of documentation, both personal and other, within the Financial Management and Control Unit (henceforth FMCU), as provided for in the terms of requirements emanating from legal provisions in such other acts as the Public Administration Act chapter 595 and directives emanating therefrom, and in accordance with the principles of data protection legislation, the National Archives Act chapter 477 and the Financial Administration & Audit Act chapter 174.

BACKGROUND

2. The General Data Protection Regulation (GDPR) (EU) 2016/679 puts forward the principle that personal and sensitive personal data, should not be retained for periods that are longer than necessary. In this context, the FMCU will be putting forward a retention policy for all records collected and processed, with the purpose of ensuring compliance to the Regulation and to ensure that no resources are utilised in the processing and archiving of data which is no longer of relevance.

OBJECTIVES

3. This policy aims to achieve the following objectives:

- Regulate the retention and disposal of the various types of records within FMCU while adhering to the Data Protection principle that personal data should not be retained for a longer period then necessary; as per Article 5 (e) in the GDPR.
- Dispose of unnecessary documentation that is no longer relevant and is taking up useful storage space: as per Article 17 of the GDPR.
- Promote the digitisation of documentation as may be reasonably possible in order to minimize the use of storage space, as well as to promote a sustainable use of paper and printing consumables.

THE DATA SUBJECT RIGHTS

4. The data subject is entitled to know, free of charge, what type of information the FMCU holds and processes about him/her and why, who has access to it, how it is held and kept up to date, for how long it is kept, and what the Unit is doing to comply with data protection legislation.

   The GDPR establishes a formal procedure for dealing with data subject access requests. All data subjects have the right to access any personal information kept about them by the FMCU, either on computer or in paper format. Requests for access to personal information by data subjects are to be made in writing using the Request for Access to Personal data By Data Subjects, and sent to the Data Protection Officer of the FMCU. The data subject identification details such as ID number, name and

surname have to be submitted with the request for access. In case we encounter identification difficulties, the data subject may be required to present an identification document.

Additionally, the data subject has the right to request that his/her information be amended, erased, and the right to withdraw consents were applicable at any time. A complaint can be lodged directed to the Data Protection Officer. In this regard, FMCU will take the appropriate corrective action in the event that it is proved that personal data has to be amended or erased.

FMCU aims to comply as quickly as possible with requests for access to personal data and will ensure that is provided within a reasonable time unless there is good reason for delay. When a request for access cannot be met within a reasonable time, the reason will be explained in writing.

Personal data is used for the purposes that it was originally collected. If further process is needed, the data subject will be informed and requested to consent accordingly. Data is minimised for the purpose for which it is processed.

ADMINISTRATION

5. Documentation is held and recorded by FMCU. This policy is therefore applicable to all such documentation kept by this unit. It will be the responsibility of the relevant Director General of the FMCU and its next level supervisor Financial Controller, Ministry for Health to ensure that all provisions of this policy are adhered to.

6. All staff within FMCU that create, maintain, process and store records mentioned hereunder in the retention schedule are responsible to perceive and implement the instructions given in this policy.

7. The Director General and the Financial Controller, following appropriate consultation and direction, are authorized to modify this policy as deemed appropriate from time to time to ensure compliance with state laws.

DOCUMENTATION HELD WITHIN THE FMCU

8. As part of its operating requirements the FMCU requests, keeps and maintains a wide range of documentation including personal data. The type of data that is being utilised by FMCU may be listed as follows:

    - Payments to employees
    - Payments to suppliers
    - Travel file

SECURITY OF DOCUMENTATION

9. All data is maintained in an accessible but secure location within FMCU with adequate access to authorized officials who have the necessary clearance level to retrieve the relevant data. In the case of documents with special category data requiring higher clearance levels, FMCU management team composed of the Director General finance and administration together with the relevant financial

Controller should, ensure that only those that have the required security clearance have access to such data.

10. In the case of personal data, the GDPR also stipulates that only those required to process personal data should have access to such records.
11. Personnel who are found to be in breach of these security protocols, and thus in breach of the GDPR, will be subject to disciplinary action as per Article 33 Clause (5) of the GDRP.

MANUAL VS ELECTRONIC RECORDS

12. The same retention period will apply for both electronic (if applicable) and paper format.

RETENTION PERIOD

13. The Retention schedule hereunder outlines the retention obligations for the various categories of documentation held by FMCU:

Key	Unit/Dept	Category	Record type	Description	Retention period	Remarks	Action to be determined by the National Archivist (when retention period expires).
1	Office of the Finance and Administration Unit	Finance Management and Control Unit	Payments to Employees	Our Department regularly refunds employees for travel, use of personal vehicle and salaries. We keep the files which contain this information for 10 years for any audit purpose.	Ten (10) years	The suppliers' details are managed centrally by the Treasury Department. These are kept in the Departmental Accounting System. All Accounting Officers working with the Financial Management & Control Unit have access to the suppliers' database as part of their job duties.	Not required for premanent preservation by the National Archives
2	Office of the Finance and Administration Unit	Finance Management and Control Unit	Payments to Suppliers	The files with payments to suppliers contain personal information taken from the financial system and also from documents such as tax invoices. These are kept for 10 years for any audit purpose.	Ten (10) years	None	Not required for premanent preservation by the National Archives

3	Office of the Finance and Administration Unit	Finance Management and Control Unit	Travel file	Public officers travelling on duty abroad. All records pertaining to travel are found in one file.	Ten (10) years		All the reocrds pertaining to this collection are to be retainedby the originated office until furthur notice

IMPLEMENTATION OF THE RETENTION PERIOD

14. The implementation of the said retention periods shall come into force as from 27th May 2019 cover all data held at FMCU. The first step will be to dispose of old documents dating back decades held within the premises according to procedure and timeframes listed in this policy. Every file destroyed shall be documented by the staff to keep a track record. Eventually officers responsible for data listed in the retention schedule will, following approval by the management team, dispose of such data according to the given timeframes.

CONCLUSION

15. This retention policy is intended towards achieving a good working balance between the retention of useful information and the disposal of data which is no longer required and is being unnecessarily archived. Data that needs to be destroyed will be disposed of in an efficient manner to ensure that such information will no longer be available within FMCU. Data Protection Controller, Heads, and DPOs will be made aware of the relevant retention periods listed in this policy and will instruct all relevant personnel to follow the indicated procedures accordingly.

It is to be noted that anonymised data do not fall within the parameters of this Retention Policy, since they do not constitute identifying personal data

The Data Controller of the Finance and Management Unit may be contacted at:
Director General
Address:
Ministry for Health
15, Triq il-Merkanti, Valletta
Email: edgar.borg@gov.mt
Telephone: 22992000

The Data Protection Officer of the Finance and Administration, may be contacted at:

E-mail: dpoadministration.health@gov.mt
Telephone: 22992286

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
Email: idpc.info@gov.mt
Telephone: 23287100