PEOPLE & STANDARDS DIVISION

Data Protection
Public Administration
Human Resources
Corporate Procedures

Research & Personnel Systems Directorate

Draft Version: 1.8 Date of 1st issue: Dec 2004 Last Amended: Apr 2020

Table of Contents

I Introduction

1.1 Scope

These procedures are intended to be used as guidelines by Human Resources Sections within the Public Administration when processing employees' personal data. Officers assigned duties in HR Sections are obliged to adopt these procedures in order to provide safeguards to processing operations related to employees in compliance with the General Data Protection Regulation (EU) 2016/679 (GDPR),the Data Protection Act (Cap. 586) and the National Archives Act (CAP. 477) of the Laws of Malta and to set standards within the HR context.

1.2 Background Information

In 2018, due to updates in Government policies, new exigencies, advances in technology and the coming into force of the GDPR, as of 25th May 2018, the need to update these procedures was imperative. In this regard, a working group was set up to effect such review. The working group was composed of officials from the Office of the Prime Minister (OPM), the Data Protection Unit (DPU) within the Ministry for Justice, Equality and Governance (MJEG), the Ministry for Health (MFH), the Ministry for the Economy, Investment and Small Business (MEIB), Transport Malta, Jobsplus and Malta Information Technology Agency (MITA).

This document is updating previous guidelines issued in December 2004 and September 2015, which reflected the provisions of the Data Protection Act (Cap. 440) transposing Directive 95/46/EC.

These guidelines shall now apply to both the Public Service and the Public Sector. It is to be noted that with regards to the Public Sector these guidelines are applicable unless stated otherwise by a Collective Agreement/specific entity policies or procedures as long as these are GDPR compliant.

1.3 GDPR Overview

The GDPR provides for stricter rules in the processing of personal data. Rights of data subjects have been considerably strengthened and this means that obligations on the part of Data Controllers and Processors have also increased.

Personal data in the HR context falls squarely within the criteria for processing personal data contained within the principles as provided for in the GDPR. The GDPR clearly identifies the need for processing where there is the necessity emanating from the performance of a contract to which the data subject is party.

One important GDPR principle is that of "storage limitation". The GDPR states that '*personal data are not kept longer than necessary, having regard to the purpose/s for which they are processed*' signifying that Data cannot be kept 'just in case'. A retention schedule has been

developed indicating the period during which personal data may be kept, depending on the process in respect of employees. Therefore, any application forms or any other documents containing personal data are to be disposed of, in a responsible manner, and without undue delay, based on the guidelines published in the Retention Policy for HR Documents.

1.4 Other Regulations governing the Public Service and Public Sector HR Sections

The revised procedures outlined in these documents are aimed at improving practices of handling personal information within the Public Administration HR Sections. These guidelines are to be followed in conjunction with the Public Service Commission (PSC) Regulations, as well as the Public Service Management Code (PSMC), which currently govern most of the procedures adopted in the HR Sections within the Public Service.

Public Sector entities are not obliged to follow the PSMC where indicated, however it is suggested that those entities which do not have set policies and procedures and/or a collective agreement may refer to the PSMC set procedures and regulations

II Procedures

2.1 Salary Statements and FS3 Forms

Description

Salary statements are sent via e-mail in the form of a pdf attachment through the Central Government Payroll System. The pdf file contains, apart from personal details, the IBAN number, breakdown of the salary including allowances, bonuses, NI contributions and FSS. There may be instances where this statement contains other sensitive data, such as alimony payments ordered by the Court. At the beginning of each calendar year, FS3[1] forms are also generated in pdf format by the system and sent via e-mail to employees for FSS purposes. These forms show all earnings, social security payments and FSS paid for the previous year. Employees who do not have a valid e-mail address receive their salary statements and FS3 forms as hard copies.

Procedure

In cases where transferring salary statements and FS3 forms through the Payroll System to the government or personal e-mail 'inbox' of the particular officer is not possible, the respective printed document should be distributed in a responsible manner by a person who is accountable to execute such duties.

All care should be taken to ensure confidentiality, providing safeguards so that payroll data related to employees is not disclosed to any persons who are neither the direct superiors of such employees, nor involved in the processing of such personal data. In cases where an employee is absent from the place of work, the salaries Statements and FS3 forms should **not**:

- be left on the desk of the concerned employee; or
- be handed to any other colleague unless the employee concerned has consented to such action.

The salary Statements and FS3 forms should:

- be collected personally from the respective responsible officer when they report back to work;
- if absence is for a long period, they should be sent by post to the employees concerned; and
- be sealed in envelopes addressed to the appropriate employees.

Alternatively, the following options should be pursued in the following cases:

- Where there is a large number of employees in a department the salary statements and

[1] Payee Statement of Earnings

FS3 may be delivered in sealed envelopes to individual employees, grouped by section within that particular department and handed to each Head of Section in a sealed envelope, to be distributed by him/her in a confidential manner.

- Where there are area offices, or outlying sections, such salary statements and / FS3 forms should be grouped by area and handed to each Head in a sealed envelope, to be distributed by him/her in a confidential manner.

In cases where an employee receives the salary by cheque instead of direct credit, the above procedures should be followed.

Reporting change of e-mail address for payslip purposes

When an employee changes his/her email account following a move to another Ministry/Department/entity or for a similar reason, the respective employee should with immediate effect notify the respective Salaries Section. This will ensure that salary statements reach the correct employee in a timely manner.

Payslips of employees paid from the Central Government Payroll Systems may be viewed online from My Personal Kiosk.

Notification to Jobsplus

As per relevant legislation, Jobsplus is to be notified whenever there is a change in employment, i.e. both when an employee is promoted or transferred. HR Sections are to send a copy of the Movement Sheet, which is submitted every month with the Employment Return, to Jobsplus.

