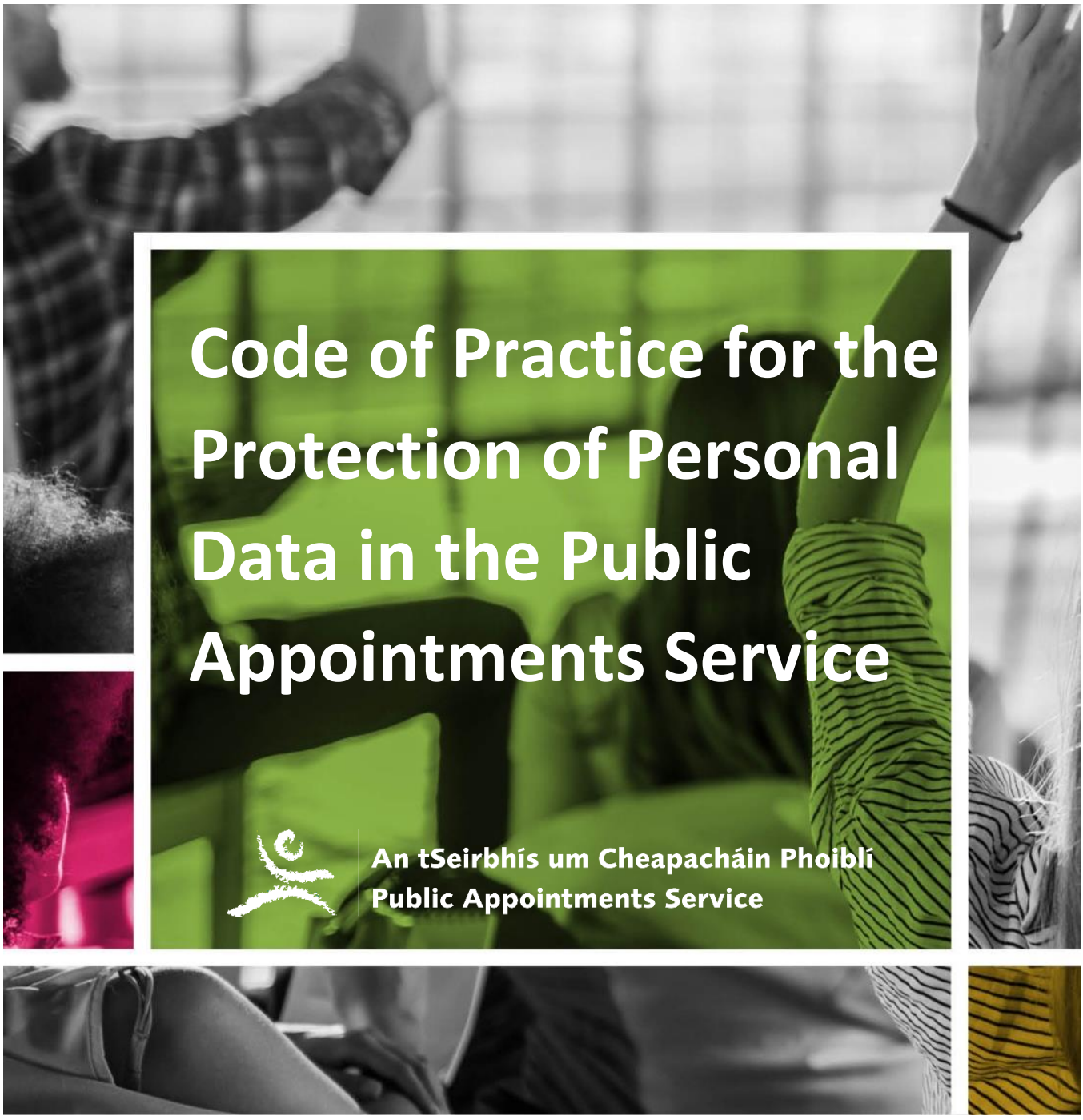


Version: 11
PAS
Updated: November 2021

Code of Practice Contents

1. Introduction

Data (including information and knowledge) is essential to the administrative business of the Public Appointments Service (PAS). In collecting personal data from our candidates, selection board members/assessors/invigilators, suppliers and staff members, PAS has a responsibility to use it both effectively and ethically. There is a balance to be struck between an individual's right to privacy and the legitimate business requirements of PAS.

It is critical that all of our staff work to the highest attainable standards. Our integrity includes both the way in which we conduct ourselves and the way in which we ensure the data we hold is compliant with relevant legislation.

Set against the General Data Protection Regulation (GDPR) the aim of this Code of Practice is to ensure each staff member in PAS has an understanding of the concepts of Data Protection and is aware of their own responsibilities. This, in turn, will assist this office in its compliance with the Regulation.

Protecting our data is common sense. We need to ensure that data gathered and processed by PAS is compliant with the General Data Protection Regulation. The reading and understanding of this Code by all staff will go a long way towards meeting this requirement.

Shirley Comerford
Chief Executive

2. Purpose and Scope of this Code

Purpose

The purpose of this Code is to ensure that staff members (and others working in or on behalf of PAS) understand our legal obligations in relation to data protection and the importance of protecting the personal data of those people who interact with our office (including candidates, selection board members/assessors/invigilators, staff, external service providers, and those registering for job alerts with publicjobs.ie and stateboards.ie).

The Code sets out our approach to ensuring compliance with all of the data protection principles for all data subject groups and how PAS ensures security of data and deals with breaches of data protection principles.

The Code also sets out a range of other policies, compliance with which is critical to ensuring the effective protection of personal data.

Scope

The Policy applies to staff and selection board member/assessors/invigilators (and former staff and selection board member/assessors). It also applies to consultants and contractors working in PAS, staff of other organisations on loan to PAS and members of the PAS Board.

Legislative Basis

The following legal framework is applicable to the manner in which PAS processes personal data;

- General Data Protection Regulation (GDPR)
- Data Protection Acts 1988-2003 (for personal data processed prior to the introduction of the GDPR and 2018
- Statutory Instruments under the Data Protection Act 2018
- ePrivacy Regulations 2011

Legislative Basis for Processing Candidate Personal Data

The General Data Protection Regulation (GDPR) provides that the processing of personal data shall be lawful where such processing is necessary for the exercise of official authority vested in the controller. PAS is mandated by statute to act as the centralised assessment and selection body for

the civil service and to carry out all the procedures necessary to undertake the recruitment, assessment and selection of suitable candidates for appointment (Section 34 of the Public Service Management (Recruitment and Appointments Act 2004) (2004 Act) therefore, the processing of personal data necessary for this purpose is lawful as Article 6(1) (e) GDPR applies.

Certain "special category" personal information is collected for Equality Monitoring purposes only. We collect such personal data to ensure that the services we provide are as accessible, fair and equitable as possible and conducted in line with PAS's public sector duty as outlined in Article 42 of the Irish Human Rights and Equality Act, 2014.

By providing any of the personal information requested in the non-mandatory equality monitoring fields, candidates consent to the collection and processing of this data for these purposes. The legal basis we are relying on to process this Data is outlined in Articles 6(1) (e) and 9(2) (a) of the GDPR. The information provided will be retained for as long as candidates wish to maintain an active publicjobs.ie account. Candidates are asked to ensure that this information is accurate and up to date and that it is updated any time their details change. Candidates are prompted to do so any time they make an application through publicjobs.ie. Candidates are informed that the information provided in this questionnaire will have no bearing on the way their application will be considered and will be used to provide information for anonymised research purposes only. The candidate has the right and ability to withdraw their consent at any time by logging on to the website and amending their details accordingly. The non-mandatory information collected comprises:

- Date of Birth
- Gender Identity
- Ethnic/Cultural Background
- Country of birth
- Nationality
- First language
- Do you consider yourself to have a disability?
- Caring responsibility
- Sexual Orientation

3. Data Protection Principles

PAS currently holds personal data on candidates (and potential candidates who have registered an interest in receiving job alerts with publicjobs.ie/stateboards.ie), selection board members/assessors/invigilators, suppliers, PAS Board members and staff.

Further details on the information held is set out in Appendix 6.

There are seven data protection principles set out in the GDPR. The manner in which PAS complies with each of these principles is set out in the following sections.

Principle One

Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject

The purposes for processing data within PAS vary greatly depending on the groups for which personal data is processed. Details about these groups are set out below.

Prospective Candidates Registering on publicjobs.ie

Prospective candidates may register with our website and complete a profile so that they can then either apply for an advertised competition or ask to be contacted in the event of vacancies arising in areas in which they might be interested. When any further competitions are being advertised for areas in which the person who registered has indicated an interest an email will issue automatically telling them what post is advertised; they can then apply for the post should they still be interested. Profiles can be updated and deleted at any stage by the person themselves or by contacting PAS and requesting same. All messages issued to those registered with publicjobs.ie are stored in the person's message board. Users can delete messages from their own message board.

Personal data captured at registration stage includes:

- Username and password*
- Security Question*
- Title
- Name*
- Date of Birth
- PPSN (if relevant)
- Gender Identity
- Email address*
- Postal address*
- Postcode
- Country*
- Daytime Phone Number*

- Other Phone Contact Number(s)
- Correspondence language preference (English or Irish)
- Highest Educational Qualification and location (i.e. name and location of School, University, Training College etc.)
- Main field of study
- Current work or study status
- Employment Sector
- Career Level
- Details of any accommodations required in the selection process
- Details of Job Alert notifications the candidate wishes to set up

*This information is mandatory as it is the minimum amount of information required to allow for the creation of a secure and unique profile and to allow PAS communicate with the user.

If prospective candidates subsequently apply for a competition, their profile details will automatically update the relevant sections of the standard application form. Other data captured when a candidate applies for a competition includes:

- Details of Education / Qualifications
- Details of membership of professional bodies and details of proficiency in Irish and English where these are essential requirements
- Whether a candidate meets the eligibility requirements for a specific post (this will change depending on the requirements for each competition)
- Citizenship details (to identify whether candidate is an EEA citizen or not, as required)
- Employment History (including title, duties and salary)
- Details of specific experience where such experience is either an essential requirement or is desirable for the role
- Examples of how the candidate has demonstrated the competencies required for the specific role
- Further details of any accommodations needed during the assessment process
- Indication of willingness to participate in candidate surveys (Yes/No)
- Details of where the candidate heard about the competition

Other information retained in a candidate's profile is:

- All applications made

- All bookings made
- All messages sent by PAS to the message board
- All job alerts registered

On occasions, PAS uses data collected from candidate profiles and/or application forms for research purposes in order to quality assure its assessment processes. This research may be retained in an anonymised form.

Candidates taking part in a Recruitment Campaign

The legislative basis for processing personal data from candidates is set out on page 4. Personal data is collected on all candidates for competitions run by PAS in order to process their applications. This information is used by the relevant recruitment unit to run a recruitment and selection competition up to the appointment of a successful candidate to the vacant post. The data is collected by means of an application. This application is used to assess eligibility for a particular competition, determine preferences in relation to the location (if applicable), determine whether the candidate meets the set shortlisting criteria (if applicable) and to aid the selection board in the interview/assessment situation (should the candidate be called to this stage). Information which is required to be provided by candidates as part of the application process relates to their relevant qualifications and experience, and examples of the competencies required for the particular post. In order to allow PAS to identify individuals and administrate the competition effectively, candidates are also required to supply their name, address and date of birth on the application form. The address and date of birth are not shared with selection board members.

