Code of Practice for the Protection of Personal Data in the Public Appointments Service

VERSION 8

PAS

May 2018

An tSeirbhís um Cheapacháin Phoiblí
Public Appointments Service

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.

Fiona Tierney
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 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.

The Data Protection Bill 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 GDPR will be subject to a “toolbox” of measures designed to safeguard the fundamental rights and freedoms of data subjects. The “toolbox” of measures includes encryption and pseudonymisation of data, obtaining the explicit consent of the data subject and includes strict time limits for the erasure of relevant personal data. The data processing must be necessary and proportionate and in accordance with the principles of data protection including data minimisation – i.e. that the data processing is limited to what is necessary for the purposes for which the data processed.

3. Code of Practice relating to 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 Six Principles set out in the GDPR, and they are: -

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 varies depending on the groups for which personal data is processed, these are set out below:

Candidates

The legislative basis for processing personal data from candidates is set out on page 5. 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 (it also includes their name, address 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 if 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 CMO (if required).

Candidates may also 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.

Prospective Candidates - On-line Registration with 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. 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 include:

- Username and password*
- Security Question*
- Title
- Name*
- Date of Birth
- PPSN
- Gender
- Email address
- Postal address
- Postcode
- Country*
- Daytime Phone Number*
- Other Phone Contact Number(s)
- Highest Educational Qualification
- Industry Sector
- Career Level

- Details of any accommodations required in the selection process
- Communications Language Preference
- Job Alerts

*Mandatory

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 changes depending on the requirements for each competition)
- Citizenship details (whether candidate is an EEA national or not)
- Employment History (including title, duties and salary)
- Details of specific experience where that is an essential requirement or is desirable
- 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

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.

On occasions, PAS uses data for research purposes in order to quality assure its assessment processes.

Selection Board Members/Assessors

Personal data is collected from all board members/assessors/invigilators in order to (i) determine the type of board/assessment process for which they might be suitable depending on qualifications, experience and training (this data is used to set board members/assessors/invigilators up on a database so that Recruitment Units can determine whether the qualifications/ experience of particular board members/assessor/invigilator would make them suitable for particular selection boards/assessment processes, and subsequently to book them) and also to (ii) pay fees/travel and subsistence to them, where appropriate; where board members/assessors are paid, bank account details are also collected (this data is used to approve board members/assessors for payment and by the Finance Unit to make the payments). Data on board member training is stored on our Learning Management System. Board members/assessors/invigilators are reminded every second year that we hold their personal data and that they can update it at any stage by contacting a named person in PAS.

Suppliers

Personal data is collected on all suppliers of goods and services in order that we can pay for the goods/services procured by electronic funds transfer and 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.

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 used by HR 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 HR or PeoplePoint at any stage.

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 keeps data for purposes which are specific, lawful and clearly stated and the data will only be processed 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. 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 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 a the lawful employer/employee relationship and to meet our statutory obligations to staff. The National Archives require PAS to submit competition files to them after 30 years. The competition files contain certain personal data, depending on how far the candidate has progressed in the competition process (see Appendix 4). Each candidate's test scores are captured and retained as part of the competition process. Candidates who progress to shortlisting stage will be included on the list of candidate presented to the shortlisting board which includes all candidate names and their most recent roles; the selection board members' assessment of their application will also be retained. At interview stage, each candidate's interview notes are retained and a copy of the marks awarded under each competency area. Scores will be retained for each candidate who completes an additional assessment process and where there is an assessment board involved, the notes of the assessment board will also be retained. Interview/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 includes, the candidate's name, address, date of birth, relevant qualifications and experience). All of this information will be retained indefinitely and ultimately sent to the National Archives.

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.

There are some transfers of personal data to agents who are carrying out operations upon the data on behalf of PAS and not retaining it for their own purposes and 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 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;
- ◊ 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 are 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 (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 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.
- ◊ 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 (as the CMO is the qualified 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.

- ◊ NCHD 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.

Regular audits are conducted on all personal information 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 (every two years) by a nominated staff member for the Data Protection Officer. The findings are reviewed by the Risk Management Group.