2.2 Movement of personal files

Description

Personal files contain personal data of employees. Personal data within this file may even include special categories of personal data, which must be handled in a strictly confidential manner. Depending on the size of the ministry/department, personal files are either held in cabinets in a registry, or else within the HR Section. Where such files are kept in a separate registry, these are sent to authorised staff by hand with a messenger in a responsible manner. The normal registry procedures are followed, i.e. marking the movement of the file in question. In cases where the files are kept within the HR Section itself, authorised HR officers have access to personal files. In such cases, a record of the file movement must be kept.

Temporary files

Separate temporary files regarding particular subject matters are created to restrict access to the personal information within the main personal file.

Temporary files are also created to store documents about distinct issues, which are unrelated to the original relevant personal file. This practice is done in order to eliminate the possibility of unauthorised disclosure of documents, which are unrelated to the issue for which a temporary file was created, especially when the file needs to be moved.

Disciplinary files

Disciplinary files are held separately but are to be attached to personal files and moved together when the employee changes Ministry/Department.

Guidelines to follow in cases of Disciplinary files can be found on the Manual on Disciplinary Procedures in the Malta Public Service.

Procedure

Access and movement of personal files

- HR Section Heads must ensure that personal files are only accessed by authorised staff in the course of exercising HR functions. For this purpose, a list of officers who are authorized to access personal files is to be drawn up. Apart from the Head of the Public Authority, only officers performing HR duties should be authorised to access personal files. In cases where personal files are held in a Registry, a copy of this list should be given to the officer-in-charge Registry.
- No personal files should be given to officers who are not authorised to have access to

personal files unless the reason for access is related to HR purposes. When the reason for access is not related to HR purposes, the Data Controller should decide whether access should be granted. A note should be inserted in the personal file in these cases. When the specific task in question is executed, the authorization to access such personal file is to be terminated.

- Every time an employee's personal file is handed to a desk officer, an entry is to be made on the file covers, indicating the receiving officer and movement date as per standard registry procedures. This serves as an audit trail of the movement of the file. All movements are to be recorded through a Registry System; the movement details are to be recorded through the application.
- Extra care should be taken in order to ensure that the contents of the file in question are not accessible by third persons, especially during the movement of file. For this reason, the following procedure should be strictly adhered to:
- When files are moved both within the same Public Authority or to a location outside the Public Authority, these should be sent in a sealed envelope clearly indicating the name of officer to receive envelope. When sending more than one personal file to locations outside the department or HR Section, these should be placed in a lockable portable container or box. When a public employee receives a personal file, s/he must take measures to safeguard personal data in that file. The employee must not leave the file lying about unattended or leave it open in a way that unauthorised persons could browse through the contents. At the end of a working day, all files should be kept under lock and key.
- In the case of the creation of a temporary file, a note should be attached inside the employee's personal file to make desk officers aware that, apart from this main file, a temporary file has also been opened for a specific issue. Such a note is to contain:
    - The Employee ID No. and Temporary File No;
    - The title of the temporary file – which indicates the issue involved;
    - A warning to destroy this note when the particular case is closed and the temporary file cover destroyed.
- Likewise, a note should be attached inside the temporary file – on the left-hand side, on top of the minute sheet – showing the following:
    - The Employee ID No. and the main Personal File No;
    - A warning to destroy this note, together with the temporary file cover, when the particular case is closed.
- Following the closure of the particular case or issue, all the documents contained in the temporary file are to be inserted in the main personal file, and the cover of the temporary file is to be destroyed, together with the above-mentioned notes – in both the main file as well as in the temporary file.

- Personal files (blue files) of public employees 'detailed' for duty with a public entity should be retained by the parent Ministry/Department and the personal file opened by the Public Entity should **not** be added to the personal file retained at the parent Ministry/Department when detailing is revoked.

2.3 Ombudsman files, Other Inquiries and Investigations

Ministries, Departments and Public Entities have Liaison Officers that serve as a link between the Office of the Ombudsman and the Ministry, department or public entity in which they are assigned. Ombudsman Cases are sent directly to either the Permanent Secretary or the Liaison Officer in the respective Ministry or Entity. The Liaison officer opens a file on each Ombudsman Case which is not to be inserted with the personal file of the officer concerned.

It is to be noted that in view of the personal data contained within such files, care should be taken that only Liaison officers and management that is related to the case have access to such files in order to accurately understand the merits and considerations to be made in each case. Access by the data subject is to be governed by the procedures covered in the GDPR and through procedures listed under section 2.6.

Further Guidelines on requests for personal data required for investigative and/or auditing purposes can be found in the Disclosure of Personal Data for Audit and Investigative Purposes

2.4 Recruitment

Recruitment procedures applicable to Public Sector entities are defined and streamlined in accordance to Directive 7 - Delegation of Authority to Recruit in the Public Sector Entities. The delegation of authority for the filling of vacancies in Public Sector Entities, introduced through Directive 7, extends to the Public Service by Directive 9 - Delegation of Authority to Conduct Selection Processes and Make Appointments in the Malta Public Service. This Directive applies to all Ministries and government departments and to their respective Permanent Secretaries. The Manual on the Selection and Appointment Process under Delegated Authority in the Malta Public Service, attached to this Directive, is to be considered as Government's official document which regulates the delegated selection and appointment procedure in the Malta Public Service.

2.5 Publication of Selection Board and examination results

Description

The procedure for selection boards is normally regulated by the Public Service Commission in the case of the Public Service. Applications for vacancies in Scales 16 upwards (excluding industrial grades) are now submitted via the Recruitment Portal. Currently, the Recruitment Portal of the Government of Malta provides an internet-based solution to the current selection processes within the Public Service, and enables employees and the general public to:

- View vacancies in the Public Service;
- Electronically submit their applications for vacancies in the Public Service.

Presently in the case of Officers below salary scale 5, when a candidate sits for an examination or applies for a post in the Public Service, the results are eventually posted on the PSC notice board. The results are also published on a notice board which is accessible to the public, pertaining to the respective department which issued the call for applications.
On the same day, a notification of the publication of the result is to appear on the Ministry's / department's website. Concurrently, an SMS alert is to be sent to all candidates who underwent the selection process and who submitted a mobile phone number (and an email address) with their application. The SMS alert (maximum of 160 characters) is to be limited to informing the candidates that the result for the particular vacancy has been published at the respective Ministry/Department.