Other data collected is required to confirm that the candidate meets the essential requirements for the competition, to provide reasonable accommodations which may be required, and for background checks conducted at clearance and assignments stage to ensure the person is suitable for appointment in respect of character and that he or she is fully competent to undertake, and fully capable of undertaking, the duties attached to the position. Data collected at clearance and assignments stage from those candidates under consideration for a position includes security checks and/or Garda vetting; employment or other references; health and medical information; health and character declaration; copies of relevant qualifications and proof of identification; workplace accommodation form (if such accommodations are required); drivers licence (if essential); reports from the Chief Medical Officer (CMO) (if required). Information on the date a candidate was assigned to a post in a particular department or office are also stored, along with whether or not the

candidate has taken up their appointment. Once a candidate has been appointed to a role, no further information relating to that employment is held by PAS.

Certain "special category" personal information may be collected by PAS for Equality Monitoring purposes only. We collect such personal data to ensure that the services we provide are as accessible, fair and equitable as possible and conducted in line with our obligations under the Employment Equality Acts. By providing any of the personal information requested in the non-mandatory fields candidates consent to the collection and processing of this data for these purposes. Candidates are informed that the information provided in this questionnaire will have no bearing on the way their application will be considered and will be used to provide information for research purposes only. The information comprises:

- Date of Birth
- Gender
- Ethnic/Cultural Background
- Whether the candidate considers themselves to have a disability or caring responsibility
- Sexual Orientation

Particular care is paid to ensure that the appropriate safeguards for the protection of the fundamental rights and interests of the data subject are in place when processing such special categories of personal data.

Candidates who progress to main interview stage for senior level campaigns or who are deemed successful at main interview for other roles may be asked to supply details of potential referees who will be contacted directly by PAS.

The Executive Search function in PAS hold data on individuals interested in being contacted about particular types of roles (names, contact numbers and CVs if supplied). These individuals are asked to provide their consent to the above details being retained by the Executive Search function.

Selection Board Members, Assessors and Invigilators

The following personal data is collected from all board members/assessors/invigilators, as required;

- Contact information such as name, contact phone number, email address, postal address

- Information on the prospective individual's qualifications, experience and training. This data is retained on a database so that Recruitment Units can determine whether the qualifications and experience of particular board members/assessor/invigilator would make them suitable for particular selection boards/assessment processes which may require specialist knowledge or senior experience
- Bank details, in order to pay fees/travel and subsistence, where appropriate; where board members/assessors are paid, bank account details are collected to approve board members/assessors for payment and are used by the PAS Finance Unit to make the payments).
- Data on board member training (trainings completed and dates of completion) are stored on our Learning Management System.
- Board Members/Assessors/Invigilators may advise PAS of their availability to take part in assessments. This information is communicated from the Board Member's Unit to relevant Recruitment Units and may be stored locally to ease administration

Board members/assessors/invigilators are reminded every second year that we hold their personal data and that they can update this information at any stage by contacting a named person in PAS.

Suppliers

Personal data is collected on all suppliers of goods and services in order to pay for the goods/services procured by electronic funds transfer and to ensure that the suppliers meet any regulations (e.g. tax clearance certificates). This information is used to set suppliers up on a financial system so that they can be used as suppliers, and for Finance Unit to make payments to them in respect of goods or services provided. While this information may not comprise of personal data depending on the nature of the supplier, in general the relevant data may include the following;

- Name and contact information of supplier contact (telephone number, email address, postal address, fax number etc.)
- Bank account information
- Tax reference Number (TRN)

PAS Staff Members

Personal data is collected on all staff members in order to maintain an accurate record of their service, to make payments to them, and to ensure all information required for the payment of a pension on retirement is in place. This information is stored on the PeoplePoint HR system (HRMS), and is accessible by the NSSO and the PSSC for HR purposes. The types of information held on PAS Staff will vary but may include the following;

- Name (including any name change), address, postal address and contact information (telephone and email)
- PPSN
- Bank Account information (PSSC only)
- Marital status
- Emergency contact information (Next of Kin)
- A picture of the staff member
- Details of Leave (including annual leave, sick leave etc.). This information is also stored on the flexi clock system.
- Pension Entitlement
- Eforms on employee schemes availed of, such as Cycle to Work or Travel Pass
- Training Summary
- Information on exposure to Covid-19 (advised via a questionnaire)

This information is used by the People & Culture team to complete any duties required of employers in relation to employees and by Finance Unit in order to make payments to staff. Staff members can update their personal data by contacting the People & Culture team or PeoplePoint at any stage. They can also make changes themselves on the self-service portal of the HRMS.

Data collected via cookies on publicjobs.ie

Certain data is collected via cookies on publicjobs.ie, in order to allow the website to function correctly, to analyse website performance and monitor the effectiveness of campaigns. This data is processed only in an anonymised form, and website users may set their own preferences for which cookies are generated as part of a session. Full details on the cookies in use on publicjobs.ie are available in the PAS Cookie Policy.

Principle Two

Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (except for archive purposes)

PAS only collects, processes, and stores personal data for purposes which are specific, lawful and clearly stated. The types of data processed by PAS generally are listed above. PAS only processes personal data in a manner compatible with the stated purpose. Data is collected from the above-mentioned groups and is used only in connection with the purpose for which it was collected. The main purposes for which PAS processes data are as follows;

- Information collected from candidates is used only in order to process their application for a particular competition
- Information collected from selection board members/assessors/invigilators is used only to determine their suitability for particular boards/assessment processes, to record all training provided to them by PAS, and to make payments to them
- Information collected from suppliers is used only to determine their eligibility for payments and to make those payments
- Information collected from staff is used only as part of the lawful employer/employee relationship and to meet our statutory obligations to staff.

Personal information which is obtained by PAS is not used for any other purpose other than that for which it was obtained. This personal data is not divulged to a third party unless it is entirely 'compatible' with the specified purpose.

Processing on behalf of the National Archives

The National Archives Act 1986 (amended 2018) requires PAS to submit competition files to the National Archives after 30 years. Competition files are the official record of any recruitment process undertaken by PAS. The competition files may contain certain personal data on candidates, Assessors/Board Members, PAS staff and suppliers, depending on the nature of the campaign and other factors such as how far a candidate may have progressed in the recruitment process (for further details on how PAS retains competition files, please see Appendix 4). The types of personal data relating to candidates which may be held on the competition file are as follows;

- Any candidate taking part in an assessment test will have their scores captured and retained.
- Candidates who progress to shortlisting stage will be included on the list of candidate's presented to the shortlisting board. This list may include candidate names, Candidate ID numbers, and their most recent roles; the Shortlisting Board Members' assessment of their application will also be retained (normally in the form of a summary comment).
- At interview stage, each candidate's interview notes are retained along with a copy of the marks awarded under each competency area. A summary comment is also retained to record the Board's Assessment of the candidate's performance.
- Scores will be retained for each candidate who completes an additional assessment process (such as a presentation exercise, a video interview, a group exercise etc.) and, where there is an assessment board involved, the notes of the assessment board will also be retained. Assessment notes may not be retained indefinitely for large volume campaigns; this is an area which is under discussion with the National Archives.
- Should the candidate be considered for appointment for a professional or technical competition for the Civil Service, a copy of the provisional recommendation issued to the employing organisations will be retained (this may include the candidate's name, address, PPSN, date of birth, relevant qualifications and experience).

All of this information will be retained indefinitely and ultimately sent to the National Archives.

Legitimate Disclosures to a Third Party

There are some transfers of personal data to agents who are carrying out operations on behalf of PAS and who do not retain this data for their own purposes; these do not constitute disclosures (e.g. transfer of staff data to the National Shared Services Offices for payroll/pension administration, other financial transactions or HR related purposes).

Examples of legitimate disclosures specific to PAS are listed below;

- Information on candidates who are being offered appointment are provided to the client organisation (this may include contact details, PPSN and information in relation to the candidate's qualifications/experience for the post)
- Material is provided to the Chief State Solicitor and any of their legal advisers, and to the Workplace Relations Commission (or other appropriate body) as required in the event of a case being taken against or involving PAS
- In the event of a staff member transferring to another government department/office, their personnel file and their details on the HRMS (Human Resource Management System) are transferred to the new Department/Office
- National Archives disclosures, as set out above
- Certain data is disclosed to assessment providers who carry out some of the assessments run by PAS; only the minimum amount of personal data is disclosed to allow them to fulfil their functions as data processors (normally comprising the name, email address and Candidate ID number)
- Where a person requests a review by the Commission for Public Service Appointments in relation to an alleged breach of the Code, or appeals a decision under the Freedom of Information Act to the Information Commissioner, or instigates a complaint process with the Data Protection Commission, the information requested by these bodies is provided to them in order for them to carry out their function
- PAS use external selection board members/assessors/invigilators as part of recruitment competitions, and these board members/assessors/invigilators may receive candidate data in order to assist in the determination of suitability for a specific role; selection board members/assessors/invigilators have a duty to keep such information confidential and secure and sign confidentiality agreements to confirm this obligation
- Information is provided to the Chief Medical Officer (CMO) where PAS has concerns in relation to a candidate's suitability for appointment on health-related grounds (the CMO is the qualified occupational health service for PAS)
- Some organisations which are involved with the security of the state (such as the Irish Prison Service or An Garda Síochána) may require that candidates assigned to them have additional security clearance conducted; additional details which may include the names and addresses of those candidates and details of their family members are collected from candidates and sent to the relevant client organisation for processing
- NCHD applications are collected for the HSE through our recruitment application

- The results of State Board assessment processes are sent to the appropriate Department in order for the Minister to make an appointment.

Regular audits are conducted on the legitimacy of all personal data processing within PAS and these have established that there is sound, clear and legitimate purposes for collecting all of the information currently collected. These audits are conducted on an ongoing basis by a nominated staff member on behalf of the Data Protection Officer. The findings are reviewed by the Risk Management Group. A full register of all personal data processing, or Record of Processing Activity (ROPA) is maintained and held by the Data Protection Officer and updated regularly to ensure compliance.

All data is obtained and processed in compliance with the GDPR. It should be noted that while PAS is permitted to collect the PPSN under legislation, the provision of this information is not mandatory. Where the PPSN is supplied to PAS, PAS may forward that information to an employing department as part of the appointment process.

Principle Three

Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes

PAS collects the minimum amount of personal data to allow it to fulfil its legislative remit. All new processes are reviewed to ensure that the amount of personal data to be collected is as minimal as possible. Data Protection Impact Assessments (DPIAs) are conducted in advance of the implementation of any new technology or process, or when PAS intends to process new types of data, or when planning to make new disclosure of data. PAS adopts a privacy by design approach at the planning stage of all new processes, and conducts a detailed risk assessment exercise aimed at protecting the privacy of the relevant data subjects and minimising the data collected. Any actions arising from this risk assessment process will be included in the appropriate risk register(s), and reviewed annually by the Risk Management Group.