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

Principle Three

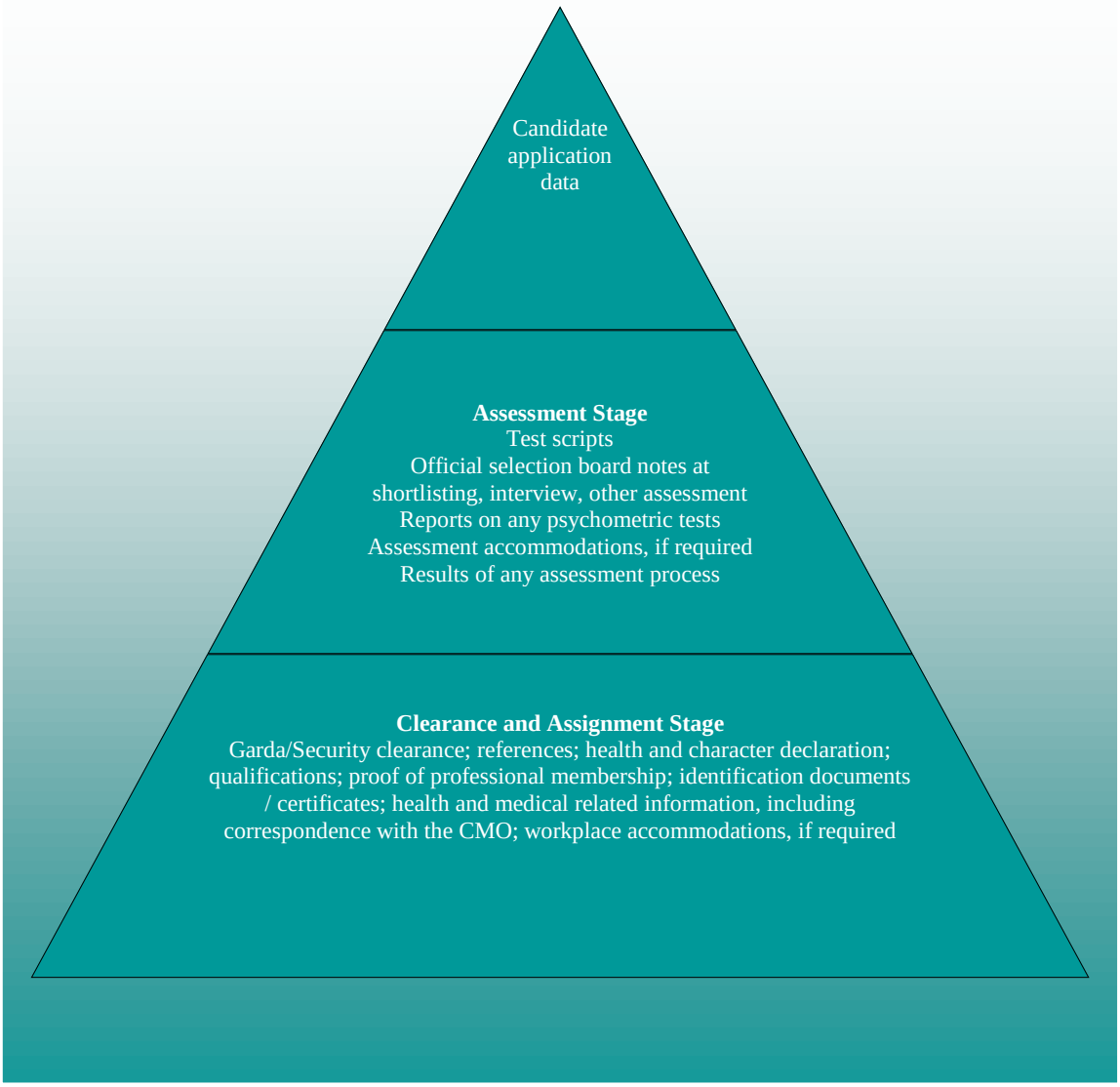
Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes

PAS collects the minimum amount of personal data to allow it fulfil its legislative remit. All new processes are reviewed to ensure that the amount of personal data to be collected is minimised. Data Protection Impact Assessments are conducted in advance of the implementation of new technology or processes, or the collection of new types of data, or when planning to make new disclosure of data. PAS adopts privacy by design approach at the planning stage of all new processes or services and conducts a detailed risk assessment exercise aimed at protecting the privacy of candidates and minimising the data we need to collect from candidates. Any actions arising from this risk assessment process will be included in the appropriate unit(s) risk register(s).