The published lists normally show the Index No, ID No, Name and Surname, Marks obtained and Order of Merit in the case of successful candidates, and the same details excluding Name/Surname and Order of Merit of unsuccessful applicants. Selection Board Results for post/positions above scale 6 are sent via e-mail to limit circulation.

Procedure

1. Calls for applications in the Government Gazette and/or circulars are to inform prospective candidates where the result would be published following the examination. Results can be published - at PSC, at the respective department issuing the vacancy and also at Examinations Department in cases of vacancies with exam.
2. The application form is to make reference to the conditions stipulated in the Government Gazette and/or circulars of the respective call for application.
3. After the selection process, the following details would be published as follows:

a) For successful candidates:

- Identity Card No
- Index No (where applicable)
- Name and Surname

- Marks obtained
- Order of merit

b) For candidates failing the examination:

- Identity Card No
- Index No (where applicable)
- Marks obtained
- Order of merit

4. The results are to remain published for 10 days, following which all results are removed from the respective notice boards.
5. After the results are removed from the notice boards, the relative details are kept at PSC or the respective department. Interested candidates who took part in the examination or interview can make a request to PSC for a breakdown of marks. This is in line with the Manual on Industrial Relations and the Selection and Appointment Process under Delegated Authority in the Malta Public Service.

2.6 Access by Employees to their Personal Data

Description

Public employees can request access to their personal file. Sick leave and vacation leave records can be viewed by logging into My Personal Kiosk.

Procedure

Requests by public employees to see personal information about them may consist of:

1. access to their personal file;
2. daily enquiries for routine information.

1. Requests for Access to personal files

a) Requests made by telephone or verbally should not be entertained.

b) Employees wishing to have access to any information contained in personal files should submit a request in writing (e-mail, memo, or letter), addressed to the Data Protection Officer (DPO) of the respective Ministry/department, giving the following identification details:

- ID Card No;
- Name and surname of employee;
- What particular details s/he would like to see.

A Subject Access Request form can be found here.

c) The DPO registers the access request on a subject access request register, taking note of the particulars mentioned in (b) above, the date when the request is received, the HR Manager to whom the request is to be referred, and the date when the request is referred to HR. It is advisable that the subject access request register be held in electronic spreadsheet format, so as to facilitate the tracking of subject access requests.

d) The DPO refers the subject access request to the HR Manager, who inserts the request in the relevant personal file.

e) If it is deemed necessary, the HR Manager or his/her delegate can liaise directly with the employee making the access request, to clarify further and determine what course of action is to be taken as shown in (f) below. Where the access request is too vague and/or generic, the HR Manager should obtain enough information to focus the request on a particular subject related to the employee.

f) The HR Manager or his/her delegate is to prepare for access to data as per Article 15 of the GDPR by:

i. making a copy of the document/papers containing the information requested; or
ii. showing the employee the file/documents to his/her satisfaction.

A note is to be signed by the employee viewing the personal file, or receiving copies of such file confirming that his/her access request has been met.

g) In giving information to the employee as the data subject, care should be taken not to divulge any information relating to third persons, unless such third person is acting in an official capacity.

h) Where the third person is not acting in an official capacity, and it is considered necessary that this information be given, prior consent should be obtained from the respective third person. If consent is not given, then information on third persons cannot be disclosed and the following measures should be taken:
   i. In cases where a copy of a particular document is going to be given to the data subject, identification details of third persons should not be disclosed;
   ii. Where the employee is allowed to view his personal file, identification details of third persons should be blanked out as well, by weeding out documents that may be prejudicial to third parties.

i) In the case where the employee has viewed his/her personal file, and signed the note confirming that s/he has had access to the personal file, a copy of the note is sent to the DPO.

j) The DPO updates the subject access register with the date when the request has been met.

k) The subject access request register should contain a column to take note of the date, termed as "retention date", when personal details should be deleted. The retention period should not exceed six months from the date when the request has been met. The DPO should therefore update this field accordingly.

l) Periodically the DPO is to check the subject access request register for requests which exceed the six-month retention period as mentioned above and delete all personal details in the columns containing the identity card number and names/surnames of the data subjects concerned.

m) The GDPR provides timeframes for Subject Access Requests to be completed. The requested information is to be provided without undue delay and within one month of receipt of the request at the latest. This period may be further extended to two months where necessary, taking into account the complexity and number of requests. In such cases, the data subject is to be informed of such an extension within one month of the receipt of the request, together with the reasons for the delay.

n) Where the data subject makes the request by electronic form means, the information is to be provided by electronic means where possible, unless otherwise requested by the data subject.

2. Day-to-day enquiries for routine information

When an employee makes a simple specific request, such as details of vacation leave entitlement, salary information and similar records, these requests will continue to be dealt with by HR Branches, without reference to the departmental DPO. Vacation leave and Sick Leave records can be accessed by the employee through My Personal Kiosk. HR staff would only need to consult the employee's records and give the required information. No record related to the enquiry needs to be kept.

2.7 Private Work by public employees

Description

Public employees are required to obtain permission from their respective Permanent Secretary before undertaking any private work outside their official duties as per PSMC Section 6.2.3. Following the granting of permissions, Directors (Corporate Services) process and retain such records. Directors (Corporate Services) are required to inform the Office of the Commissioner for Revenue of public officers authorised to engage in private work.

Procedure

1. Public employees should submit the Request to Perform Private Work form (PSMC Appendix 6 ii) to their respective Permanent Secretary to obtain permission before undertaking any private work outside their official duties. Requests should be channeled through the respective Head of Department.
2. Directors (Corporate Services) should still keep records of public officers granted approval to perform private work.
3. When Directors (Corporate Services) inform the public officers of the approval to perform private work, they should draw the officers' attention to the fact that the particulars relating to approvals of permission to perform part-time work are being sent to the Commissioner for Revenue.
4. HR Managers/officers are to update records of employees by contacting individually the employees already granted such permission and confirm the relevant details or otherwise.
5. The HR Branch is to inform the respective Department Head of any changes in the conditions of permissions in respect of their employees who were granted approval to perform part-time jobs.
6. If during the period of approval to perform private work, the public officer is transferred, progresses or is promoted to a higher scale, the permission shall be deemed as having been automatically withdrawn and a fresh approval shall be sought.
7. Public officers who benefit from work-life balance measures may **not** engage in private-work or work with any voluntary organisations even after hours.