Candidate Data Processed as part of an Assessment Process

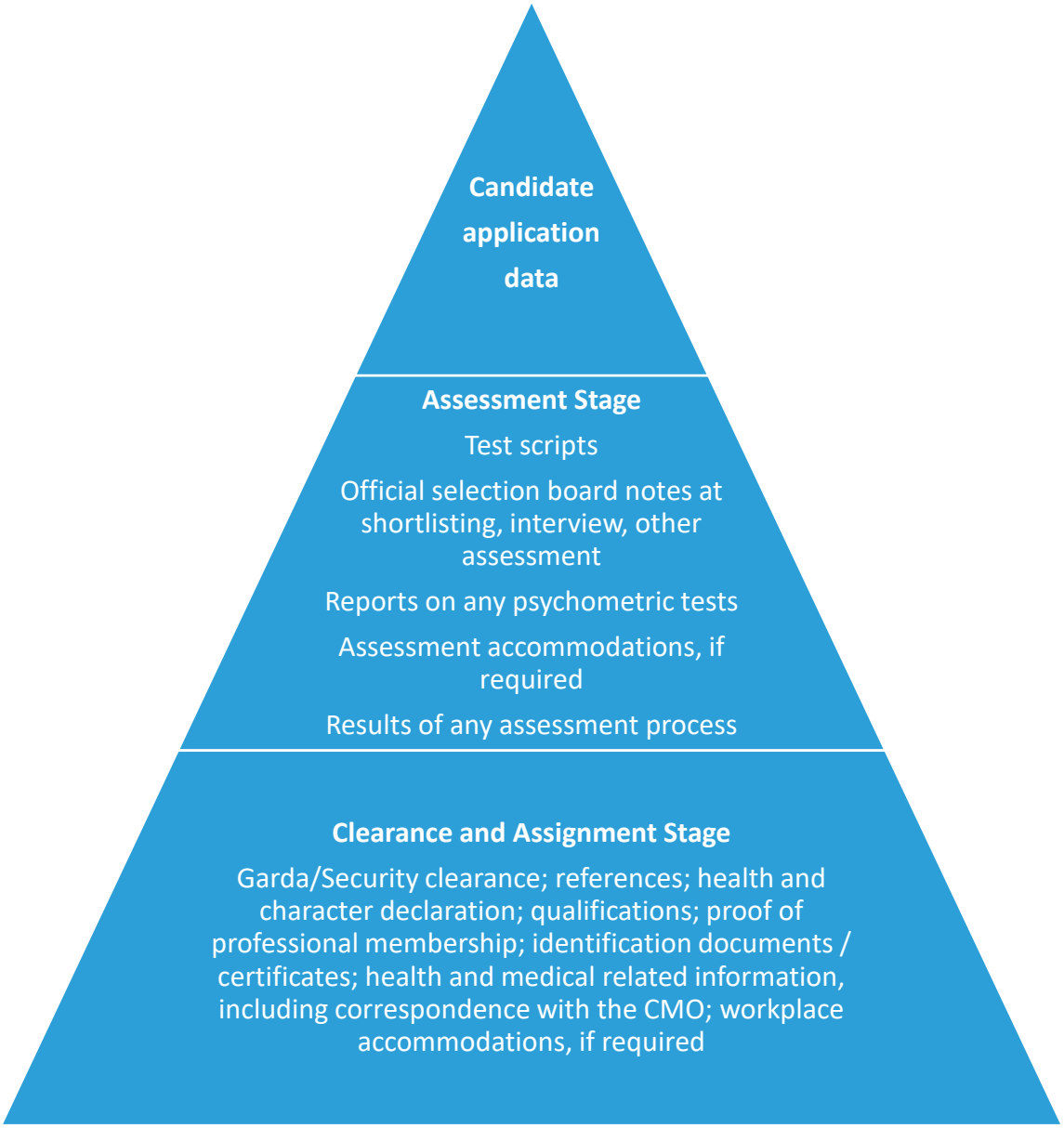
Section 24 (9) of the Public Service Management (Recruitment and Selection) Act 2004 states that "only candidates who have successfully completed the recruitment or promotion process under this Act, including compliance with the code of practice concerned shall be eligible for appointment".

Section 24 (11) of the 2014 Act states that "a candidate shall not be appointed to a post unless – (b) he or she is fully competent and available to undertake, and fully capable of undertaking, the duties attached to that position".

The 2004 Act also sets out the functions of PAS (in Section 34) "to act as the centralised recruitment, assessment and selection body" and "to ensure standards of probity, merit, equity, and fairness, consistent with the codes of practice set down by the Commission are followed in the public interest in the recruitment, assessment and selection of persons for appointments in the Civil service and other public service bodies" and "to carry out all procedures necessary to undertake the recruitment, assessment and selection of suitable candidates for appointment".

The amount of personal data collected in order for PAS to comply with the 2004 Act depends on the stage of the assessment process that the candidate progresses to, with the minimum amount of data

collected initially and additional data collected at various points of progress through the recruitment and selection process (as can be seen in the Chart below).



Processing Special Categories of Data

Certain "special category" personal information is collected by PAS to carry out certain processes. This information includes the following;

- As outlined above, some special category data is collected for Equality Monitoring purposes. PAS collect such personal data to ensure that the services we provide are as accessible, fair and equitable as possible, and are conducted in line with PAS's public sector duty as outlined in Article 42 of the Irish Human Rights and Equality Act, 2014. By

providing any of the personal information requested in the non-mandatory fields candidates consent to the collection and processing of this data for these purposes. The information provided will be retained for as long as candidates wish to maintain an active publicjobs.ie account. Candidates are asked to ensure that this information is accurate and up to date as possible. Candidates are prompted to update this information any time they make an application through publicjobs.ie. Candidates are informed that the information provided in this questionnaire will have no bearing on the way their application will be considered and will be used to provide information for research purposes only.

- Data may also be collected from candidates who require reasonable accommodations as part of the assessment process. This includes a medical or psychological report which the candidate may provide to PAS in order to facilitate the Occupational Psychologists within the Assessment Services Unit in determining what reasonable accommodations may be provided. The information retained will include a copy of that report, the candidate name and identification number, the accommodations granted and the date awarded, and the type of disability for which they candidate requires accommodations. This report is retained for the life of the panel for which it applies, and candidates will be reminded every three years that we store this data and can ask PAS at that stage (or at any time) not to retain this data.
- Where PAS conducts Garda Vetting or other Security Clearance for candidates under active consideration for a role, PAS may receive sensitive data in relation to convictions and cases which are pending, including details of the alleged offence and nature of the conviction. PAS retains such records for six months (the period of validity for Garda Vetting) or for length of any legal process concerning decisions made by PAS on the basis of this information.
- When candidates who have previously served in the public service exceed the allowed sick leave limits or indicate that they have current health related issues, their information is sent to the Chief Medical Officer (CMO) for the Civil Service (who provides Occupational Health Advice to PAS). The CMO may ask the candidate for additional information and the CMO holds this information in accordance with that office's data retention policy.

The reason behind the processing of personal data is contained in the Privacy Notices for all groups for which we process data. Files are purged in compliance with the PAS Record Management Guidelines so that personal data is not retained any longer than necessary. The Record Management Guidelines set out the retention period for all items of personal data held and the procedures in place to implement this policy. Necessary approval has been sought from the Director of the National Archives to destroy electronic and physical records as appropriate.

The PAS recruitment database contains candidates' personal profile, their previously submitted applications and electronic correspondence from PAS in relation to competitions for which they have applied. It also contains the candidates' results / progress at each stage of a competition for which they have applied.

As advised above, PAS conducts Data Protection Audits (every two years) to ensure that the information sought and retained is the minimum amount needed for the specified purpose and is adequate, relevant and not excessive in relation to the purpose(s) for which it is kept.

Principle Four

Personal data shall be accurate and, where necessary, kept up to date

The PAS Privacy Notice outlines what personal data is processed for each group on which data is processed by PAS, and informs the data subjects what information is held on them and the reason for holding this information.

Most of the personal data held by PAS is supplied by the data subject themselves and can be updated at any stage by contacting PAS. Candidates may change the information held on their profile at any time. Once a candidate reaches the later stages of a selection process, references may be sought from their previous employers/nominated referees. Candidates deemed unsuitable for appointment on the basis of reference received will be given the opportunity to challenge the information being relied upon to make the decision, and may request a copy of the reference provided under FOI or a Subject Access Request.

The equality monitoring information on a candidate's profile provided is retained for as long as candidates wish to maintain an active publicjobs.ie account. Candidates are asked to ensure that this information is accurate and up to date and that it is updated any time their details change. Candidates are prompted to do so any time they make an application through publicjobs.ie. PAS will not amend this information unless instructed to do so by the data subject, and only then after verifying the identity and authority of the instructor.

Board members/assessors/invigilators are asked to contact the Board Members Unit in order to update their personal data. Records of training completed are updated on behalf of Board Members by PAS.

Staff members are asked to update their details on PeoplePoint and/or contact Human Resources with any changes. All updates are made immediately.

Suppliers are deactivated on a regular basis if not used within the previous two years.

All of these groups on which personal data may be held have been informed that they can view or change the information stored on them at any time.

Principle Five

Personal data shall be kept in a form which permits identification of the data subjects for no longer than is necessary for the purposes or which it was collected

PAS retains personal data for no longer than is necessary for the purposes for which it was collected, except where that data is required by the National Archives (as outlined above). Retention periods for personal data held by PAS are set out in our Records Retention Guidelines. These retention periods have been agreed with the National Archives where appropriate.

Some data in relation to testing (for examples test scores) are anonymised and retained for research, validation and statistical purposes. The minimum amount of data is retained for the shortest period possible, as set out in the Records Management Guidelines.

PAS retains individual competition application forms for up to three years from the closing date for receipt of applications for the particular competition. If an applicant wishes to continue to retain access to their individual application, they must save the form to their device as it will no longer be accessible on their *publicjobs* account after the period of three years has elapsed. In the meantime, applicants may delete their competition application forms at any via their publicjobs.ie account. It is important to note that if a candidate deletes their application or profile while taking part in an active competition, they will automatically be removed from that particular competition and will receive no further consideration.

Principle Six

Personal data shall be processed in a manner that ensures the appropriate security of the personal data, including protection against unlawful or unauthorised processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures

High standards of physical, technological and organisational measures have been put in place to protect the security and confidentiality of personal data. The measures that are in place are listed below. A high standard of security is expected of all staff members and board members/assessors/invigilators in respect of processing personal data. These include, inter alia:

- Compliance with our Information Security Policy which is regularly updated and is available to all staff on the Intranet
- Compliance with our Security Policy
- Keeping premises secure, especially when unoccupied (our building can only be accessed by staff swipe card or through the Careers Store where visitors must sign-in and then be accompanied by a staff member; board members and candidates register with the reception desk on the first floor; the building is checked and locked each evening by an appropriate officer and there is an alarm system in place)
- Board Members/Assessors/Invigilators receive training regarding the importance of data security, are required to sign a confidentiality agreement before the assessment process begins. While working remotely, Board Members are not generally permitted to print documents, and where this is unavoidable (for example the PAS Representative may need to take notes of the process), PAS has supplied a lock box to ensure that any papers held outside the office are inaccessible. All papers processed outside of the office are securely couriered to the Board Members home, and are couriered back to Chapter House when the assessment process has concluded
- Compliance with all guidance in relation to working remotely issued by the DPO, including the following documents
    - Tips for remote interviewing
    - Working remotely using Sharefile
    - Remote working using a VPN or Citrix

    - Tips to avoid a data breach when working from home
- Inserting appropriate data protection and confidentiality clauses in arrangements with any processors of personal data on the organisation's behalf, including
    - the conditions under which data may be processed
    - the minimum security measures that the data processors must have in place
    - mechanisms or provisions that will enable the data controller to ensure that any data processor is compliant with the security practices which include a right of inspection or independent audit
    - Standard Contractual Clauses ensuring data which must be processed outside of the EEA is processed in line with the requirements of the GDPR (where appropriate).This takes the form of a Data Processor Agreement, and must be agreed before processing can take place.

