poistphoiblí
publicjobs

Code of Practice for the Protection of Personal Data

Updated March 2025

poistphoiblí publicjobs

Table of Contents

I. Introduction

Data (including information and knowledge) is essential to the administrative business of publicjobs. In collecting personal data from our candidates, selection board members/assessors/invigilators, suppliers and staff members, publicjobs strives to strike the balance between an individual's right to privacy and the legitimate requirement to process data in order to conduct recruitment competitions and conduct the business of a state body generally.

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. We have an obligation to use the data collected both effectively and ethically, and this Code of Practice will provide you with some context as to how these aims are achieved.

Set against the General Data Protection Regulation (GDPR) and the Data Protection Act 2018, the aim of this Code of Practice is to ensure each staff member in publicjobs understands the concepts of Data Protection and is aware of their own responsibilities regarding same. This, in turn, will assist this office in its compliance with the Regulation. The reading and understanding of this Code by all staff will go a long way towards meeting this requirement.

The secondary purpose of this Code is to provide some assurance to our stakeholders, whether candidates, Board Members, suppliers or staff members, that publicjobs has put serious thought into how we process personal data and can demonstrate compliance with the relevant legislative frameworks governing these activities.

Protecting our data is common sense. By reading this Code, I trust that you will understand the common-sense approach to data collection and processing which publicjobs strives to achieve.

Margaret McCabe

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 publicjobs) 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; this includes 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 the principles of data protection (as outlined in the GDPR) for all data subject groups, how we ensure the security of the data we process, and how we deal with breaches of those 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

This Code applies to staff and selection board members/assessors/invigilators (and former staff and selection board members/assessors/invigilators). It also applies to consultants and contractors working in or on behalf of publicjobs, staff of other organisations on loan to this Office, and the members of the publicjobs Board.

STAR and Oleeo

Throughout this Code, you will see reference to two different processes in place for processing data in publicjobs; the STAR process and the Oleeo process. That is because publicjobs introduced a new recruitment platform in March 2025, which is built on the Oleeo platform. Prior to this, we relied upon STAR, which is a recruitment platform that was designed specifically for publicjobs in 2009. The STAR database is stored on servers within publicjobs, while the Oleeo platform is hosted in the UK, and with cloud services supported through data centres based within the European Economic Area.

While there is no difference in legal terms to the data we collect, why we collect it and why we process it, you will see throughout this Code that the change of recruitment platform has slightly changed the way we collect the information and the journey your data goes on

throughout the recruitment process. Where the data is treated the same on both platforms you will see only one description of processing, and where there is a difference this will be outlined.

Legislative Framework

The following legal framework is applicable to publicjobs;

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

Legal Basis for Processing Personal Data

The specific legal basis applicable to all processing carried out by publicjobs will be outlined throughout this Code. To summarise how publicjobs is authorised to collect personal information from candidates, Article 6(1)(e) of the GDPR provides that the processing of personal data shall be lawful where such processing is necessary for the exercise of official authority vested in the controller. This is the legal basis relied upon for the majority of processing carried out by publicjobs, as we are 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. This obligation is laid out in Section 34 of the Public Service Management (Recruitment and Appointments Act 2004 (2004 Act).

Certain “special category” personal information is collected for Equality Monitoring purposes only. We do not make it mandatory to supply this data as we respect that candidates have a right to privacy, especially in regard to sensitive information. The reason we collect this personal data is to ensure that the services we provide are as accessible, fair and equitable as possible and are conducted in line with PAS’s public sector duty as outlined in Article 42 of the Irish Human Rights and Equality Act, 2014. We are committed to ensuring our processes are fair and equitable to everyone, and use the data provided to generate anonymous statistics which allow us to measure the effectiveness of our Equality, Diversity and Inclusion measures and the accessibility of our assessment processes.

By providing any of the personal information requested in the non-mandatory equality monitoring fields, candidates are consenting to the collection and processing of this data for these purposes. The legal basis we are relying on to process this data is outlined in Articles 6(1)(e) (exercising an official duty) and 9(2)(a) (consent) of the GDPR. Candidates are informed that the information provided will have no bearing on the way their application will be considered and will be used to provide information for anonymised research purposes only.

The non-mandatory information collected comprises:

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

STAR Process

On STAR, candidates provide this equality monitoring data on their candidate profiles. The information provided will be retained for as long as candidates wish to maintain an active account. Candidates are asked to ensure that this equality information is accurate and up to date and that it is updated any time their details change. The candidate has the right and ability to withdraw their consent at any time by logging on to the website and amending their details accordingly.