2.8 Sick Leave certificates

Description

Employees who are away from work on sick leave are to submit their medical certificate (NI 46) to their department on the date when they resume duty as per PSMC Section 3.2.4.1. In some departments, sick leave certificates are attached to attendance sheets until such time as the latter are referred to the HR Branch.

Procedure

1. Sick leave certificates are to be attached to attendance sheets in a sealed envelope.
2. Sick leave certificates sent in or handed by employees are to be referred to the HR Branch, through the respective Head of Section, for retention by HR personnel.
3. In cases of outlying offices, these sick leave certificates are to be submitted to senior officers dealing with HR matters, through their respective immediate superiors.
4. The sick leave card and other related records are to be updated accordingly. Public Service employees may access information regarding sick leave on My Personal Kiosk.
5. Sick Leave certificates are not to be put away in personal files.
6. Sick leave certificates are to be retained for one (1) year from date of issue of the certificate.

2.9 Access to IT Applications for HR purposes and Security

Description

In the course of routine duties, HR staff consults and accesses "corporate" IT systems such as, but not limited to **Human Resources Information Management System (HRIMS), Government Payroll System,** the **Absence Management System AMS and Common Database (CdB)**.

HRIMS is an application that is used to manage employment information about government employees. Apart from employee identification details, its database contains other data such as grade, salary scale, career progression, etc.

The **Government Payroll System** is used to maintain salaries, allowances, NI, FSS, IBAN and other salaries related details and information, and to issue salaries and payments to employees and students whose details are on this system. Payments are issued every 28 days, and eventually a set of salary-related reports are system generated with every payroll run.

AMS complements the Government Payroll System, and records all absences availed of by persons whose details are on this system. This system, apart from the basic personal details of employees, contains details of vacation leave, sick leave, study leave, maternity leave, and all other absences which public employees are authorised to avail of according to the provisos of the Public Service Management Code (PSMC). User accounts are also administered by the People and Standards Division (P&SD)

CdB contains personal information of all the persons who come across the Public Registry and the Electoral Register, within Identity Malta Agency. The CdB is owned by Identity Malta and is used in government departments to check individuals' personal details such as ID Card number, name and surname, date of birth/marriage/death, addresses, and relationships such as parents, children, and spouses.

Procedure

Safeguard Procedures

1.1 These databases can contain special categories of data and, therefore, the following safeguards must be introduced to control access:

a) Access to these systems must always be given on a "need-to-know" basis – requests for new users should be restricted.

b) Existing users should be checked to see if they do, in fact, truly need access to these systems.

c) Access passwords should not be divulged to any other officer. Staff must ensure that they safeguard their passwords in accordance with GMICT policy.

d) Staff logged in to any HR application should log off before leaving their PC unattended.

e) In all cases, where a public officer granted access to any particular database is transferred to another department or is performing other duties, access to these databases should be terminated. HR should inform the Ministry/Department IMU Section to raise an eRFS so that the respective system owner deletes account of user without undue delay.

1.2 Furthermore, databases cannot be passed from one HR department/branch to another if the processing is different from the purpose for which the data was collected. Databases are fully equipped with audit facilities to monitor access and to avoid unnecessary access to data. Disciplinary measures may be resorted to if unauthorized processing is detected.

1.3 In instances of change or update of e-mail, the HR section (Director Corporate Services or delegate) should inform the IMU or Head of IT section within the respective section or Department with immediate effect when an employee is promoted or transferred to another Department.

2.10 Disclosing HR records to other Ministries or Departments

Description

HR officers are occasionally asked by officers outside their branch to give information about employees within their own department. These requests are often made by telephone.

Procedure

1. HR staff must not automatically answer questions from a senior official (or any other official) from another department or ministry about an employee's personal data.
2. There should be a written communication, stating what information is required, the reason, and if applicable, under what section of the law that information is being requested.
3. The HR Manager should seek the approval of the Data Controller whether such information is to be given, after s/he considers the request. Furthermore, the Data Protection Officer is to be consulted when sharing of personal data is not as per usual procedure.
4. Such request should be turned down if the information being requested is not for:

a) HR purposes related to the employee in question; or

b) As required under a particular law.

5. Inform the data subject prior to the disclosure, unless this will prejudice any action under a particular law (e.g. Criminal Code).
6. Where the request is made by an audit and/or investigative entity, the guidelines Disclosure of Personal Data for Audit and Investigative Purposes apply.

2.11 Public Service Research

Description

The People and Standards Division is often asked to invite Public Officers to participate in any research involving the Public Service. Normally, this research is carried out by students or public officers as part of their studies.

Similar requests may also be made by applicants through the Freedom of Information Act. It is pertinent to note that applicants making an FOI request cannot be asked to specify the reasons why they have submitted such a request. In the event that an FOI request points towards access to personal data as specified below, this is considered as exempt through Article 5 (3) (a). Requests for information arising from an FOI request are to be dealt with in accordance with the FOI Act and its subsidiary legislation.

(Note: Research exercises include also surveys.)