Responsibility for the above is assigned to the relevant functional manager. Periodic reviews of the measures and practices in place will be carried out by a staff member nominated by the Data Protection Officer.

As part of our commitment to protecting the data we hold, PAS retains backups of all critical data in multiple locations. Our primary data backups are retained onsite on local disk storage. A secondary copy of our backups is stored in the public Cloud for disaster recovery purposes. Backups to the Cloud are encrypted in transit and at rest. All Cloud based backups are stored in data centres located within the European Union.

Principle Seven

The Controller shall be responsible for, and be able to demonstrate compliance with, the Principles

PAS has a Data Protection Unit in place to enable us to monitor and ensure compliance with data protection legislation and principles. The Data Protection Officer (DPO) regularly audits, or has a nominated staff member audit, each business area to measure compliance. Policies, including this Code of Practice, are reviewed and updated every six months to ensure the most up to date information is reflected. The ROPA and the Retention Schedule are also regularly reviewed.

The DPO attends training courses for Board Members to offer guidance on data protection, and delivers specific training to PAS staff including a session on these principles and how they apply to PAS. A Data Protection Liaison Officer network is maintained throughout PAS, reporting to the DPO on data protection matters.

The DPO may be contacted directly for evidence of PAS's compliance with the above mentioned Principles by making a request in writing, or emailing dpo@publicjobs.ie.

4. Subject Access Request Policy

PAS is aware of its obligations as a data controller with primary responsibility for, and a duty of care towards, the personal data within its control. Our obligations are set out in the legislative framework outlined in Section 2, above.

Data subjects whose personal data is held by PAS are entitled to ask PAS and receive confirmation as to whether or not personal data concerning them is being processed. Where that is the case, data subjects are entitled to access their personal data. Data subjects may also avail of the following rights in relation to their personal data;

- To be advised of the purpose(s) of processing said data
- To be advised of the recipients or categories of recipients to whom personal data has been or will be disclosed
- Where possible, to be advised of the envisaged period for which personal data will be stored, or if not possible, the criteria used to determine that period (e.g. if the information will be provided to the National Archives)
- To request the rectification of personal data where it is incorrect or misleading
- To request the erasure of their personal data (where possible)
- To request to restrict the processing of their personal data, or it object to its processing
- The right to lodge a complaint with the Data Protection Commissioner
- To request, where the personal data is not collected from the data subject, any available information regarding the source of this data
- The right to be informed of the existence of automated decision-making (including profiling) being operated on the data subject's data (where relevant), to include meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject. It should be noted that at present, no automated decision-making is operated by PAS
- To be advised of, where personal data is transferred to a third party, the appropriate safeguards pursuant to the GDPR relating to such transfer.

Individuals may exercise any or all of these rights by making a Subject Access Request (SAR).

Form of the Request

The subject access request should be made in writing, and should include sufficient information to identify the data subject to our reasonable satisfaction so we can verify that we are not releasing your data to someone who is impersonating you. PAS has a Subject Access Request Form available on publicjobs.ie in order to facilitate these requests administratively and to advise the requester of the type of evidence required by PAS, though completion of this form is not mandatory in order for your request to be accepted. When the criteria are satisfied, we will be in a position to commence the work involved in responding to your request. PAS will strive to respond as quickly as possible and in any event without undue delay, but if we have not been able to complete our work in that regard within one calendar month we will update you as to the progress of our response to your request, and may request an extension.

It should be noted that during the Covid-19 crisis, access to the PAS Office is strictly limited, and it is not currently possible to conduct searches for paper or hard-copy records which may be stored in Chapter House. In such cases where this is relevant, PAS has conducted all relevant searches and provided all information available electronically, and intends to conduct searches of hard copy records as soon as the offices are safely accessible.

Communicating with the Data Subject

PAS will communicate directly with the data subject once a valid subject access request has been received. This contact may help you specify the exact information you wish to receive. You can help us to expedite responding to your request by giving us as much information as possible about the data you are seeking access to and limiting the range, scope and time of data sources you wish us to search as much as possible. If you wish to receive a copy of everything we hold about you, then we will fulfil a complete and exhaustive search of all relevant data in PAS 9subject to the Covid-19 restrictions outlined above).

Systems Search

Unless there is a legitimate option to reduce the scope of the request (such as Covid-19 restrictions impeding our ability to conduct paper searches), a search of all databases and all relevant filing systems which are relevant under the GDPR will be carried out throughout PAS.

PAS will organise the response to the request by giving one or more individuals (the Data Protection Liaison Officers) the responsibility for conducting searches of their relevant filing systems and databases. A response to the request will be directed, co-ordinated and provided by the Data Protection Unit, who have responsibility for issuing such responses.

Manual Files

All relevant manual files (as set out in the Records Management Guidelines) will be searched for your data.

Restrictions Following Receipt of a Request

Compliance with GDPR and related legislation is not intended to interfere with the normal running of PAS business, and following receipt of a valid request, we are permitted to make changes to the requested information in the normal course of operation (provided no changes are made because of the request itself). This includes the correction of incorrect data, where discovered.

Third Party Personal Data

Once the personal data relevant to your request has been collected, we will consider our obligations to other data subjects who may be referred to in the same records. The person(s) preparing our response will consider the rights of third parties and any obligations of confidentiality which may apply, in addition to any relevant exemptions under GDPR. Where the identity of third parties would be disclosed in data which related to you, we may either blank out (redact) that data to protect the privacy and confidentiality of such third parties, or we may provide you with an extract from the data instead of the original source material.

Exemptions

Some material is exempt from inclusion in the response to a subject access request. This includes the content of negotiations with the data subject, and information which is subject to legal professional privilege. It also includes information relating to ongoing professional investigation or determination processes. If we are negotiating with you at the same time you make a subject access request, we do not have to reveal requested information if to do so would be likely to prejudice those negotiations. Once the negotiations are complete and put into effect, the file again becomes subject to GDPR.

Emails are subject to subject access, as are archived computerised and manual data held in a relevant filing system. CCTV footage will be included within the scope of request, where required.

Subject Access Requests cannot be used to infringe trade secrets or intellectual property rights. PAS therefore will not release test material or scoring keys to candidates as part of a Subject Access Request.

Where personal data contains health information, there may be a duty on PAS to consult an appropriate health professional before information can be disclosed. This is to avoid disclosing information about adverse health conditions to a data subject where the disclosure may be harmful or distressing to the data subject or another person. This does not apply where the data subject already had access to, or supplied, the information.

We recognise that failure to respond to your request within the requisite period gives rise to the ability of the individual to complain to the Office of the Data Protection Commissioner, and may give rise to an investigation by the Commissioner. We will do our best to ensure that all subject access requests are handled efficiently and effectively at all times and we appreciate your co-operation and assistance in vindicating your rights under GDPR.

Form of Response

PAS will provide the data subject with any relevant data in response to a subject access request in electronic format. If you do not wish to receive our response to your request by email, please let us know in advance. Once our response to your subject access request has been finalised, we will make a full copy of the material to be retained for our own reference. These records will be used as a reference should there be any dispute as to the content or timeliness of the response provided. It will be retained for seven years.

Any individual may apply at any stage (to the Data Protection Officer or the relevant Unit within PAS, as indicated in Section 2 above) to have any personal information held by PAS updated or corrected, if the individual believes that any information held is incorrect.

5. Responsibility of PAS Staff

All staff members of PAS have a duty to ensure compliance with the principles of Data Protection and undertake to follow the provisions of this Code of Practice in accordance with our policies and procedures.

All staff members are charged with the responsibility of ensuring that all data that they access, manage and control as part of their daily duties is carried out in accordance with the GDPR and this Code of Practice. Regular training is held to ensure that staff are reminded of these obligations and responsibilities.

Staff members found to be in breach of data protection legislation either purposefully or due to negligence may be found to be, in certain circumstances, committing an offence under GDPR. All current and former staff members of PAS may be held accountable in relation to all data processed, managed and controlled by them during the performance of their duties in the organisation.

Breaches of this Code are subject to appropriate action under the Disciplinary Code. Staff members should also note the content of the Code of Standards and Behaviour and the Guidelines for this Office, and in particular the requirement therein only to access information which is required in the course of their work, not access information in relation to colleagues or acquaintances (or other not for work purposes) and not to discuss any candidate with, or disclose personal data to, anyone other than staff members who are working on the particular competition the candidate is taking part in (or other relevant staff, such as a Formal Reviewer or Data Protection co-Ordinator, as appropriate).

Audits of Data Protection and Code of Practice Procedures

When determining their work programme (in consultation with the CEO), the PAS Internal Audit Committee will ensure that the programme contains adequate coverage of areas within PAS which are responsible for the storage, handling and protection of personal data. The particular focus of any review will be on assessing the adequacy of the control systems designed and in place in these areas for the purpose of minimising the risk of any breach of data protection regulations. Risks associated with the storage, handling and protection of personal data are included in our Corporate Risk Register. External audits of all aspects of Data Protection within PAS may be conducted on a periodic basis by the Office of the Data Protection Commissioner.

Protocol for Reporting Breaches

If any breaches of data protection regulations or of this Code of Practice are committed, our Breach Management Plan must be followed.

A Breach Notification Form is available on the PAS intranet, which requires staff to provide the information required by the Data Protection Commission to the DPO when reporting a breach. The Form must be submitted without delay, and no later than within 72 hours of the breach being discovered. A member of the Data Protection Unit will then contact the relevant staff member to clarify any information required, and report the breach to the Data Protection Commission. A template breach notification email is also on the intranet, and staff will be asked to complete this or otherwise advise all data subjects impacted by the Breach, as appropriate.

Data Protection Awareness

PAS is committed to ensuring all staff are aware of their Data Protection obligations generally and the requirements of this Code specifically. This includes:

- Staff training and awareness raising on the contents of this Code and Data Protection legislation
- Information available on the Intranet in relation to data protection
- Coaching/training all new staff on the contents of this Code before they are given access to personal information
- Regular reports to the Management Board on data protection matters
- The use of further staff communication resources as required on an ongoing basis.

Monitoring and Review

All managers are responsible for ensuring the implementation of this Code in their unit and raising awareness of data protection on an ongoing basis with their staff. All staff are responsible for adhering to this Code at all times. Managers are also responsible for complying with the data protection audits which are conducted every two years and addressing any issues which arise in those audit (or at any other stage as issues come to light). The onus is on Managers to bring data protection related concerns to the attention of the Data Protection Officer as they arise. They should also raise such issues with their colleagues through the regular Leadership Team meetings or through the Quality Group.