Oleeo Process

On Oleeo, candidates are asked to provide the Equality Monitoring Data when applying for a job, as part of the application process. Application Forms are stored by publicjobs for three years, after which point the equality monitoring data will only be retained anonymously unless recorded by the candidate on their profile.

3. Data Protection Principles

As mentioned above, publicjobs processes personal data relating to candidates (and potential candidates), people who have registered an interest in receiving job alerts with publicjobs.ie, selection board members/assessors/invigilators, suppliers, publicjobs Board members and staff members.

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

There are seven data protection principles set out in the GDPR. In the following sections, we will set out how publicjobs complies with each of those principles.

Principle One

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

The purpose and use of processing personal data in publicjobs can vary greatly depending on the groups for which the data is processed. Details about these groups are set out below.

Prospective Candidates registering on publicjobs.ie

Prospective candidates may register with our website 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. 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, however deleted messages will still be visible to publicjobs.

Information retained on all candidate profiles includes:

- All applications made
- All bookings made
- All messages sent by publicjobs to the Messageboard
- All job alerts registered

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 candidate data for research purposes in order to quality assure its assessment processes. This data may be retained in an anonymised form.

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 publicjobs. This data is not stored on the profile.

STAR Process

When registering an account, you will be asked to create a profile. Profiles can be updated and deleted at any stage by the person themselves or by contacting publicjobs and requesting same. Personal data captured at registration stage includes:

- Username and password*
- Security Question*
- Title
- Name*
- Date of Birth
- PPSN (if relevant)
- Gender Identity
- Email address*
- Postal address*
- Postcode
- Country*
- Daytime Phone Number*
- Other Phone Contact Number(s)
- Correspondence language preference (English or Irish)
- Highest Educational Qualification and location (i.e. name and location of School, University, Training College etc.)
- Main field of study
- Current work or study status
- Employment Sector
- Career Level
- Details of any accommodations required in the selection process
- Details of Job Alert notifications the candidate wishes to set up

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

If prospective candidates subsequently apply for a competition, their profile details will automatically update the relevant sections of the standard application form.

Oleeo Process

Personal data captured at registration stage on Oleeo is:

- Email Address
- First Name
- Last Name
- Password

When a candidate then applies for a competition, the following additional information will be captured:

- Date of Birth
- PPSN
- Gender
- 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

Candidates taking part in a Recruitment Competition

The legislative basis for processing candidates' personal data is set out on page 5 of this Code. Personal data is collected from all candidates for competitions run by publicjobs 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 the candidate profile, the

application form and, should the candidate be successful at the final assessment, through supplementary information collected as part of the pre-employment checks process.

The 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 (should the candidate be called to these stages). Information which is required to be provided by candidates as part of the application process relates to their relevant qualifications and work experience, and examples of the competencies and capabilities required for the particular post. To allow publicjobs to identify individuals and administrate the competition effectively, candidates are also required to supply their name, address and date of birth on the application form. Only the name, qualifications, work experience and responses to the competency/capability questions are provided to the Assessment Board.

Other data is required at the pre-employment checks stage to confirm that the candidate meets the essential requirements for the competition, to provide reasonable accommodations which may be required, and for background checks conducted at clearance and assignments stage to ensure the person is suitable for appointment in respect of character and that he or she is fully competent to undertake, and fully capable of undertaking, the duties attached to the position. Data collected at clearance and assignments stage from those candidates under consideration for a position may include;

- Security checks, Garda vetting and international police clearance certificates
- Employment and/or other references
- Relevant health and medical information (to allow for the arrangement of suitable accommodations in the workplace as required)
- A workplace accommodation form (if such accommodations are required)
- A health and character declaration
- Copies of relevant qualifications (required to confirm eligibility for certain roles)
- Proof of identity (via a valid photographic ID)
- Proof of valid driver's licence (if essential to the role applied for)
- Reports from the Chief Medical Officer (CMO) (if required)

Other information may be required for certain roles; where additional information is needed the candidate will be notified accordingly.

Information on the date a candidate was assigned to a post in a particular department or office are also stored, along with whether or not the candidate has taken up their appointment. Once a candidate has been appointed to a role, no further information relating to that employment is held by publicjobs. A copy of the assignment notice is held by this Office for thirty years, before transfer to the National Archives.