Procedure

1. Every individual (student or public officer) who needs to carry out research should first obtain permission in writing from the respective Head of Department. The application should contain the following details:

a. Name and surname of individual carrying out research;
b. ID Card No.;
c. Address;
d. Brief description of research required;
e. Purpose of research;
f. What personal details are required; and
g. Any terms of references and/or approval from ethics committees, universities, institutions, etc., - if research is not being done on a personal basis.[2]

2. If the research concerns the Public Service in general, involving a number of government departments, the application with the details mentioned above should be directed to the Data Protection Officer, at the People and Standards Division (P&SD)[3] on e-mail address dataprotection-psd.opm@gov.mt. In such cases, an approval or otherwise will be communicated in writing to the individual conducting the research. The DPO at the P&SD will forward the researcher's details and questions to the Directors, Corporate Service of each Ministry and s/he will disseminate to all staff, or as the case may be.
3. In cases where the research concerns a specific Ministry department/entity or Grades

[2] Data Controllers cannot disclose personal data to research being conducted on a personal basis

[3] If the research concerns the Public Sector, the application with the details mentioned above should be directed to the Data Controller of the entity.

pertaining to a specific Ministry, the application with the details mentioned above should be first referred to the Director Corporate Service (or to the person who performs such function within the Ministry), who is to request the researcher to present the necessary approvals to conduct such a study as issued either by ethics committees, universities, institutions etc. At this point, prior to any decision in respect of the research to be undertaken, the DCS or person performing such function within the Ministry should inform the Data Protection Officer, at the People and Standards Division (P&SD).

4. The DPO of the respective Ministry/Department or entity should be notified of this research request and verify that the person requesting research has the correct approvals to conduct the study.
5. In all cases, the approval for such research as communicated in writing should also oblige the individual making the research to apply necessary safeguards as a condition for carrying out this research, namely:
    a. The personal data accessed or given are only to be used for that specific purpose to conduct the research and for no other purpose;
    b. At the end of the research, all personal data should be destroyed;
    c. All references to personal data should be omitted in the report unless consent is specifically obtained from the person being identified in the research report;
    d. Participation by public officers in the research being conducted should be at their discretion, and they can refuse any participation whatsoever if they so wish;
    e. The People and Standards Division is to be provided with a copy of the research report; and
    f. Any other measure deemed fit by the respective Head, depending on the nature of the research to be carried out.
6. Where research in the public interest involves the processing of genetic, biometric or data concerning health, in terms of Article 7 of the Data Protection Act, the controller shall consult and obtain authorisation from the Information and Data Protection Commissioner. Approval is given after the Commissioner consults a research ethics committee. To facilitate this process, the Commissioner recognised research ethics committees which endorse research proposals on his behalf, as these committees not only assess such proposals from an ethical point of view, but also after taking into account data protection requirements. The approval of the research ethics committee presented by the individual shall therefore constitute authorisation by the Commissioner for the purposes of the Data Protection Act. If this approval is not presented, the request should be turned down. In the case of secondary processing of health data the provisions emanating from the procedures indicated in Subsidiary Legislation 528.10 Processing of Personal Data (Secondary processing) (Health Sector) should be followed.
7. In all circumstances, employees are to be encouraged to participate, however, they

should be free to decide whether to participate or not. Participants should also be made aware that they may opt out at any time during the course of the research.

8. Researchers are to be encouraged to use online survey tools when conducting research and requesting participation from participants. This method ensures GDPR compliance and preserves the respondents' anonymity.
9. At no point should the researcher make direct contact with the participants by making use of the Global Address List.

2.12 Performance Appraisals and Performance Bonus Reports

Description

The online Performance Appraisal system, introduced in 2016, provides for a holistic assessment of the employee. In addition to the workplan, the form contains additional sections including career development, personal attributes and going the extra mile. Performance Appraisals are done annually. The employee is given mid-year and end-of-year ratings by the supervisor, which are then confirmed at end-of-year by the next- level supervisor.

Performance Review Reports are also drawn up for officers engaged on contract basis who are entitled to a Performance Bonus. These reviews se are inserted in the Personal File and are retained for the duration of employment.

Procedure

1. Indefinite Contract Employees

- Since the form is now online, the employee has access to his/her Performance Appraisal/s. These can be printed in cases of Progression/promotion.
- Online Performance Appraisal forms are to be retained for three (3) full years.

2. Definite Contract Employees

- Performance Review Reports of officers engaged on contract basis should be filed in the respective personal file.

2.13 Attendance Sheets and Attendance Verification Devices

Description

All office personnel, with the exception of Assistant Directors and headship positions are to record their attendance daily on an attendance sheet (or on other electronic attendance devices) when reporting for work. They register their time as of morning and afternoon sessions. In cases of absences on account of vacation or sick leave, attendance sheets are to be marked accordingly. Attendance sheets are certified by senior officers authorised to monitor attendance and sent to HR Section every week. Occasionally, attendance sheets are consulted to verify attendance of a particular officer for a specific period. All absences are to be recorded on the Absence Management System.

Procedure

1. Authorised officers certifying the attendance sheets should record the Medical Certificate number in the remarks column of the attendance sheet.
2. Sick leave certificates are to be attached to the attendance sheet in an envelope (refer to section 2.8 of this document).
3. Any changes to attendance sheets must be crossed out and modifications must be signed by the authorized officer in charge.
4. HR officers inspecting the attendance sheets are to ensure that:
    a. all absences are recorded in their appropriate record forms (Leave Card, Sick Leave Card, Temporary Absences, etc.).
    b. update all other records which may be kept in the Absence Management System (AMS), or any other system running at the department concerned.
5. Attendance sheets are not to be kept for more than two years, in line with the retention policy for HR related records. This retention period is not applicable in the case of attendance sheets covering the years 1976 to1979 since officers employed between these years are entitled to a Treasury Pension.

Ministries/departments having Attendance Verification Devices installed to record attendance should refer to the Attendance Verification Systems Policy and Guidelines Document, Data Protection Requirements for Attendance Verification Systems, and The Use of Biometric Devices at the Workplace. Any Ministries/departments or entities that wish to introduce these methods should first carry out a Data Protection Impact Assessment.

Those Ministries/Departments having CCTV Surveillance installed should first carry out a Data Protection Impact Assessment. It is also advisable to refer to this link CCTV Surveillance Cameras

2.14 Definite Agreements for Contract Employees (non-Public Officers)

Description

Agreements for the engagement of contract employees from outside the Public Service, whose engagement does not require PSC endorsement (Persons of Trust, members of Ministers' and Parliamentary Secretaries' private secretariats and public employees seconded to the public service) are made to regulate the conditions of engagement in respect of the services rendered by such employees. These contracts are normally for a fixed term and can be renewed by the respective Permanent Secretary. "Position" files are also opened to retain personnel records related to the contract employee subject to OPM approval. In the case of Private Secretariat contractual staff, authority to renew such contract is delegated to the respective Permanent Secretary.