The Code will be reviewed every year (by the Data Protection Officer) and the most up-to-date version will be available on the People & Culture and Data Protection Knowledge Hubs on the intranet at all times. The revised Code will be approved by the Senior Management Team. This Code is effective from February 2021 and will be reviewed in January 2022.

Appendix 1: Definitions of Data Protection Terms

GDPR – The General Data Protection Regulation. This is an EU Regulation which replaced the previous Data Protection Directive and came into effect on 25th May 2018. It is an EU Regulation and therefore is directly effective. It was intended to harmonise privacy laws in the EU and allow data transfers to occur safely and without administrative difficulties within the EEA.

Data Protection Act 2018 – This Act was introduced in May 2018 in order to give full effect to the GDPR in Ireland. It contains specific provisions for data processing in an Irish context.

Personal Data – Any information relating to an identified natural person who is or can be identified, directly or indirectly, in particular by reference to an identifier such as a name, identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identify of that natural person.

Subject Access Request – this is where a person makes a request to the organisation for the disclosure of their personal data under GDPR.

Data Processing - any operation or set of operations which is performed on personal data, or on sets of personal data including the collection, recording, organising, structuring, storage, adaption or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, or erasure or destruction of same.

Data Subject – an individual who is the subject of personal data.

Data Controller - a person who (either alone or with others) determines the purposes and means of the processing of personal data.

Data Processor - a person or body who processes personal information on behalf of a data controller. A Data Processor Agreement will form part of the Contract Terms and Conditions in relation to the provision of services for all Data Processors used by PAS.

Special Categories of Personal Data – includes personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health data, data concerning a person's sex life or sexual orientation. Special rules apply to the processing of this data as it is particularly sensitive.

Pseudonomysisation – removing all personal identification factors from personal data so that an individual can no longer be identified directly, but keeping a method of reintegrating that data so that the Controller may associate the data with a specific individual if required (e.g. referring to a candidate by Candidate ID only).

Automated Decision Making and Profiling – automated individual decision-making means making a decision solely by automated means without any human involvement. Profiling means using personal data to evaluate certain things about an individual. Profiling can be part of an automated decision-making process. Only profiling that is based on purely automated processing, i.e. without meaningful human intervention, and which produces "*legal*" or "*similarly significant*" effects on a data subject is generally prohibited under Article 22 GDPR. In all other cases of profiling, the general provisions of the GDPR apply.

Appendix 2: Enforcement of Data Protection Legislation

Data Protection Commission

The Data Protection Act 2018 established the independent Office of the Data Protection Commission (DPC). The DPC currently has one Commissioner, who was appointed by Government. The DPC is independent in the performance of its functions. The DPC is responsible for ensuring that those who process personal data in Ireland do so in compliance with data protection legislation.

The DPC has a wide range of enforcement powers to assist in ensuring that the principles of Data Protection are being observed. These include but are not limited to the serving of legal notices compelling a data controller to provide information needed to assist their enquiries, compelling a data controller to take action to comply with data protection law, and issuing a fine for non-compliance. The DPC can obtain information, enforce compliance, prohibit overseas transfers of date, and enter an office to examine data. The DPC also has prosecution powers.

The DPC investigates complaints made by the general public in relation to personal data and has wide powers in this area. For example, the DPC may authorise officers to enter premises and to inspect personal information held on computer or relevant paper filing systems. Members of the public who wish to make formal complaints may do so by visiting www.dataprotection.ie and raising a concern, or by writing to the Data Protection Commission, 21 Fitzwilliam Square South, Dublin 2 D02 RD28.

Advice/Assistance

All requests for advice and assistance on data protection issues within the organisation should be directed to the Data Protection Officer.

Where employees of PAS, in the normal course of their duties, become aware that an individual (including employees of the organisation, Board Members/Invigilators/Assessors or suppliers operating on behalf of PAS) may be breaching data protection law or have committed or are committing an offence under the Acts, they should report the matter to the Data Protection Officer by emailing dpo@publicjobs.ie or writing to Data Protection Officer, Public Appointments Service, Chapter House, 26/30 Abbey Street Upper, Dublin 1 D01 C7W6.

Appendix 3: Associated Policies and Procedures

1) Data Security Policy

PAS has an obligation to keep personal data safe and secure and have appropriate measures in place to prevent unauthorised access to, or alteration, disclosure or destruction of that data, and against accidental loss or destruction in compliance with data protection legislation. It is therefore imperative that we have security measures and policies in place to ensure that only those staff members with a business need to access a particular set of personal or sensitive data are allowed to access that data.

This PAS Security Policy sets out who can access the various types of personal data in PAS, the procedures for handling personal data and for ensuring the security of personal data (both manual files and on IT systems). It also contains procedures for the transmission of data to other parties.

The implementation of this Policy is subject to audit by a staff member nominated by the Data Protection Officer and may also be the subject of an internal audit investigation and report to the Audit Committee at any stage.

Access

Staff in Recruitment and Selection Units have access to personal data in respect of candidates for competitions and prospective board members/assessors/invigilators. This data must only be used for the purposes of progressing a recruitment competition and must not be released outside of the organisation, or to anyone inside the organisation who is not involved in that particular recruitment competition, without permission from a senior manager.

Staff in support areas may have access to personal information on staff, candidates, board members/assessors/invigilators and suppliers, based on the function of the support area. This data must only be used for the purposes for which it was collected (contained in the relevant section of the privacy notice) and must not be released outside of the organisation, or to anyone inside the organisation who does not have a legitimate reason for possessing the data, without permission from a senior manager. All staff in People & Culture must sign a Confidentiality Statement.

All PAS staff are regularly reminded of the importance of confidentiality, and where appropriate are asked to sign a confidentiality agreement before being given access to certain personal data.

Procedures for Handling Personal Data (Manual Files and on IT Systems)

It is important that all personal data processed by PAS is used only for the purposes for which it was obtained and is kept confidentially in PAS. Where personal data is processed outside of the PAS Offices due to remote working, this data must be processed in accordance with the relevant policies and procedures in place to ensure appropriate levels of security are maintained. These policies and procedures are available on the eHub.

The following IT security measures are also in place and these procedures must be complied with:

(i) The Information Security Policy should be complied with at all times. PAS IT enforce a policy that requires a complex password for access to the corporate network. PAS have implemented a centrally controlled policy to force staff to change their network passwords regularly. The sharing of a user's individual network credentials is prohibited. Staff are required to lock or log off their pc when leaving their desk unattended, **including while working remotely** – all computers are set to lock automatically after 5 minutes.

(ii) Emails should be checked before sending to ensure they are addressed to the intended recipient and have the correct attachments (where appropriate)

(iii) Staff are required to ensure personal or confidential information is not displayed on computer screens in public areas of the office or in areas of their home which are accessed by other people

(iv) All personal and sensitive data held electronically is stored centrally. Access to both IT and Data Centre (hosts hardware and software on which personal data is stored) is restricted to staff in IT unit (swipe card required with IT access); access records and procedures are reviewed by senior management regularly

(v) PCs are disposed of securely using a specialist company; the hard drives shredded.

(vi) The permissions of shared drives are regularly reviewed and restricted where appropriate (e.g. staff that have moved units will have their permissions changed). It is the responsibility of the Line Manager to notify IT of any staff changes and to request access rights be changed

(vii) Remote access is only permitted through a secure encrypted channel using two factor authentication (*see paragraph below*)

(viii) Anti-virus and anti-spyware software is installed on all personal computers and laptops

(ix) Corporate firewalls are in place to prevent unauthorised access to office network.

(x) All computers and servers are regularly and centrally patched against latest known vulnerabilities

(xi) Access to systems which are no longer in active use and which contain personal data is removed where such access is no longer necessary or cannot be justified

(xii) Staff members who retire, resign or transfer from PAS will be removed immediately from mailing lists and access control lists. Relevant changes will also occur when staff are transferred to other assignments internally

(xiii) Personal or sensitive data held on applications and databases with relevant security and access controls in place (e.g. STAR) can only be copied to personal productivity software (such as word processing applications, spreadsheets, etc.) if it is copied into a directory to which only those working on a particular competition have access; this will be subject to audit and breaches may lead to actions under the Disciplinary Code.

(xiv) Personal data should not be stored outside of Citrix or VPN while working remotely; personal data should never be stored outside of shared directories (as outlined above)

(xv) For interviews or shortlisting exercises occurring in Chapter House, tablets may now be used for selection boards. This means that applications may be temporarily stored on ShareFile in preparation for the board meeting. The tablets must be stored securely in PAS, and when being issued to board members, the relevant unit must ensure that the tablet is received only by the person for which it was intended. The unit must also ensure that all tablets are returned to IT after the relevant board meeting and that the board member has logged out; expiration dates for board data must be set on ShareFile;

(xvi) Where interviews or shortlisting exercises are conducted remotely, the same security measures regarding Sharefile must apply. Board Members must confirm that any copies of candidate applications, scoring sheets or other assessment data are not stored on their personal devices once the assessment process has concluded. Any hard copy papers containing personal data (such as interview notes) must be securely couriered to the PAS Office on completion of the assessment process, and the Board Member must complete a cover sheet confirming that all

papers have been returned. Failure to comply with this procedure constitutes an offense under the Data Protection Act 2018, and may result in appropriate actions being taken by PAS and/or the Data Protection Commission.

(xvii) Other than as set out in (xiii) above, personal data must never be copied to portable storage devices such as laptops, memory sticks, etc. that may be stolen or lost; the following also apply to the use of portable storage devises:

1. Personal, private, sensitive or confidential data must never be stored on portable devices.
2. With regard to laptops, full disk encryption must be employed regardless of the type of data stored; staff are encouraged to exercise caution when accessing public Wi-Fi networks.
3. No confidential or sensitive corporate information should be accessed or transmitted over an unsecured public Wi-Fi network.
4. Passwords are enforced on smart phones and mobile devices and passwords used should be strong and secure as stated in the Information Security Policy
5. When portable computing devices or mobile phones are being used in public spaces or within a shared home environment, care must be taken to avoid unwitting disclosure of information, e.g. through overlooking or overhearing by unauthorised persons. **This includes by Alexa, Siri, or other virtual assistant technologies**
6. Each device is authorised for use by a specific named individual and responsibility for the physical safeguarding of the device will then rest with that individual
7. Laptops must be physically secured if left in the office overnight; when out of the office, the device should be kept secure at all times. Work laptops must not be used for personal purposes.
8. portable devices should never be left in an unattended vehicle
9. all mobile laptops are regularly called in for AV updates and patches (immediate compliance with this is required) and all have full disk encryption; USB devices are centrally controlled and restrictions are in place in relation to the use of USB devices; USBs are only used for non-confidential and non-personal information, e.g. public presentations).

Remote Access

Accessing data remotely must be done via a secure encrypted link or via Citrix or VPN.

Staff are expected to comply with this Code when accessing data remotely. If this involves downloading personal data on to your machine, you must save the completed document on the network and delete any information stored on your machine when you have completed your work. You must only use a machine (desktop PC, laptop, mobile phone or PDA) which is configured appropriately to PAS standards (e.g. with up-to-date anti-virus and anti-spyware software, full encryption, etc.) when remotely accessing centrally held personal or sensitive data. All wireless technologies/networks used when accessing PAS systems must be encrypted to the strongest standard available.

The above directions also apply to PAS Board Members or IT support consultants (if applicable and with appropriate permission) when accessing PAS systems remotely.