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

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

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

Selection Board Members, Assessors and Invigilators

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

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

STAR process

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

Oleeo Process

Board members/assessors/invigilators will have access to their own profiles on the Oleeo system, where they may update their information as regularly as they see fit.

Suppliers

Personal data is collected on all suppliers of goods and services in order to pay for the goods/services procured by electronic funds transfer and to ensure that the suppliers meet

any regulations (e.g. tax clearance certificates). This information is used to set suppliers up on a financial system so that they can be used as suppliers, and for our Finance Unit to make payments to them in respect of goods or services provided. While this information may not be personal data depending on the nature of the supplier, in general the relevant personal data may include the following;

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

Publicjobs Staff Members

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

- Name (including any name change), address, postal address and contact information (telephone and email)
- PPSN
- Bank Account information (accessible by PSSC only)
- Marital status
- Emergency contact information (Next of Kin)
- A picture of the staff member
- Details of Leave (including annual leave, sick leave etc.). This information is also stored on the flexi clock system.
- Pension Entitlement
- Eforms on employee schemes availed of, such as Cycle to Work or Travel Pass
- Training Summary
- From 2020 – 2023; Information on exposure to Covid-19 (advised via a questionnaire)

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

Data collected via cookies on publicjobs.ie

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

Principle Two

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

This Office only collects, processes, and stores personal data for purposes which are specific, lawful and clearly stated. The types of data we process generally are listed above. Data is collected from the above-mentioned groups as required, and is used only in connection with the purpose for which it was collected. The main purposes for which publicjobs processes data are as follows;

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

Personal information which is obtained by publicjobs 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.

Legitimate Disclosures

There are some transfers of staff member's personal data to other bodies who are carrying out operations upon the data on behalf of publicjobs, and who are not retaining it for their own purposes; these do not constitute disclosures. An example of this is the transfer of staff data to the National Shared Services Offices for payroll/pension administration, other financial transactions or HR related purposes.

Examples of legitimate purposes which require publicjobs to share some personal information with other parties include:

- Information on candidates who are being offered appointment is provided to the client organisation to whom they have been assigned (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 publicjobs;
- In the event of a staff member transferring to another government department/office, their personnel file and their details on the HRMS (Human Resource Management System) are transferred to the new Department/Office;
- National Archives disclosures (as set out below)
- Certain data is disclosed to assessment providers who carry out some of the assessments run by publicjobs; only the minimum amount of personal data is disclosed to allow them to fulfil their functions as data processors (usually name, email address and candidate identification number)
- Where a candidate requests a review by the Commission for Public Service Appointments (CPSA) in relation to an alleged breach of the CPSA Code of Practice, appeals a decision under the Freedom of Information Act to the Information Commissioner, or submits a complaint about how their data has been processed by publicjobs to the Data Protection Commission, the information requested by these bodies is provided to them in order to facilitate their investigations
- External selection board members/assessors/invigilators may receive candidate data in order to assist in the determination of suitability for a specific role; selection board members/assessors/invigilators have a duty to keep such information confidential and secure and sign confidentiality agreements to confirm this obligation
- Where publicjobs has concerns in relation to a candidate's suitability for appointment on health related g or other appropriate Medical Officer for the

relevant Sector rounds Information is provided to the Chief Medical Officer (CMO)

- Some organisations which have responsibilities for ensuring the security of the state (e.g. An Garda Síochána) 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 and shared with the HSE for medical consultant competitions
- 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 the legitimacy of all personal data processing within publicjobs, and these have established that there are sound, clear and legitimate purposes for collecting all of the information currently processed. These audits are conducted on an regular and ongoing basis by nominated staff members on behalf of the Data Protection Officer. The findings are reviewed by the Risk Management Group. A full register of all personal data processing, or Record of Processing Activity (ROPA) is maintained by all staff and held by the Data Protection Officer. This is updated regularly to ensure compliance.