Procedure

The practice of opening a "position" file to maintain all personnel records as required in respect of the contract employee is to be continued.

1. Procedure 2.2 is to apply for the movement of such personal file.
2. All relevant personal records related to such contract employees, are to be retained at least for the duration of the contract, for monitoring and assessing the performance of such employee, and eventually to enable a considered decision on the renewal or otherwise of the employment contract.
3. In the event that the contract is renewed for another term, all relevant personal records (including all documents in relation to the first term) are to be retained for the validity period as specified in the renewal of the contract.
4. If the contract is terminated or not renewed, all personal records related to the performance or conduct/discipline of the contract employee, - with the exception of other documents related to the conditions of work including the employment contract in question, and any other record which may be required under the employment law, or by or under any other law, - are to be disposed of and/or deleted, provided that there are no pending issues. In case of pending issues, such records may only be disposed of and/or deleted, when the pending issue is resolved.

2.15 Outsourcing Verification of Sick Leave

Description

Government departments often enter into agreements with medical practitioners to certify the condition of their employees who report sick. This measure is often required to reduce the abuse of sick leave. It may also occur that certain departments provide free medical service to their employees. Government departments will have to furnish personal details to the contractor to carry out the visits on their behalf. If such agreements do not cover data protection requirements, government departments will be in breach of the General Data Protection Regulation (GDPR).

Procedure

Government departments may take this measure if deemed necessary. From a data protection point of view, government departments will still be responsible for employee data forwarded to the contractor. Entering into an agreement with the medical practitioners will constitute a relationship between the data controller (the department concerned) and the processor (the contractor). The General Data Protection Regulation (GDPR) requires that this relationship be governed by a legally binding instrument. In this regard, the following procedure is to be followed:

1. When a tender is issued, the conditions for the delivery of the service should include data protection clauses to regulate the processing of personal data by a processor. A specimen agreement with the contractor is found on the Data Protection Intranet section through this link. This can be included as a section within the Contract to be signed.
2. Alternatively, where government departments have already signed contracts which do not include data protection contractual clauses with the service provider, such contracts are to be revised to provide for data protection requirements. An amendment to the contract can be made by filling in the specimen agreement mention in 2.15.1 and consider it as an addendum or annex to the main contract.
3. Any medical data, gathered by the medical practitioner exclusively for treating the employee, other than that required to certify or verify the sick leave or health condition of the individual, should remain the property of the medical practitioner as governed by the medical profession and health ethics.

Conclusion

The guidelines outlined in this document are meant to cover most of the HR procedures used in Ministries, government departments and entities. There may be procedures other than those contained in this document, which have been developed in particular HR branches to meet specific requirements. In such cases, HR officers are directed to follow the spirit contained in these procedures. It is also pertinent to point out that these procedures are seen in conjunction with other rules and regulations governing the Public Service, namely:

1. Public Service Commission Regulations
2. Public Service Management Code, Manuals and Directives
3. OPM/MPO/PAHRO/ People and Standards Division (P&SD) Circulars related to HR issues
4. Retention policy for HR documents
5. National Archives Act (Cap. 477)

These HR corporate procedures have been approved by the People and Standards Division (P&SD) and the Data Protection Unit, Ministry for Justice, Equality and Governance. Where clarification or further guidance is required, employees are directed to contact the DCS or HR Section and the DPO within their respective Ministry or Department.

These procedures will be updated as and when the need arises.

Retention Policy for HR Documents

Scope

This policy establishes retention periods in relation to HR personal data and sets out the guidelines and procedures to be adopted by government ministries and departments to implement this policy. This document also includes a retention policy that may be adopted by entities in the Public Sector. These guidelines have been drawn up by the People and Standards Division (P&SD).

Background Information

One of the basic principles of the General Data Protection Regulation (GDPR) and the Data Protection Act Cap 586 (DPA) is that personal data cannot be kept longer than is necessary, having regard to the purposes for which data is processed. Public officers are also bound by the National Archives Act Cap 477 (NAA), which requires that all public documents of endurance value, including HR related data, be retained for archival purposes. In the exercise of reviewing corporate HR procedures, the issue of retention periods to be applied arose quite often during the discussions. It was therefore quite evident that it was necessary to develop a retention policy to give clear guidelines on the retention of HR-related data, to strike a balance between the requirements of the DPA and the NAA. Discussions were also held with the National Archivist, so as to agree on retention periods for HR data as well as on the implementation method to be applied.

Manual Records including Personal File

The retention schedule below provides guidance on retention periods for different categories of recruitment and other personnel management records. This list includes the working papers most commonly used in government departments and is not meant to be exhaustive. Other forms may be included in the future as more forms and procedures are identified if the need arises. The schedule refers to the original paper documents and does not obviate the need to retain electronic records required for the purposes of effective human resources management. Personal files related to public officers are opened at OPM Registry as well as line ministries and departments upon recruitment. Whenever a public officer is transferred to another ministry/department, the departmental personal file is sent to the new ministry/department.

The personal file is to be retained by the line ministry or department for 10 years following termination of employment. The OPM Registry shall retain the personal file for ten (10) years from the date of retirement age. The retention schedule (Annex A) outlined below refers to various documents that are inserted in the Personal file, which therefore means their retention should be in line with this period as indicated. This retention period is being set in view of conditions of reemployment and reinstatement as indicated in the Public Service Collective Agreement (2017-2024).