Appropriate Access and Audit Trail Monitoring

In order to capture instances of inappropriate access (whether internal or external), addition, deletion and editing of data, audit trails will be used as part of STAR.

The following procedures must be adopted in relation to manual records/paper files:

- Board members must be asked to sign a "Confidentiality Statement" and must be briefed by the PAS Representative on the requirement for confidentiality at all stages of the process. Assessors/Invigilators must also be asked to sign a "Confidentiality Statement" and be briefed by the relevant recruitment unit on the requirement for confidentiality.
- When interviewing in the PAS Offices, care must be taken to ensure that candidates and selection board members calling at reception are not allowed to view personal data on other candidates/other boards (this includes the names of other candidates) so care should be taken with the board folders to ensure they cannot be accessed, and care should also be taken when checking candidates in that they cannot view information on other candidates.

- When interviewing in the PAS Offices, all board papers must be taken from the board room when the board is finished, and the room must be locked if board papers are left unattended in the room at any stage.
- All board room keys must be handed into reception and the press where the keys are stored should be locked at all times when reception is unattended (e.g. overnight). The key to that press must be stored in a secure location.
- When assessing in the PAS Offices, care must be taken that candidates signing-in at test venues are not allowed to view personal data on other candidates (including names and candidate IDs).
- When assessing in the PAS Offices, personal information which is being destroyed (e.g. copies of application forms following shortlisting/interviews) should be placed in the Confidential Waste Bin only. It will then be shredded in-house or externally by a contractor who has in his/her contract agreed to the office's data protection procedures and ensure that the confidentiality of all personal data is protected.
- When in the PAS Offices and photocopying or printing personal information (e.g. application forms) care should be taken to ensure all copies are removed from the photocopying room.
- Personal and sensitive information must be locked away when not in use or at end of day (e.g. application forms, order-of-merits, confidential reports, etc.). This includes when working remotely.
- When assessing candidates remotely, all efforts should be made to ensure no paper records are created. Board Members are not permitted to print copies of documents sent to them via Sharefile; where this is unavoidable (e.g. where a PAS Rep must hand-write the notes of the assessment), the relevant papers will be brought to the home of that Board Member via a secure courier. The PAS Rep must store all papers in a lock box or other secure location inaccessible by other members of the household. No papers should be left out or visible to other household members. Once the assessment process has completed, the Board Member or PAS Rep must complete a cover sheet and advise PAS the papers are ready for collection. A courier will collect the papers from the home of the Board Member and return them securely to the PAS Offices
- Where a Board Member has printed papers or taken notes as part of a process which would normally be shredded in the PAS Offices, these papers must either be securely couriered to PAS for secure destruction, or, if appropriate, burned. **Disposing of these papers through any other means, including using a home shredder, will constitute a**

breach of these guidelines and may be considered an offence under the Data Protection Act 2018.

- Access to paper records and files containing personal data is restricted only to those staff with business reasons to access them (files are stored off-site in secure storage when not in use; files in use are stored in the section to which they relate). Requests for files stored off-site are sent to Business Support Unit and the person to whom the file is released is recorded.
- Access to files containing personal data will be monitored by supervisors on an ongoing basis and is also subject to audit at any stage.

The following procedures must be adopted for sending personal information outside of PAS:

- Personal information should not be sent to external parties unless it is absolutely necessary and complies with Data Protection Legislation; you must check with a senior manager before sending any personal information to persons outside of PAS.
- Personal information should not be sent by email unless it is encrypted, and customers should be informed that where possible they should not send in personal information by email; the disclaimer at the bottom of office emails advises customers of this*[1]. A DPIA has been conducted on the receipt of documents to verify identity and as part of the Clearance and Assignments process while working remotely and the process developed on foot of same must be followed exactly.
- The fax must never be used for transmitting documents containing personal data.
- You should ensure that the data will be delivered only to the person to whom it is addressed, and that all of the documents are returned and when no longer required are disposed of in the confidential waste.
- Internal post must be delivered only to the person to who it is addressed or to their manager if they are absent. While working remotely, all such post is scanned by a staff member from the Business Support Unit and sent via email to the person to whom it was addressed.

1

If data is being sent via standard email to an individual there should be a clear understanding and acceptance by the recipient of the risk involved in transmitting personal and sensitive data using this technology. There is a statement on our website that personal and sensitive data should not be sent to us by email.

- If a request is received from another organisation for access to personal data, you must consult a senior manager who will decide whether releasing the information is justified. The senior manager will consult the Data Protection Officer for advice if necessary.
- Contractors, consultants and external service providers (including on-line test providers) contracted by PAS will be subject to strict procedures with regard to accessing personal data by way of formal contract in line with the provisions of the GDPR. The terms of the contract and undertakings given are subject to review and audit to ensure compliance.

Transfers of data should take place only where absolutely necessary, using the most secure channel available. To support this, PAS staff should adhere to the following:

- Data transfers should, where possible, only take place via secure on-line channels where the data is encrypted;
- Manual data transfers using removable physical media (e.g. memory sticks, CDs, tape, etc.) should not take place; if a senior manager decides that this must take place the data must be encrypted using the strongest possible encryption method available. Strong passwords/passphrases must be used to encrypt/decrypt the data; any such encrypted media should wherever possible be accompanied by a member of staff, be delivered directly to, and be signed for by, the intended recipient. Care should be taken to ensure that the password is sent securely to the intended recipient and that it is not disclosed to any other person; if the data is being sent by registered post/courier there should be a clear understanding and acceptance by both senders and recipients of the risk involved in transmitting personal and sensitive data using this technology.
- When a data transfer with a third party is required (including to/from other Government Departments/Offices and with on-line test providers), a written agreement should be put in advance of any data transfer (a Data Processing Agreement). Such an agreement should define, where required;
    - The information that is required by the third party (the purposes for which the information can be used should also be defined, if the recipient party is carrying out processing on behalf of PAS)
    - Named contacts in each organisation responsible for the data
    - The frequency of the proposed transfers
    - An explanation of the requirement for and legal basis of the transfer
    - The manner in which the transfer(s) will be carried out, including encryption level used

- The acknowledgement procedures on receipt of the data
- The retention schedule for the data (both for PAS and the third party)
- Confirmation that the information will be secured to at least the standard that PAS applies, and in line with the requirements of data protection legislation
- Confirmation as to the point at which the third party will take over responsibility for protecting the data
- The method of secure disposal of the personal data by the third party, and the timeline for said disposal
- The method by which data breaches by the third party will be notified to PAS
- For data controller to data controller transfers (rather than where PAS is the data controller and transfers data to a data processor operating on PAS's authority), it must be clear that only the data necessary to meet the purpose of the transfer is provided
- Clarification must be obtained from the Data Protection Officer that such transfers are legal, justifiable and proportionate to the purpose(s) of the processing
- Particular attention should be focussed on data made available to third party processors who are based outside of the EEA and/or who are processing special categories of data or other sensitive information (such as test providers). Live data

Staff, board members, assessors and invigilators are also instructed not to speak about confidential information in public or to mention PAS or any PAS related data when using social media. Guidelines for assessing remotely have been provided to all Board Members who are involved in remote assessment and compliance with this guidance is mandatory.

2) CCTV Policy

Chapter House has a CCTV system in place for security reasons in all of the lift lobbies, stairwells and the basement. Cameras are also present at the reception desk and facing inside Chapter House from the Luas stop. CCTV cameras have been installed in the Smart Centres, 1st Floor Reception, certain corridors surrounding the Interview Rooms on the First Floor in order to ensure the safety and security of personnel and assessment material. It must be noted that all other cameras which may be present in or around Chapter House are not operated by PAS and are therefore not subject to this policy.

Footage will only be made available on the approval of senior management to identified PAS personnel, or to external parties (e.g. An Garda Síochána) in relation to the investigation of certain incidents which are outlined in the following paragraph.

CCTV footage may be accessed by this Office in the interests of

- Preventing or investigating interference with property, or harm to persons in the Office
- Ensure the safety and security of assessment material or the assessment process
- Health and safety
- Helping investigate any complaints involving harm to persons or interference with property.

This footage may also be used in relation to any of the above areas and to assist with any criminal investigations. Footage will only be used to assist with serious issues which may occur.

Footage may also be used to assist with responding to issues raised in a candidate's requests for a review of a decision made by PAS in relation to the assessment process. This will be determined on a case by case basis and will only form part of the review process where strictly relevant and necessary.

PAS does not allow the use of any other type of recording equipment on its premises to protect the privacy of staff and customers and the integrity of our assessment material.

Security and Retention Arrangements

CCTV footage is recorded on a hard drive which is retained for one month (before it is recorded over by new footage).

Footage which is extracted for purposes referred to above may be retained for longer periods as part of legal/disciplinary investigations. The footage will be viewed by Business Support staff as required. A limited number of those staff members have access to this data.

The computer on which the data can be viewed is password protected and only security staff have access to this data. The hard drives are stored in secure locations.

Third Parties to Whom the Data May be Supplied

The potential third parties are set out above.

Requests for copies of CCTV footage from An Garda Síochána (or other regulatory or investigatory bodies) will only be acceded to where a formal written (or fax) request is provided to the Data Controller (PAS) stating that An Garda Síochána (other body) is investigating a potential breach of the law. To expedite a request in an urgent situation, a verbal request may be sufficient to allow for release of the footage. However, any such verbal request must be followed up by a formal written request. A log of all such requests will be maintained by the Data Controller. Any such requests must be on headed paper and quote the details of the CCTV footage required and the legal basis for the request.

If An Garda Síochána make a request to view footage on the premises without requesting a copy, this may be acceptable without a written request.

Data Protection

CCTV footage will not generally be provided as part of a Subject Access Request response, as the data is not stored long enough to generally be extracted as part of such a request. Where a data subject specifically requests access to such data, and if the request is made within the retention period of that data, it may be possible to provide the data subject with a redacted copy of the relevant footage. The footage will be redacted to ensure only the relevant data subject is identifiable, and the redaction will be carried out by a third party expert in this area, who will be required to agree to appropriate confidentiality agreements before the raw footage is provided to them.

Any enquiries as to the processing of personal data relating to CCTV footage should be directed to dpo@publicjobs.ie.