Section 24 (9) of the 2004 Act 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 if 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

Data may be processed in relation to the grounds set out in Equality legislation to ensure PAS processes are not unfairly impacting on any particular group. This is collected on a voluntary basis and therefore is subject to consent; it can be deleted or updated at any stage by the candidate themselves (through their profile). This may also be collected by the external test provider at testing stage on a voluntary basis.

Data may also be collected from candidate's who require accommodations as part of the assessment process. This includes a medical report. 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. 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.

The reason why the information is being processed is contained in the Privacy Notices for all groups on which we hold 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 sets out the retention period for all items of personal data kept 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. The PAS 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.

This office 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

Privacy Notices are in place for each group on which data is stored informing them what information is held on them and the reason for holding this information.

Most of the data held by PAS is supplied by the person themselves and can be updated at any stage by contacting PAS. Candidates have online access to change the information on them in 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.

Board members/assessors/invigilators are asked to contact our Recruitment Support Unit and staff members are asked to update their details on PeoplePoint and/or contact Human Resources with any changes and these are made immediately. Suppliers are deactivated on a regular basis if not used within the previous two years. All of these groups 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

Retention periods of personal data are set out in our Records Retention Guidelines. These are agreed with the National Archives. 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 Management Guidelines.

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; the high standard of security is expected of all staff members in this respect. 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);
- ◊ Inserting appropriate data protection and confidentiality clauses in arrangements with any processors of personal data on the organisation's behalf, including –
    a) the conditions under which data may be processed;
    b) the minimum security measures that the data processors must have in place;
    c) 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.

  This should be in the form of a Letter of Agreement/Contract with the processor (and included in the conditions section when issuing a request for tender).

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

PAS does not currently store any data in the cloud. Prior to any future decision to in relation to

such an option, a risk analysis will be conducted to ensure that the management team are satisfied that personal data will be secure if it is outsourced to a cloud provider. This will include being satisfied that the cloud provider will only process the data in accordance with PAS instructions, and that the cloud provider has taken *appropriate security measures against unauthorised access to, or unauthorised alteration, disclosure or destruction of the data.* Data will not be transferred outside of the EEA, and a written contract will be put in place with the cloud provider and any sub-processors to underpin the obligations as set out above.

Subject Access 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 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 the following information in relation thereto:

(i) The purposes of processing
(ii) The categories of personal data concerned
(iii) The recipients or categories of recipients to whom personal data has been or will be disclosed
(iv) Where possible. the envisaged period for which personal data will be stored, or if not possible, the criteria used to determine that period
(v) The existence of the right to request from PAS rectification or erasure of personal data or restriction of processing personal data concerning the data subject or it object to such processing
(vi) The right to lodge a complaint with the Data Protection Commissioner
(vii) Where the personal data is not collected from the data subject, any available information regarding the sources
(viii) The existence of automated decision-making (including profiling) being operated on the data subject's data, where relevant, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject
(ix) Where personal data is transferred to a third party the appropriate safeguards pursuant to the GDPR relating to such transfer.

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. 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.

Communicating with the Data Subject

PAS will communicate directly with you 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.

Systems Search

Unless there is a legitimate option to reduce the scope of the request, a search of all databases and all relevant filing systems (manual files) 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 responsibility for issuing requests for information throughout PAS and receiving all the retunes. The co-ordination of your subject access request will be the responsibility of such person(s).

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.

Third Party Data

Once the information has been collected, we will consider our obligations to other data subjects. 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 may provide you with an extract from the data instead of the original sources 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 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 cannot 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. 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.

It should be noted that where a request is made by, or on behalf of, a person seeking access to their own personal information under the Freedom of Information Act, this request should also be taken as a request under the Data Protection Acts. This is because a valid Data Protection request does not need to refer to the GDPR.

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.

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 policy 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.

Staff members found in breach of the Data Protection principles may be found to be acting in breach of or, 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 with, or disclose to, anyone other than staff members who are working on a particular competition.

Audits of Data Protection and Code of Practice Procedures in PAS

The PAS Internal Audit Committee, when determining in consultation with the CEO, the work programme of the Internal Audit Unit, 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 the Code of Practice or of the GDPR are committed, our Breach Management Plan must be followed.