Electronic Records

In view that both the GDPR, the DPA and the NAA apply equally to manual and electronic records, the need is felt to draw the attention of ministries and departments to the obligation to establish retention periods to cover HR records on electronic systems as well. As a general guideline, it is being recommended that the same retention periods be extended also to all electronic records related to employees. HR electronic records are held in the HR Management Information System (HRIMS) which is managed by P&SD. Therefore, the retention periods applicable to data held by P&SD will apply to HRIMS records. In cases where line ministries and departments also keep electronic records of their employees in other forms of databases or spreadsheets, the line ministry and department concerned is responsible to delete the data following the expiry of the retention periods applicable to them, provided that there is no pending issue related to any particular employee.

However, it is pertinent to note that prior to deleting personal data from the HR system, the following basic details of public officers are to be maintained in accordance with article 88 and article 89 of the GDPR:

Employee Historic Record to be retained in HR System

1. Identity Card number
2. National Insurance number
3. Name and Surname
4. Date of Birth
5. First Position, salary scale, salary point, the actual salary (if the grade or position is not tied to a salary scale), any allowances (if applicable), date of first appointment, and ministry/department where assigned
6. Other Positions held, indicating salary scale, salary point, the actual salary (if the grade or position is not tied to a salary scale), any allowances (if applicable), date of appointment and ministry/department where assigned
7. Date of Termination
8. Termination Reason (resignation; resignation in the course of disciplinary procedures; retirement; boarded out; dismissal; definite contract expiry; death while in service; took up permanent employment with Public Sector)

Salary details with regard to different positions held by the officer concerned may be imported from the Payroll System where required to build the historic record.

It should also be noted that removing the identification details in any record, rendering it anonymous, would be deemed as physically deleted for the purposes of the GDPR, and could be further processed for statistical purposes.

Exclusions

Any form of record is to be kept longer than the period stipulated hereunder if:

a) Such record has been identified to be of archival value by the National Archivist. This record is to be kept in accordance with the NAA. As it is considered more likely that public officers in headship positions would have records that are of significant historic value, it is required that all personal files related to such officers be kept for an indefinite period, and sent

to the National Archives at a stipulated time to be agreed upon between the ministry/department concerned and the National Archives.

For the purposes of this policy, the term "public officers in headship positions" refers to officers occupying positions of Assistant Directors, Directors, Directors General and Permanent Secretary.

b) There are pending issues in relation to the employee in question and the personal file is still considered to be active. In such instances, the file will be destroyed after all pending issues have been resolved and all necessary historic records have been updated as necessary.

Implementation

The implementation of the retention schedule mentioned in Annex A is to be approached on three prongs as follows:

a) Personal and Disciplinary Files;
b) Forms which are used **as from the date of issue** of these policy guidelines termed as "New Forms";
c) Forms which have been collected **prior** to the issue of these guidelines termed as "Old Forms".

As this process is an HR management function, HR Managers are to co-ordinate any disposal of personal files and forms identified in the retention schedule, in line with established guidelines. HR Managers or public officers performing such a function in government departments are considered to be the contact persons where it is required that the National Archivist be consulted on the disposal of personal files. OPM are also to nominate a contact person who will need to co-ordinate with the National Archives to dispose of personal files held at OPM Registry. On the other hand, the National Archivist is to nominate an officer representing the National Archives to co-ordinate with the HR Managers and P&SD in this exercise.

a) Personal and Disciplinary Files

The National Archives acknowledge that there is a probability that information regarding public officers who at any time have occupied a headship position may be of historic value and needs to be archived. Therefore, all such personal files of public officers in headship positions are not to be disposed of unless there is specific authorisation by the National Archivist or his representative. Arrangements are to be made with the National Archives for the transfer of such files following the normal archives procedure.

As regards the personal files of all other government employees, these are to be disposed of after the expiration of the retention period indicated for line ministries and departments respectively. An annual exercise is to be conducted to identify employees whose retention period would have expired during the previous year. The HR Manager should generate this list of employees from the HRIMS. The personal files related to these employees are brought up for disposal.

When there are files for disposal, the National Archives are to be informed four months in advance, to provide ample time for Inspector of Records from the National Archives to carry out sampling exercises by randomly selecting files to be archived if they so deem it fit. Files not selected by the National Archives are to be destroyed once the four-month notice period to the National Archives has elapsed. If the National Archives' Inspector of Records does not carry out this selection process, one of the personal files brought up for disposal (chosen at random by the HR Manager) should be kept and handed over to the National Archives. All

the other files are to be destroyed.

HRIMS contains record of all public service employees as from 1996. This implies that all personal files of government employees who terminated their employment prior to 1996 will not be selected, as their personal details are not included in HRIMS. Therefore, a separate exercise is to be performed to bring up all those files and decide which are to be archived and not. The criteria mentioned above will apply for those cases as well. This exercise is to be performed depending on resources available and taking appropriate time as necessary.

A record is to be kept of all personal files transferred to the National Archives as well as of all personal files that are destroyed. **No personal file is to be disposed of if there are pending issues regarding the employee concerned.**

b) New Forms

The forms and records referred to in the retention schedule, which are generated as from the date of issue of these policy guidelines, are to be destroyed after the retention period indicated. It is pertinent to note that all forms and records which are normally placed in the personal files of respective officers are to conform to disposal procedures regarding personal files.

c) Old Forms

All forms and records which had been retained before the date of issue of these guidelines fall under this category. Where these forms are held in personal files, they will be destroyed when the respective personal file is brought up for disposal. In cases where other old forms mentioned in this policy document are kept separately, such forms are to be also destroyed. This covers also the old attendance sheets which have been stored, with the exception of those attendance sheets for the years between 1976 and 1979.

All soft copies of documents inserted in the personal files whose retention period has elapsed, including those that might have been forwarded to the National Archivist, are henceforth to be deleted should such soft copies not have already been deleted.

Conclusion

This retention policy aims to strike a balance between the requirements of the National Archives and good HR practice in the management of disposal of personal records, taking into consideration data protection requirements. Notwithstanding the retention periods mentioned, the National Archives reserve their right under the NAA to request samples of personal files, forms and records to be archived. Any such requests would be communicated to Heads of Department. In the absence of such requests, all HR Managers are expected to conform to the retention schedule established, and the implementation procedures described above. It is pertinent to note that destruction of records, where indicated in this policy, should be carried out appropriately, making sure that such records cease to exist any longer. Heads of Department and Data Protection Officers are expected to be aware of retention and disposal procedures, and they are to be informed and kept abreast of developments in any exercise that involves disposal of personal records and files. In this context, Heads of Department and Data Protection Officers should liaise with their respective Assistant Managers Records or Records Officers.