3) Records Retention Schedule

Type of File / Record	What is included on File / Record	Retention Period
Competition File (Physical)	As per Competition File Checklist	Indefinite – transfer to National Archives
Other Competition Documents	Board members notes not forming part of the official record (i.e. not the notes taken by PAS Representative) and duplicate applications/other duplicate records	Destroy once board report has been prepared
Competition Documents (Electronic)	Board Member Correspondence, Supplementary Applications, other documents containing personal information	Three years
Competition Documents (Electronic)	General competition related documentation containing no personal information or templates with personal information deleted	Indefinite
Clearance & Assignments File (Physical)	As per Clearance & Assignments File Checklist	Three years
Requests for Reviews (Electronic)	Request received; acknowledgement; response from PAS; all associated research	Three years (unless there is a legal case underway)

Type of File / Record	What is included on File / Record	Retention Period
STAR Information – non personal	All non-personal information on STAR	Retain indefinitely
STAR Information –personal	All personal information on STAR (candidate application data including title, name, phone number(s), email address, postal address, gender, PPNS, date-of-birth, qualifications, work experience); CVs and Personal Statements for some competitions; assessment details and scores*; interview details and scores*; assignment details*; correspondence to candidates message board)	Indefinite; can be deleted my candidates themselves; *where a candidate has progressed through a selection process this information will be anonymised rather than deleted unless it forms part of the Competition File for transfer to the National Archives
Personality Questionnaires	Reports based on responses provided by candidates	2 years
Verbal References (for competitions with one vacancy only)	Record of all verbal references provided	3 months
Verbal References (for competitions with a panel)	Record of all verbal references provided	Lifetime of the panel
Hospital Consultant Referee Report	Reports on Training and Relevant Experience	1 year

Type of File / Record	What is included on File / Record	Retention Period
Special Accommodations Documentation	Record of candidate name and number, details on disability for which accommodations are required, photocopy of original medical reports, accommodations agreed, competitions applied for	Records on candidates retained indefinitely Photocopies of Medical Reports retained for 3 years; candidates will be reminded every three years that PAS is retaining this data and the candidate can request PAS delete this information at any stage
Scripts, Presentation Exercises, Work Samples, other written assessments	Candidate number/name, candidates own work on these exercises	Securely destroyed one year after the panel is exhausted
Assessors notes in relation to Scripts, Work Samples, other written assessments	Candidate number/name, assessors notes and comments on these exercises	Securely destroyed one year after the panel is exhausted; breakdown of scores retained on the Competition File
Assessor notes from presentation exercise	Candidate number/name, assessors notes & marks and comments on these exercises	Securely destroyed one year after the panel is exhausted; breakdown of scores retained the on Competition File

Type of File/Record	What is included on File/Record	Retention Period
Website Registration / Profile	Username, Candidate I.D., Title, Name, Address, Phone Number(s), Email Address, Postal Address, Date-of-Birth, Highest Qualification, Career Level, Special Needs, Job Alerts, Job Category, Job Sub Category	Information to be retained indefinitely. Candidates will have the option to delete their profile.
Google Data Analytics used to help analyse how users use Publicjobs.ie. This analytical tool uses cookies to collect standard internet log information and visitor behaviour information in an anonymous form.	• The name of the domain from which you access our site • The date and time you access our site • The Internet address of the website from which you linked directly to our site.	50 months
Psychometric Tests	Candidate name and number and candidate scores	Full data to be retained for as long as campaign is active. Historical data to be anonymised and retained indefinitely.
Bespoke Tests	Candidate name and number; candidate responses and scores	Full data to be retained for as long as campaign is active. Historical data to be anonymised and retained indefinitely.
Testwise (PAS in-house testing system)	Candidate name and number; candidates' responses to each question for some tests, candidates' scores	Full data to be retained for as long as campaign is active. Historical data to be anonymised and retained indefinitely.
Candidate Feedback	All requests for and responses to candidates in relation to assessment feedback	Securely destroyed one year after the panel is exhausted

Type of File/Record	What is included on File/Record	Retention Period
Equal Opportunities Data	Information gathered at exam stage in relation to specific grounds from the Equality legislation.	Information retained for statistical purposes
Irish Interview Results	Candidate and board member's names; results/scores of Irish Interview	Indefinite – retained on relevant Competition File
Video Interview records	Candidate's video interview	One year after the panel is exhausted
Remote Proctoring records	Record of candidate's test sitting	One year after the panel is exhausted
Documentation collected from candidates called to interview who are not successful at interview	Copies of Certificates and identification documentation; Garda vetting application; Health and Character Declaration	Destroy immediately once final board report signed
Board Member / Assessors / Invigilators Questionnaires and Details	Contact details (title, name, phone number(s), email address; postal address); service on selection boards; relevant training and experience where provided; CVs where provided. For those who are paid – bank account details, PPSN, tax credits and record of all payments.	Indefinite – Personal Information on board members/assessors/invigilators will be retained indefinitely for current interview board members/assessors/invigilators. Reminders issued every two years of data held and that it can be deleted on request.

Type of File/Record	What is included on File/Record	Retention Period
Suppliers	Tax Clearance Certificate Electronic Format, via ROS; Company name, address and contact details; bank account information; records of all payments made	Supplier Forms and details and details of redacted bank details will be held indefinitely
Parliamentary Questions (Physical/Electronic)	Question asked, response submitted and any supporting material	3 years
Correspondence from TDs (Physical)	Question asked, response submitted and any supporting material	3 years
Personnel Files	Name, address, PPNS, contact numbers, sick leave record and medical documents, civil service career history, salary and superannuation details, contracts, record of annual and other types of leave or work-life balance; PMDS ratings; training records; live disciplinary or other investigation related documentation; merit awards, next-of-kin information, education and qualifications records.	Sent to new organisation on transfer; retained indefinitely for pension purposes

Type of File / Record	What is included on File / Record	Retention Period
PAS – Personnel Legacy System	Name, address, PPNS, contact numbers, sick leave record, civil service career history.	Indefinite for pensions purposes
Microfiche details for former staff	Name, address, contact numbers, sick leave record	Indefinite for pensions purposes
Staff Census Forms (Optional)	Disability status of staff on an annual basis – self declaration	Three years
Ethics in Public Office Returns (Physical)	Returns received from all relevant PAS staff / members of the PAS Board	15 years
Legal Files	Records of legal problem and legal advice sought and received	Indefinite – Transfer to National Archives
Policy Files	Documentation in relation to any policy decisions made by PAS and any discussions around those decisions	Indefinite – Transfer to National Archives
Validation / Trialling Data	Candidate ID, name, any equality data captured such as age and gender, test Scores, any assessment/ exercise scores, interview scores, scores from predictive criterion e.g. training scores or manager/supervisor ratings	Files need to be kept indefinitely but identifiers removed once analysis is complete

Type of File/Record	What is included on File/Record	Retention Period
Procurement Files (Physical)	As per Procurement Checklist on Intranet	7 years
Finance Files (Physical)	Staff Salary Files Fees and Travel Expenses for Board Members and Board of PAS	Indefinite
FOI (Physical)	FOI request and request for review (if appropriate); acknowledgement(s), response(s) from PAS, copies of all associated documents; all correspondence with the Information Commissioner	1 year unless the case has gone to the Information Commissioner; 2 years if case has gone to the Information Commissioner
Data Protection (Physical)	Data protection request and response	7 years
Complaints (Physical)	Request received; acknowledgement; response from PAS; all associated research	One year after the panel is exhausted
General Correspondence	Query and response	If by email retained in mailmeter for 3 years; otherwise 1 year
Emails	All emails received and sent	Retained for three years
CCTV Footage	All footage captured on PAS CCTV	30 days
Executive Assessment Reports	Report of candidate's executive assessment if called for final interview	3 months

Type of File / Record	What is included on File / Record	Retention Period
Correspondence / Meetings with the Department of Public Expenditure and Reform	Records of non-campaign specific correspondence and meetings with D/PER	Indefinite Information relating to specific campaigns should be retained indefinitely on competition files
Correspondence / Meetings with Local Government Management Authority (LGMA) and the County and City Managers Association(CCMA)	Correspondence / Meetings with LGMA and CCMA	Indefinite Information relating to specific campaigns should be retained indefinitely on competition files
Correspondence / Meetings with Clients	Correspondence / Meetings with Clients	Indefinite
PAS Board documentation Management Board documentation Senior Management meeting documentation Recruitment Management meeting documentation Internal Audit Committee documentation Risk Management Group	Documentation related to these committee/groups and official minutes of meetings	Indefinite
Quality Group documentation; Project Group documentation	Documentation related to these committee/groups and official minutes of meetings	Indefinite
Administrator Report Forms from Test Sessions	Notes on the testing session and any issues raised	6 months where there are no related requests for a review; 3 years where there is a related review

4) Competition File Data Retention

When a competition is deemed as “closed” or the panel exhausted, the competition files are to be prepared for transfer to Business Support Unit in PAS. Competition files will be stored for 30 years before being transferred to the National Archives to be permanently stored there. Please ensure the following instructions are adhered to before files are Put Away;

- Only completed and final versions of documents are retained (no draft or incomplete versions) for each stage of the competition process. Some competitions will not contain all the listed stages.
- All other documents that are not required on the file should be stored as a soft copy in the campaign folder for the length of time indicated on the Retention Schedule. These documents may include blank application forms, Advertisements, Board Member Contact Information and Letters, Competition Checklists and Campaign Statistics.
- Important letters, emails and other pertinent information which is not stored electronically should be retained in the back of the Competition File in a file pocket.
- All boxes to be Put Away must have a Box ID Number (Business Support Unit will allocate a specific ID number) and a printed list of all the competition files contained in the box should be fixed to the inside of the lid of the box.
- Label to go on each competition file with the date file put away and notice of no further processing on files – files are read only.

If you are unsure of any of the above when Putting Away files, please discuss with the Information Governance Representative from your Unit or the Records Manager in Business Support Unit.

Files that are Put Away cannot be amended at a later date except when complying with a request for data rectification, as provided for under the GDPR; information can be sought from these files for legitimate business purposes (such as requests for information to allow “professional added years” to be calculated – such files will only be released on the request of a recruitment / senior manager). Breaches of this legal requirement will be subject to the PAS Disciplinary Code.

Planning

Competition Request/Sanction/Statutory Request/Consultant Appointment Letter

SLA/Competition plan/ Proposal for Provision of Recruitment Services (agreed timescales, assessment methods to be used, additional publicity, etc.)

Agreed information booklet

Confirmation of invasive procedures EPP (Hospital Consultants Unit Only)

Proposed Interview panel nominations (agreed and signed)

Testing

All candidate test scores and order of merit (if applicable).

Shortlisting

Copy of ineligible message issued through STAR

Shortlisting guide (if any) ***Shortlisting Board Report – Bound***

Public Appointments Service Representative's Report
Signed Report of the Shortlisting Board (Confidential Report)
List of Candidates/Candidates Assessments at Shortlisting
Agreed Criteria
Confidentiality & Conflict of Interest Forms (signed)
Information Booklet

Copy of non-shortlisted message to candidates

Copy of message calling candidates to next stage

Preliminary / Main Interviews/Presentation Exercises/Other Tests

Interview Guide

Interview Board Report - Bound

Public Appointments Representative's Report
Signed Report of the Preliminary/Main Board (Confidential Report)
Signed Report from Presentation Exercises/Other Tests
Marking Sheet

Candidates Assessments

Confidentiality & Conflict of Interest Forms (if board members change from SL)

Information Booklet

Copy of message to unsuccessful candidates

Copy of message to successful candidates

Assignments

Ministerial Sanction

Recommendation Letters/Copy of Provisional Recommendations

5) Clearance and Assignments File Data retention (retained for 3 years)

Action Sheet

Original Application of candidate

Copy of Information Booklet

General Declaration/Statutory Declaration (if applicable)

Garda Vetting Report

Additional Security Clearance if applicable (name and all addresses sent to client organisation for clearance plus response received)

Foreign Security Clearance, if applicable

Health Declaration, Chief Medical Officer Clearance / Advice

Birth Certificate / Copy of Passport / Drivers Licence (where applicable)

Marriage Certificate (if applicable)

Certificates of Educational Qualifications of Professional Memberships (if applicable)

Employer/Other References

Workplace Accommodation Form (if required)

Health and Character Declaration

Risk Assessment Submission (if applicable)

Provisional Recommendation and Ministerial Sanction (if applicable)

Assignment notices to candidate

6) Privacy Statement

(1) Candidate Privacy Statement

Data Controller – Public Appointments Service, Chapter House, 26-30 Abbey Street Upper, Dublin 2

Data Protection Officer – DPO@publicjobs.ie

Legal Basis for Processing Data

The Data Protection Act 2018 provides that the processing of personal data shall be lawful where such processing is necessary for the performance of a statutory function of a controller. PAS is mandated by statute[i] to act as the centralised assessment and selection body for the civil service and to carry out all the procedures necessary to undertake the recruitment, assessment and selection of suitable candidates for appointment, therefore, the processing of personal data necessary for this purpose is lawful as Article 6(1) (e) of the General Data Protection Regulation (GDPR) and Section 71 (2) (a) of the Data Protection Act 2018 apply.