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

Processing on behalf of the National Archives

The National Archives Act 1986 (amended 2018) requires publicjobs to submit competition files and other records to the National Archives after 30 years. Competition files are the official record of any recruitment process undertaken. The competition files will contain certain personal data on candidates, Assessors/Board Members, publicjobs staff and suppliers, depending on the nature of the campaign and other factors such as how far a candidate may have progressed in the recruitment process (for full details of what is contained on the Competition File, please see Appendix 3, part 4). The types of personal data relating to candidates which may be held on the competition file are as follows;

- Any candidate taking part in an assessment will have their assessment outcomes captured and retained.
- Candidates who progress to shortlisting stage will be included on the list of candidates' presented to the shortlisting board. This list may include details such as candidate names, Candidate ID numbers, and their most recent roles; the Shortlisting Board Members' assessment of their application will also be retained, in the form of a summary comment
- At interview stage, each candidate's interview notes are retained along with a copy of the marks awarded under each competency area. A summary comment is also retained to record the Board's assessment of the candidate's performance.
- Scores will be retained for each candidate who completes an additional assessment process (such as a presentation exercise, a video interview, a group exercise etc.)
- Should the candidate be considered for appointment for a professional or technical competition for the Civil Service, a copy of the provisional recommendation issued to the employing organisations will be retained (this may include the candidate's name, address, PPSN, date of birth, relevant qualifications and experience).
- Where candidates are appointed to a role, copy of the assignment notice sent to the employing Department is retained

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

Principle Three

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

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

Full details of the information held by publicjobs and the length of time this information will be retained is set out in the publicjobs Retention Schedule, as outlined in Appendix 3

Candidate Data processed as part of a Recruitment process

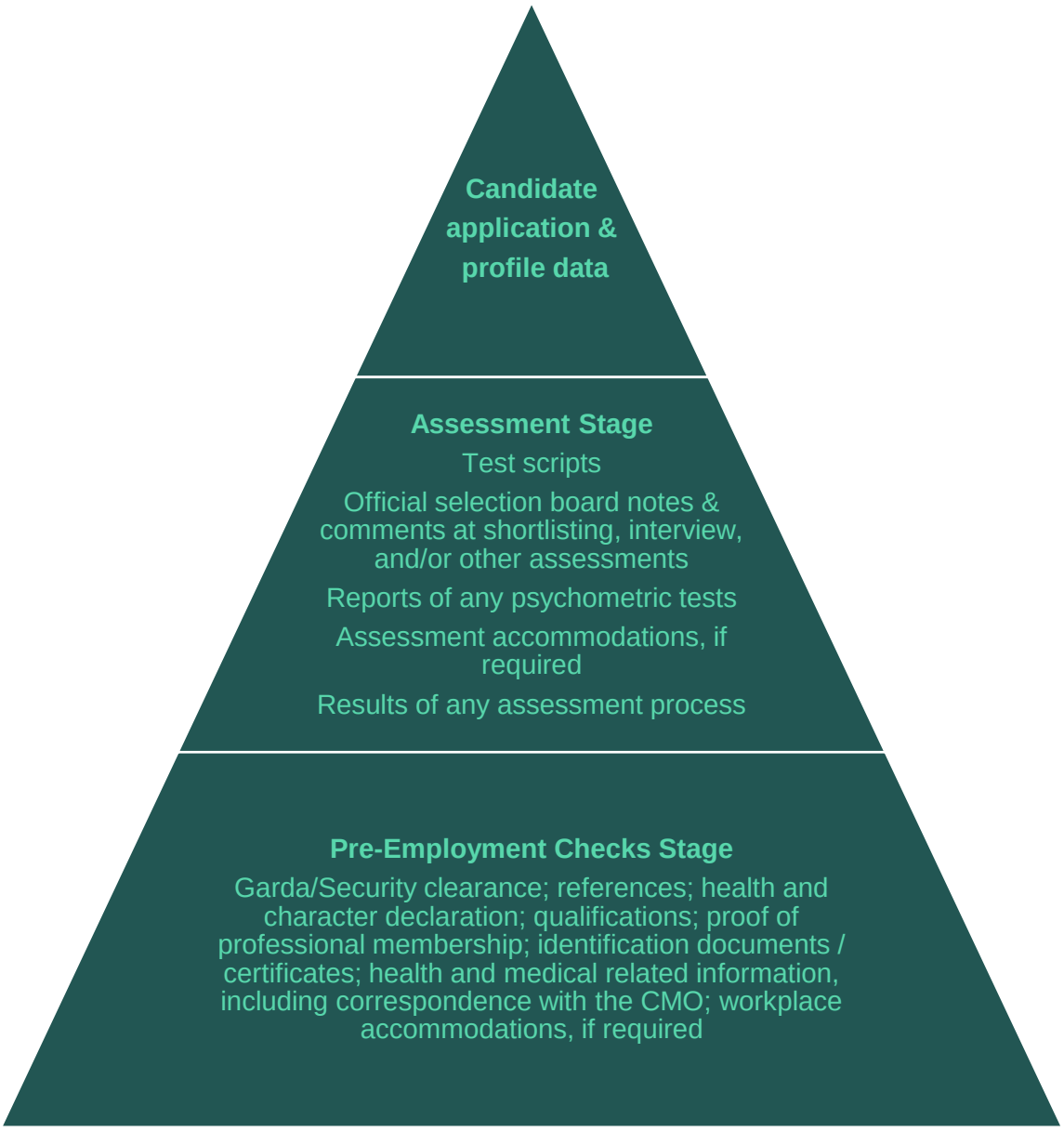
Section 24 (9) of the Public Service Management (Recruitment and Selection) Act 2004 states that “only candidates who have successfully completed the recruitment or promotion process under this Act, including compliance with the code of practice concerned shall be eligible for appointment”.