Awareness Raising

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

- ◊ Staff training and awareness raising on the contents of this Code and GDPR;
- ◊ Making a Guidance Note available on the Intranet and included in awareness raising sessions;
- ◊ Coaching/training all new staff on the contents of this Code before they are given access to personal information;
- ◊ 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 audit which is conducted every two years and addressing any issues which arise in that audit (or at any other stage). 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 network meetings or through 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 HR Intranet page at all times. The revised Code will be approved by the Senior Management Team. This Code is effective from May 2018 and will be reviewed in April 2019.

Appendix 1

Definitions of words/phrases used in relation to the protection of personal data and referred to in the text of the Code of Practice

GDPR – This Regulation replaces existing Data Protection Legislation from 25th May 2018. It is an EU Regulation and therefore is directly effective. It is intended to harmonise privacy laws in the EU.

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:
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.

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.

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. This data should be collected only with explicit consent.

Pseudonomysisation – removing all personal identification factors from personal data so that an individual can no longer be identify but keeping a method of reintegrating that data.

Automated Decision Making and Profiling – automated individual decision-making (making a decision solely by automated means without any human involvement); and profiling (automated processing of 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 the GDPR

Data Protection Commissioner

The Data Protection Acts established the independent office of the Data Protection Commissioner (DPC). The Commissioner is appointed by Government and is independent in the performance of his/her functions. The Data Protection Commissioner's function is to ensure that those who keep personal data in respect of individuals comply with the provisions of the GDPR.

The DPC has a wide range of enforcement powers to assist in ensuring that the principles of Data Protection are being observed. These include the serving of legal notices compelling a data controller to provide information needed to assist his enquiries, compelling a data controller to implement a provision in the GDPR. 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 Commissioner may authorise officers to enter premises and to inspect personal information held on computer or relevant paper filing system. Members of the public who wish to make formal complaints may do so by writing to the Office of the Data Protection Commissioner, Canal House, Station Road, Portarlington, Co. Laois, or by email to info@dataprotection.ie.

Where employees of the organisation, in the normal course of their duties, become aware that an individual including employees of the organisation may be breaching the Acts or have committed or are committing an offence under the Acts, they should report the matter to the DATA PROCTECTION OFFICER.

Advice/Assistance

All requests for advice and assistance on data protection issues within the organisation should be directed to the DATA PROCTECTION OFFICER.

Useful Contacts

Data Protection Commissioner's Office,

Phone: 1890 252231,

http://www.dataprotection.ie

info@dataprotection.ie

Appendix 3 – Associated Policies and Procedures

(1) Security Policy

PAS has an obligation to keep information 'safe and secure' and have appropriate measures in place to prevent unauthorised access to, or alteration, disclosure or destruction of, the data and against their accidental loss or destruction in compliance with the GDPR. It is imperative, therefore, 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 and recruitment support areas (such as Assessment Services, Clearance and Assignments, Candidate Support, and Executive Search) have access to personal data in respect of candidates for competitions and prospective board members. 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 have access to personal information on staff members (HR and Finance Unit), candidates (IT), board members/assessors/invigilators (IT, Finance Unit and Recruitment Support) and suppliers (Recruitment Support and Finance Unit). This data must only be used for the purposes for which it was collected (contained in the relevant 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 HR/CDU must sign a Confidentiality Statement.

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

It is important that all personal data in PAS is used only for the purposes for which it was obtained and is kept confidential in PAS.

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 – all computers are set to lock automatically after 5 minutes. Emails should be checked before sending to ensure they are addressed to the intended recipient.

(ii) Staff are required to ensure personal or confidential information is not displayed on computer screens in public areas of the office.

(iii) 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.

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

(v) 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).

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

(vii) Anti virus and anti spyware software is installed on all personal computers and laptops.

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

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

(x) 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.

(xi) 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;

(xii) 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;

(xiii) As part of the office's move towards paperless boards, 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;

(xiv) 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:

a. Personal, private, sensitive or confidential data must never be stored on portable devices. 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. No confidential or sensitive corporate information should be accessed or transmitted over an unsecured public wi-fi network.
b. passwords are enforced on smart phones and mobile devices and passwords used should be strong and secure as stated in the Information Security Policy;
c. When portable computing devices or mobile phones are being used in public places, care must be taken to avoid unwitting disclosure of information, e.g. through overlooking or overhearing by unauthorised persons;
d. 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;
e. 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;
f. portable devices should never be left in an unattended vehicle;
g. 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

When accessing this data remotely, it must be done via a secure encrypted link.
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.
- ◊ 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 be taken when checking candidates in that they cannot view information on other candidates (ensure they only receive a copy of their own application form).