The Data Protection Act 2018 also provides a legal basis for the processing of "special categories" of personal data for the performance of a function conferred by or under an enactment. The information collected from applicants that falls within the "special categories" of personal data set out in Article 9 of the GDPR will be subject to a range of more stringent measures designed to safeguard the fundamental rights and freedoms of data subjects. This range of measures includes: obtaining the explicit consent of the data subject, pseudonymisation of data where possible, and includes strict time limits for the erasure of relevant personal data once the legal basis for processing that data has expired. The processing of any such data will be necessary, proportionate and undertaken in accordance with the principles of data protection with a particular focus on data minimisation. The specifics of the data collected by PAS which are included in the "special categories" of personal data and the processing thereof are explained further in the Code of Practice for the Protection of Personal Data, available at https://www.publicjobs.ie/documents/data-protection/Code-of-Practice-for-the-Protection-of-Personal-Data-in-the-Public-Appointments-Service.pdf

Categories of Personal Data Concerned

Personal data is collected on all candidates for competitions run by PAS in order to process their applications. This information is used by the relevant recruitment unit to run a recruitment and selection competition from application up to appointment in the case of a successful candidate. The data is collected primarily by means of an application form. This application is used to assess eligibility for a particular competition; determine preferences in relation to the location (if applicable); determine whether the candidate meets the shortlisting criteria (if applicable); and to aid the selection board in the interview/assessment situation (should the candidate be called to this stage). Information which is required to be provided by candidates as part of the application process includes their relevant qualifications and experience, and examples of the competencies required for the particular post; it also includes their name, address, contact details, and date of birth; (the date of birth is not shared with selection board members).

Other data collected is required to confirm that the candidate meets the essential requirements for the competition and for background checks conducted at clearance and assignments stage to ensure the person is suitable for appointment in respect of character and that he or she is fully competent to undertake, and fully capable of undertaking, the duties attached to the position. Data collected at clearance and assignment stage from those candidates under consideration for a position includes security checks and/or Garda vetting; employment or other references; health and medical information; health and character declaration; copies of relevant qualifications; proof of identification; workplace accommodation form (if such accommodations are required); drivers licence (if essential); and reports from the Chief Medical Officer (CMO) (if required).

Candidates may also be asked to provide equality monitoring information on a voluntary basis; this is used to ensure that our assessment processes are fair to all groups covered by the Equality legislation and processed only in line with our obligations for processing “special categories” of data.

PAS only keeps data for purposes which are specific, lawful and clearly stated. Personal data will only be processed in a manner compatible with the stated purpose and information collected from candidates will only be used in order to process their application for a specified competition.

Regular audits are conducted on all personal information collected from all sources. This establishes that there continues to be sound, clear and legitimate purposes for collecting all of the information currently collected. These audits are conducted on an ongoing basis by a nominated staff member

for the Data Protection Officer. The findings are reviewed by the Risk Management Group, who report to the Management Board.

All data is obtained and processed in compliance with the General Data Protection Regulation (GDPR) and the Data Protection Act 2018; PPSN are only requested where required in order to support the provision of a public service to a customer (i.e. for recruitment and selection purposes).

Information on Cookies is provided in a separate statement on the Data Protection page of publicjobs.ie, available at https://www.publicjobs.ie/documents/Cookies-Policy.pdf

Recipients or Categories of Recipients

Examples of legitimate disclosures specific to PAS are listed below:

- Information on candidates who are being offered appointment is provided to the client organisation (this includes contact details and information in relation to the candidate's qualifications/experience for the post);
- Material is provided to the Chief State Solicitor and any of their legal advisers, and to the Workplace Relations Commission (or other appropriate body) as required in the event of a case being taken against PAS;
- National Archives disclosures are set out in the Code of Practice for the Protection of Personal Data;
- Certain data is disclosed to assessment providers who carry out some of the assessments run by PAS; only the minimum amount of personal data is disclosed to allow them to fulfil their functions as data processors (name, email address and PAS candidate identification number);
- Where a candidate requests a review by the Commission for Public Service Appointments in relation to an alleged breach of the Code, or appeals a decision under the Freedom of Information Act to the Information Commissioner, the information requested by these bodies is provided to them in order for them to respond to the candidate's request for a review;
- PAS use external selection board members/assessors/invigilators and these board members/assessors/invigilators may receive, or have access to, candidate application data in order to assist in the determination of suitability for a specific role; selection board members/assessors/invigilators have a duty to keep such information confidential and secure;

- Information is provided to the CMO where PAS has concerns in relation to a candidate's suitability for appointment on health related grounds (as the CMO provides the occupational health service for PAS);

- Some organisations (which are involved with the security of the state) may require that candidates assigned to them have additional security clearance conducted; the names and addresses of those candidates are sent to the relevant client organisation for processing.

- Non Consultant Hospital Doctors' applications are collected for the HSE through our recruitment application;

- The results of State Board's assessment processes are sent to the appropriate Department in order for the Minister to make a decision.

Period for which personal data will be retained

The Record Retention Schedule (available at https://www.publicjobs.ie/documents/data-protection/Records-Retention-Schedule.pdf) sets out the retention period for all items of personal data kept. Necessary approval has been sought from the Director of the National Archives to destroy electronic and physical records.

PAS retains individual competition application forms for up to three years from the closing date for receipt of applications for the particular competition. If an applicant wishes to continue to retain access to their individual application, they must save the form to their device as it will no longer be accessible on their *publicjobs* account after the three years has elapsed. In the meantime, applicants can delete their competition application form at any stage from their profile. Importantly, they should note that if they do so and are currently in an active competition, they will automatically be removed from that particular competition and will receive no further consideration.

Some data in relation to testing (test scores) are anonymised and retained for research, validation and statistical purposes. The minimum amount of data is retained for the shortest period possible, as set out in the Records Retention Schedule.

A record of candidate participation in a competition may be retained for archiving purposes

Your responsibility

You can update your own profile at any stage and should do so as your circumstances change.

Subject Access Requests

PAS is aware of its obligations as a data controller with primary responsibility for, and a duty of care towards, the personal data within its control. Our obligations are set out in the GDPR and associated implementing and supplementary legislation in Ireland (Data Protection Act 2018).

Data subjects whose personal data is held by PAS are entitled to ask PAS and receive confirmation as to whether or not personal data concerning them is being processed. Where that is the case, data subjects are entitled to access the personal data as well as certain information in relation the processing of that data.

The subject access request should be made in writing, and should include sufficient information to identify the data subject to our reasonable satisfaction so we can verify that we are not releasing your data to someone who is impersonating you. When the criteria are satisfied, we will be in a position to commence the work involved in responding to your request. PAS will strive to respond as quickly as possible and in any event without undue delay, but if we have not been able to complete our work in that regard within one calendar month we will update you as to the progress of our response to your request. The Subject Access Request Form is available on the Data Protection page of publicjobs.ie at https://www.publicjobs.ie/en/data-protection

PAS will provide the data subject with any relevant data in response to a subject access request in electronic format. If you do not wish to receive our response to your request by email, please let us know in advance. Once our response to your subject access request has been finalised, we will make a full copy of the material to be retained for our own reference. These records will be used as a reference should there be any dispute as to the content or timeliness of our response provided to you. It will be retained for seven years. Any individual may apply at any stage (to the Data Protection Officer) to have any personal information held by PAS updated or corrected (if the individual believes that any information held is incorrect/incomplete).

[1] Public Service Management (Recruitment and Appointments) Act 2004 (2004 Act), Section 34

(2) Selection Board Members/Assessors/Invigilators Privacy Statement

Legal Basis for Processing Data

The Data Protection Bill provides that the processing of personal data shall be lawful where such processing is necessary for the performance of a statutory function of a controller. PAS is mandated by statute to act as the centralised assessment and selection body for the civil service and to carry out all the procedures necessary to undertake the recruitment, assessment and selection of suitable candidates for appointment (Section 34 of the Public Service Management (Recruitment and Appointments Act 2004) (2004 Act) therefore, the processing of personal data necessary for this purpose is lawful as Article 6(1) (e) GDPR applies.

Categories of Personal Data Concerned

Information retained includes contact information and additional information which is required to make any payments to you. We also retain information on your training and experience where this is provided to us. PAS also retains information on all training carried out by PAS, including online training, face-to-face training and follow-up workshops attended by you.

Recipients or Categories of Recipients

Names of board members/suppliers and the extent of their services for PAS may be disclosed if asked for as part of a Parliamentary Question or FOI Request (however no sensitive personal information is disclosed)

Period for which personal data will be retained

This information will be retained indefinitely; it will be used only for the transactions being carried out in relation to your role as a selection board member/ assessor/invigilator and will be stored in a secure manner

Your responsibility

You are entitled to review and update the information which PAS holds on you at any stage. We would encourage you to ensure that when any of your details change you notify PAS, so that the information stored on you can be updated.

Anyone interacting by standard email should be aware that there are risks involved in transmitting personal or sensitive information using this technology (as email generally is not a fully secure method of sending data). Therefore, please do not send any personal or sensitive data by email / fax to this office.

Subject Access Requests

PAS is aware of its obligations as a data controller with primary responsibility for, and a duty of care towards, the personal data within its control. Our obligations are set out in the GDPR and associated implementing and supplementary legislation in Ireland.

Data subjects whose personal data is held by PAS are entitled to ask PAS and receive confirmation as to whether or not personal data concerning them is being processed. Where that is the case, data subjects are entitled to access the personal data as well as certain information in relation the processing of that data.

The subject access request should be made in writing, and should include sufficient information to identify the data subject to our reasonable satisfaction so we can verify that we are not releasing your data to someone who is impersonating you. When the criteria are satisfied, we will be in a position to commence the work involved in responding to your request. PAS will strive to respond as quickly as possible and in any event without undue delay, but if we have not been able to complete our work in that regard within one calendar month we will update you as to the progress of our response to your request.

PAS will provide the data subject with any relevant data in response to a subject access request in electronic format. If you do not wish to receive our response to your request by email, please let us know in advance. Once our response to your subject access request has been finalised, we will make a full copy of the material to be retained for our own reference. This records will be used as a reference should there be any dispute as to the content or timeliness of our response provided to you. It will be retained for seven years.

Any individual may apply at any stage (to the Data Protection Officer) to have any personal information held by PAS updated or corrected (if the individual believes that any information held is incorrect.