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

The 2004 Act also sets out the functions of public (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 publicjobs 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

Special Category data is defined in the GDPR and amounts to personal information which is more sensitive. Certain “special category” personal information is collected by publicjobs to carry out certain processes. This information includes the following;

- As outlined above, some special category data is collected for Equality Monitoring purposes. We collect such personal data to ensure that the services we provide are as accessible, fair and equitable as possible, and are conducted in line with PAS’s public sector duty as outlined in Article 42 of the Irish Human Rights and Equality Act, 2014. By providing any of the personal information requested in the non-mandatory fields candidates consent to the collection and processing of this data for these purposes. The information provided will be retained for as long as candidates wish to maintain an active publicjobs.ie account. Candidates are asked to ensure that this information is accurate and up to date as possible. Candidates are prompted to update this information any time they make an application through publicjobs.ie. Candidates are informed that the information provided in this questionnaire will have no bearing on the way their application will be considered and will be used for research purposes only
- Similar data may also be collected from candidates who require reasonable accommodations as part of the assessment process, based on their disability status or medical needs. This may include a medical or psychological report which the candidate may provide to publicjobs in order to allow the Occupational Psychologists within the Assessment Services Unit to determine what reasonable accommodations may be appropriate. The information retained will include a copy of that report, the candidate’s name and publicjobs candidate identification number, the accommodations agreed and granted and the date the assessment was made, and the type of disability for which they candidate requires accommodations. This report is retained for three years, and candidates will be reminded every three years that we hold this data and can ask to keep their reports on file for future assessments. Candidates can ask for this information to be deleted at any time.
- Where publicjobs conducts Garda Vetting or other Security Clearance for candidates under active consideration for a role, we may receive sensitive

data in relation to convictions and cases which are pending, including details of the alleged offence and nature of the conviction. Such records are retained for six months (the period of validity for Garda Vetting) or for length of any legal process concerning decisions made by publicjobs on the basis of this information.

- When candidates who have previously served in the public service exceed the allowed sick leave limits or indicate that they have current health related issues, their information is sent to the CMO for the Civil Service (who provides Occupational Health Advice to publicjobs as described above). The CMO may ask the candidate for additional information, which the CMO will hold in accordance with that office's data retention policy. Only the outcome of the CMO assessment is shared with publicjobs.

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

Both Oleeo and STAR hold candidates' personal profile, their previously submitted applications and electronic correspondence from PAS in relation to competitions for which they have applied. Both platforms also contain the candidates' results/progress at each stage of a competition for which they have applied. Candidates applying to competitions through STAR will supply their Pre-Employment Checks documents through email, which are then stored on our internal filing system. Candidates applying through Oleeo will upload documents directly to that platform, where they will also be securely held. Pre-Employment Check data is retained for three years, unless subject to a legal case.

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

Principle Four

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

The publicjobs Privacy Notice outlines what personal data is processed for each group (as outline above) on whose behalf data is processed by publicjobs and informs the data subjects of what information is held on them and the reason for holding this information.

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

The equality monitoring information supplied by candidates is retained for as long as candidates wish to maintain an active publicjobs.ie account and is reported on anonymously. Candidates are asked to ensure that this information is accurate and up to date and that it is updated any time their details change. This information can only be amended by publicjobs staff if the identity of the data subject is confirmed, and only at the specific instruction of the data subject.

Information supplied by candidates on their Application Forms is held for three years, after which time it is deleted. Certain information is ported from Application Forms to the candidate profile on Oleeo; it is the candidate's responsibility to ensure this is kept up to date.

Board members/assessors/invigilators may update their profiles directly on the Oleeo platform and are asked to contact the Board Members Unit in order to update their personal data held on STAR. Records of training completed are updated on behalf of Board Members by publicjobs directly.