- ◊ 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 stages that reception is unattended (e.g. overnight) and the key to that press must be stored in a secure location.
- ◊ Care must be taken that candidates signing-in at test venues are not allowed to view personal data on other candidates (including names).
- ◊ 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 photocopying 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.).
- ◊ 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 other external parties unless it is absolutely necessary and complies with the General Data Protection Regulation, 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 they should not send in personal information by email; the disclaimer at the bottom of office emails advises customers of this*[1].
- ◊ The fax must never be used for transmitting documents containing personal data.

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.

- ◊ You should ensure that the data will be delivered only to the person to whom it is addressed or someone acting on their behalf 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.
- ◊ 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 and would be accepted under the terms of the GDPR. 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. Such an agreement should define, where required: -
    (i) 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);
    (ii) named contacts in each organisation responsible for the data;

(iii) the frequency of the proposed transfers;
(iv) an explanation of the requirement for the information/data transfer;
(v) the transfer method that will be used (e.g. Secure FTP, Secure email, etc.);
(vi) the encryption method that will be used;
(vii) the acknowledgement procedures on receipt of the data;
(viii) the length of time the information will be retained by the third party;
(ix) confirmation from the third party that the information will be handled to the same level of controls that PAS applies to the information;
(x) confirmation as to the point at which the third party will take over responsibility for protecting the data (e.g. on confirmed receipt of the data);
(xi) the method of secure disposal of the transfer media and the timeline for disposal;
(xii) the method for highlighting breaches in the transfer process;
(xiii) for data controller to data controller transfers (as opposed to a data controller to a data processor transfer), it needs to be clear that only necessary data is transferred to meet the purposes;
(xiv) clarification must be obtained in advance from the Data Protection Officer that such transfers are legal, justifiable and that only necessary data is transferred to meet the purposes;
(xv) particular attention should be focussed on data made available to third party data processors under contract for testing purposes. Live data should not be used for this purpose.

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.

(2) CCTV Policy as it relates to Candidates and other Visitors to PAS

This building has a CCTV system in place for security reasons in all of the lift lobbies, Stairwells and the basement. CCTV cameras have been installed in the SMART CENTRES and the CAREERS STORE in order to ensure the safety and security of personnel and assessment material.

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 incidents in relation to the areas covered 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; to ensure the safety and security of assessment material or the assessment process; for health and safety reasons; or to help 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.

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

The 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 below may be retained for longer periods as part of a legal/disciplinary investigation. The footage will be viewed by Business Support staff, as required, and only those staff have access to this data on an ongoing basis. 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 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 this may be acceptable without a written request.

(3) Records Retention Guidelines

Type of File / Record	What is included on File / Record	Retention Period
Competition File (Physical)	As per Competition Checklist at Appendix E	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	18 months
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.

Type of File/Record	What is included on File/Record	Retention Period
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
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

Type of File/Record	What is included on File/Record	Retention Period
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.
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

Type of File/Record	What is included on File/Record	Retention Period
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
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

Type of File / Record	What is included on File / Record	Retention Period
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

Type of File/Record	What is included on File/Record	Retention Period
Executive Assessment Reports	Report of candidate's executive assessment if called for final interview	3 months
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

Type of File / Record	What is included on File / Record	Retention Period
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

APPENDIX 4 - Competition File Data Retention (to be sent to National Archives)

PLEASE ENSURE THAT ONLY THE FOLLOWING DOCUMENTS ARE RETAINED ON COMPETITION FILES – NO DRAFT DOCUMENTS TO BE STORED ON COMPETITION FILES (PLEASE NOTE THAT NOT ALL DOCUMENTS WILL BE REQUIRED FOR ALL UNITS) ALL OTHER DOCUMENTS SHOULD BE STORED AS A SOFT COPY ON THE CAMPAIGN FOLDER

(E.g. – blank application forms, Advertisements, Board Member Contact Information and Letters, Competition Checklists and Statistics Forms)

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)

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 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

Important letters, emails and other pertinent information which is not stored electronically should be kept in back of file in a file pocket.

APPENDIX 5 - Clearance Files 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

Appendix 6 - Candidate and Board Member Privacy Statements

(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/data-protection/Code-of-Practice-for-the-Protection-of-Personal-Data-in-the-Public-Appointments-Service.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.

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.