Endorsement of retention schedules

This retention policy was endorsed by the National Archivist on the 20th April 2020, after consultation with the Data Protection Unit, in line with the provisions of the National Archives Act (Cap 477).

All Ministries/Departments are to ensure that they seek the advice and approval of the National Archivist prior to disposal of files/records, in line with the provisions of the NAA (CAP 477).

ANNEX A

Retention Schedule – Public Service

The following is a retention schedule listing the forms and the relative retention period to be applied for the Public Service:

CATEGORY – Public Service	RETENTION PERIOD
Recruitment and Career Progression	
Application Form for the filling of posts in the Public Service	1) In the case of appointed persons:
	a) Line ministries and departments – Ten (10) years from date of termination of employment.
	2) All others, one (1) year subsequent to the validity period of the relevant call for applications (unless, in the interim, a complaint connected with a particular call for applications has been filed)
Application Forms for the filling of positions co-financed from EU funds	1) In the case of appointed persons:
	a) Line ministries and departments – Ten (10) years from date of termination of employment
	2) All others, to be retained for the period stipulated in the regulations governing the relative EU programme/s
Application Forms for the filling of Headship Positions	One (1) year from the filling of post (unless, in the interim, a complaint connected with a particular call for applications has been filed)
Application Form for the filling of Vacant Positions of Assistant Director	One (1) year from the filling of post (unless, in the interim, a complaint connected with a particular call for applications has been filed)
Applications for External Training	One (1) year from conclusion of selection process
Declaration on Employment/ Appointment	a) Line ministries and departments – Ten (10) years from date of termination of employment
Confirmation of Appointments (PSMC 1.2.8.4)	a) Line ministries and departments – Ten (10) years from date of termination of employment
Personal Record Sheet (GP46)	a) Line ministries and departments – Ten (10) years from date of termination of employment

Service & Leave Record Form (GP47)	For the same period as that kept for the relevant job application forms
Annual Performance Reports (including Performance Appraisals)	Three (3) full years
Performance Bonus Reports	a) Line ministries and departments – Ten (10) years from date of termination of employment
Progression Reports	a) Line ministries and departments – Ten (10) years from date of termination. of employment
Non-Public Officers files	One (1) year after the duration of the legislature, and further if the same person is re-appointed during another legislature
General Employee Records	
Approval to perform private work	a) Line ministries and departments – Ten (10) years from date of termination of employment
Pension Form	a) P&SD – Ten (10) years from age of retirement;
	b) Line ministries and departments – Ten (10) years from date of termination of employment
Discipline	
Admonishments	Refer to Manual on Disciplinary Procedures in the Malta Public Service
Written warnings (PSC Regulation 19)	Refer to Manual on Disciplinary Procedures in the Malta Public Service
Minor Disciplinary Cases Serious Disciplinary Cases	Refer to Manual on Disciplinary Procedures in the Malta Public Service
Absence Management	
Attendance sheets	Two (2) years
Vacation Leave application forms	Two (2) years
Vacation Leave Cards (GP 44)	Three (3) years
Health and Medical records	
Sick leave certificates (copies held at employing department)	One (1) year from issue of certificate
Request for the appointment of a Medical Board (GP 49)	a) Line ministries and departments – Ten (10) years from date of termination of employment.

Report by a Medical Board (This has been replaced by a communication from the department dealing with medical health, giving only the result of the board declaring whether the employee is fit or unfit for work).	a) Line ministries and departments – Ten (10) years from date of termination of employment
Sick Leave Card	Ten (10) years from date of termination of employment

ANNEX B

Retention Schedule – Public Sector

The following is a retention schedule listing the forms and the relative retention period to be applied for the Public Sector:

CATEGORY – Public Sector	Retention Period
Personal Information	
Employees (& Students) Personal Files (this specifically includes:	Ten (10) years from termination of employment.
Copy of Advert applied for, CV, Jobsplus engagement and termination forms, induction records, PMDP ratings and bonuses, promotion communications (incl. Career Progression), movement and salary increments, recommendations and awards. Other conditions of work (ex. Teleworking and/or reduced hours or other deductions/demotions).	
Application emails and CVs pertaining to internal/external calls, positions including interview score sheets/reports	For unsuccessful candidates 6 - 12 months after notifying candidates of the outcome of the recruitment process, unless in the interim, a complaint connected with a particular call for application has been filed.
Application Forms for the filling of positions co-financed from EU Funds	To be retained for the period stipulated in the regulations governing the relative EU programme.
Applications for training opportunities (Personal Development & Training Plan)	Ten (10) years
Training Courses provided (including certifications attained)	Ten (10) years from termination
PMDP (including student assessments)	Three (3) years from date of report
Application for Private Work	Ten (10) years from termination
Police Conduct/Security Services Records (latter to replace former once attained)	Three (3) years from issue
Failed Career Progression results	Three (3) years
Post Training Candidate Feedback	One (1) year
Post Training Manager Feedback	Two (2) year
Exit Interview	One (1) year

Disciplinary records	
Admonishments	
- written &	One (1) year
- verbal warnings	Six (6) months
These are kept separate from personal file	
Disciplinary Charges (involving disciplinary action) – separate from personal file	Ten (10) years from termination if found guilty or inconclusive
	Two (2) months if not found guilty
Health & Medical Records	
Sick Leave Certificates (or hospital notes*)	One (1) year (*stamp/section on hospital note is to be redacted)
Sick Leave Records (number of days taken in a year)	Three (3) years
Medical History (routine employee on shift test)	Three (3) years
Collective Agreement	
Collective workforce agreements and past agreements that could affect present employees.	Any copy of a relevant collective agreement retained on an employee's record will remain while employment continues and for 10 years after termination of employment