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

Suppliers are deactivated if not used within the previous two years. This action is carried out on a regular basis.

All groups on which personal data may be held are made aware 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 for which it was collected

publicjobs keeps personal data for no longer than is necessary for the purposes for which it was collected, except where that data is required by the National Archives (as outlined above). Retention periods for personal data held by publicjobs are set out in our Records Retention Schedule (Appendix 3). These retention periods have been agreed with the National Archives, where appropriate. The minimum amount of data is retained for the shortest period possible, as set out in the Retention Schedule.

Some data in relation to testing (such as test scores) are anonymised and retained for research, validation and statistical purposes. Similarly, equality monitoring and other statistical data may be retained indefinitely in an anonymised form, for reporting and analysis purposes.

Application Forms are retained for three years from the closing date of the relevant competition. These Application Forms are deleted automatically. If an applicant wishes to continue to retain access to their individual application, they must save the form to their device as it will no longer be accessible on their publicjobs account after the period of three years has elapsed. In the meantime, applicants may delete their competition application forms at any via their publicjobs.ie account.

Candidates applying to competitions through Oleeo will have certain information provided on their Application Documents (such as name, address, email address and phone number) automatically ported to their publicjobs.ie account, in the interest of saving the candidate time in re-typing that information. This information will be retained on the profile for as long as the candidate wishes their profile to remain active.

It is important to note that if a candidate deletes their application or profile while taking part in an active competition, they will automatically be removed from that particular competition and will receive no further consideration.

While candidates may delete their profile at any time, it is important to note that where records are held by publicjobs which are required by the National Archives, their information will be retained on those documents for archive purposes.

Principle Six

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

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

- 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. Visitors to Chapter House must sign-in and then be accompanied by a staff member throughout their time in the building; board members and candidates must 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 and a security guard in place
- Board Members/Assessors/Invigilators receive training regarding the importance of data security, are required to sign a confidentiality agreement before the assessment process begins. While working remotely, Board Members are not generally permitted to print documents, and where this is unavoidable (for example the publicjobs Representative may need to take handwritten notes of the process), they must provide adequate assurance of the security measures in place in their home to prevent unauthorised access. All papers processed outside of the office are securely couriered to the Board Members home and are couriered back to Chapter House when the assessment process has concluded.
- Compliance with all guidance in relation to working remotely issued by the DPO, including the following;
    - Tips for remote interviewing

- Working remotely using Sharefile
- Remote working using a VPN or Citrix
- Tips to avoid a data breach when working from home

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

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

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

Principle Seven

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

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

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

The DPO may be contacted directly for evidence of publicjobs' compliance with the above-mentioned principles by making a request in writing, or emailing dataprotection.officer@publicjobs.ie

4. Subject Access Request Policy

As a data controller with primary responsibility for, and a duty of care towards, the personal data within its control, publicjobs has certain obligations regarding how that data is processed and managed. Our obligations are set out in the legislative framework outlined in Section 2, above.

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

- To be advised of the purpose(s) of processing said data
- To be advised of the recipients or categories of recipients to whom personal data has been or will be disclosed
- Where possible, to be advised of the envisaged period for which personal data will be stored, or if not possible, the criteria used to determine that period (e.g. if the information will be provided to the National Archives)
- To request the rectification of personal data where it is incorrect or misleading
- To request the erasure of their personal data (where possible)
- To request to restrict the processing of their personal data, or to object to its processing
- The right to lodge a complaint with the Data Protection Commissioner
- To request, where the personal data is not collected from the data subject, any available information regarding the source of this data
- The right to be informed of the existence of automated decision-making (including profiling) being operated on the data subject's data (where relevant), to include meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject. At present, publicjobs does not carry out any automated decision-making
- To be advised of, where personal data is transferred to a third party, the appropriate safeguards pursuant to the GDPR relating to such transfer.

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

Form of the Request

All requests for personal data are considered Subject Access Requests, but for the purposes of this policy publicjobs will focus only on those requests directed to the Data Protection Unit. An SAR should be made in writing and should include enough information to allow publicjobs 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). A Subject Access Request Form available on publicjobs.ie in order to facilitate these requests and to advise the requester of the type of evidence required by publicjobs for verification purposes, though completion of this form is not mandatory in order for your request to be accepted. When your identity has been confirmed, we will be in a position to commence the work involved in responding to your request. We will try to respond as quickly as possible, and in any event without undue delay, but if we have not been able to complete your request within one calendar month we will update you as to the progress of our response and may request an extension. This occurs very infrequently in publicjobs as most requests are responded to within the statutory timeframe.

Communication

We will communicate directly with you, the data subject, once a valid subject access request has been received. This contact may help you identify the exact information you wish to receive. You can help us to respond to your request quickly 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 held by publicjobs.

We recognise that failure to respond to your request within the 30-day period set out in legislation 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.

Systems Searches

Unless there is a legitimate option to reduce the scope of the request, a search of all databases and all relevant filing systems will be carried out throughout publicjobs. A response to the request will be directed, co-ordinated and provided by the Data Protection Unit, who have responsibility for issuing such responses.

STAR Process

publicjobs will organise the response to the request by giving one or more individuals (the Data Protection Liaison Officers) the responsibility for conducting searches of their relevant filing systems and databases. This information will be added to a secure file sharing system internally, and the Data Protection unit will engage with the relevant Teams to ensure a full response including all relevant personal data is issued.

Oleeo Process

The Data Protection Unit will be given access to the information held on the Oleeo platform which relates to you and will compile the information directly from that source. A Data Protection Liaison Officer will be asked to confirm that no other data relevant to your request is stored on the relevant Team's filing systems.

Manual Files

All relevant manual files (as set out in the Records Management Guidelines) will be searched for your data. This may include information held in the File Storage room within Chapter House, and records held in our secure File Storage location (provided by Iron Mountain). Records more than 30 years old and which have already been sent to the National Archives will not be included in our searches.

Restrictions following receipt of a request

Compliance with GDPR and related legislation is not intended to interfere with the normal running of publicjobs business, and so if following receipt of a valid request, we are made aware of inaccuracies or other issues in the data, publicjobs is permitted to make changes to the requested information in the normal course of operation (provided no changes are made

because of the request itself). This includes the correction of incorrect data, where discovered.

Personal Data relating to Third Parties

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

Exemptions

Some material is exempt from inclusion in the response to a subject access request. This includes the content of negotiations with the data subject, and information which is subject to legal professional privilege. It also includes information relating to ongoing professional investigations 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 doing so would be likely to prejudice those negotiations. Once the negotiations are complete and put into effect, the requested information can be released.

Emails are subject to subject access requests, 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. For this reason, we will not release test material or scoring keys to candidates as part of a Subject Access Request.

Where personal data contains health information, there may be a duty on publicjobs 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 that information or supplied it to publicjobs directly.

Form of Response

We will provide you (the data subject) with any relevant data in response to a subject access request, via pdf documents attached to emails. If you do not wish to receive your response by email, please let us know in advance. Once the response to your subject access request has been finalised, we will make a full copy of the material to be retained for our own reference. These records will be used as a reference should there be any dispute as to the content or timeliness of the response provided. That file will be retained internally for seven years unless subject to a Data Protection Commission investigation (should you make a complaint following receipt of your information), in which case it will be retained indefinitely.

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

5. Responsibilities of publicjobs staff

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

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

Staff members found to be in breach of data protection legislation either purposefully or due to negligence may be found to be, in certain circumstances, committing an offence under GDPR. All current and former staff members of publicjobs 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, to never access information in relation to colleagues or acquaintances (except for work purposes) and not to discuss any candidate with, or disclose personal data to, anyone other than staff members who are working on the particular competition the relevant candidate is taking part in (or other relevant staff such as a Formal Reviewer or Data Protection Liaison Officer, as appropriate).

Audits of Data Protection and Code of Practice Procedures

When determining their work programme (in consultation with the CEO), the publicjobs Internal Audit Committee will ensure that the programme contains adequate coverage of the areas within publicjobs which are responsible for the storage, handling and protection of personal data. The focus of any data protection 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 may be conducted on a periodic basis by the DPC.

Protocol for reporting Data Breaches

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

A Breach Notification Form is available on the intranet, which requires staff to provide details as to the nature of the breach, how it occurred, and any measures put in place (or which will be put in place going forward) to limit the impact of same. These are aligned with the information required by the Data Protection Commission when making a report to that Office. The Form must be submitted without delay, and no later than within 72 hours of the breach being discovered. A member of the Data Protection Unit will then contact the relevant staff member to clarify any outstanding information and will determine if a report the breach to the DPC is required. The DPC only require a report to be provided to that body where a data breach may impact on the rights and freedoms of the data subject. Low risk data breaches are not reported to the DPC.

A template breach notification message is also on the intranet, and staff will be asked to complete this or otherwise advise all data subjects impacted by the Breach, as appropriate.

Data Protection Awareness

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

- Conducting Staff training and awareness raising on the contents of this Code and Data Protection legislation
- Providing data protection information and updates on the Intranet or Viva Engage platform in
- Coaching/training all new staff on the contents of this Code before they are given access to personal information
- Regular reports to the Management Board on data protection matters
- The use of further staff communication resources as required

Monitoring and Reviewing

All managers are responsible for ensuring the implementation of this Code in their Units and raising awareness of data protection on an ongoing basis with their staff. All staff are responsible for always adhering to this Code. Managers are also responsible for complying with the data protection audits and addressing any issues which arise in those audit (or at any other stage as issues come to light). The onus is on Managers to bring data protection related concerns to the attention of the DPO as they arise. They should also raise such issues with their colleagues through the regular Leadership Team meetings or through any other appropriate forum.

The Code will be reviewed every year by the DPO (though if processing activities have not changed, it may not be updated) and the most up-to-date version will always be available on the Policy Hub and Quality Administration knowledge bases on the Intranet. This Code will also be published on publicjobs.ie. The revised Code will be approved by the Senior Management Team. This Code is effective from March 2025 and will be reviewed in January 2026.

Appendix I: Definitions of Data Protection Terms

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

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

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

Subject Access Request – this is where a person makes a request to access their personal data, or information on how that data has been processed, under the GDPR.

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

Data Subject – the person to whom the personal data relates.

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

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

Special Categories of Personal Data – Sensitive personal data. This includes personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs,

trade union membership, health data, data concerning a person's sex life or sexual orientation. Special rules apply to the processing of this data as it is particularly sensitive.

Pseudonymisation – the process of removing all personal identification factors from personal data so that an individual can no longer be identified directly but keeping a method of reintegrating that data so that the Controller may associate the data with a specific individual if required (e.g. referring to a candidate by their publicjobs Candidate or Application ID number, rather than their name).

Anonymisation – The process of removing all personal identification factors from personal data, so that an individual can no longer be identified

Automated Decision Making and Profiling – automated individual decision-making means making a decision solely by automated means without any human involvement. Profiling means using personal data to evaluate certain things about an individual. Profiling can be part of an automated decision-making process. Only profiling that is based on purely automated processing, i.e., without meaningful human intervention, and which produces "*legal*" or "*similarly significant*" effects on a data subject is generally prohibited under Article 22 GDPR. In all other cases of profiling, the general provisions of the GDPR apply. Publicjobs does not engage in automated decision making or profiling.

Appendix 2: Enforcement

Data Protection Commission

The Data Protection Act 2018 established the independent Office of the Data Protection Commission (DPC). The DPC can have up to three Commissioners, who are appointed by Government. The DPC is independent in the performance of its functions and is responsible for ensuring that those who process personal data in Ireland do so in compliance with data protection legislation.

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

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

Data Protection Officer

All requests for advice and assistance on data protection issues within the organisation should be directed to the Data Protection Officer (DPO). The DPO's responsibilities include;

- Overseeing data protection compliance within the organisation
- Carrying out data protection audits and investigations
- Reviewing and offering guidance on Data Protection Impact Assessments
- Providing data protection training
- Notifying the CEO and Management Board of data protection risks
- Offering advice and guidance on data protection matters

Where publicjobs staff members, in the normal course of their duties, become aware that an individual (including employees of the organisation, Board Members/Invigilators/Assessors or suppliers operating on behalf of publicjobs) may be breaching data protection law or have committed or are committing an offence under the Acts, they should report the matter to the Data Protection Officer. Reports can be made verbally, but preferably by email to dataprotection.officer@publicjobs.ie. Alternatively, you can write to Data Protection Officer, Public Appointments Service, Chapter House, 26/30 Abbey Street Upper, Dublin 1 D01 C7W6. The current Data Protection Officer for publicjobs is Sinéad Dolan.

Appendix 3: Associated Policies and Procedures

1. Data Security Policy

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

This publicjobs Data Security Policy sets out who can access the various types of personal data in publicjobs, 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 Units and recruitment ancillary units (such as Assessment Services, Pre-Employment Checks, Candidate Support, Client Relations Management 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. Where not specified in this policy document, permission should be sought from a senior manager before releasing any data to third parties to ensure that there is a legislative basis to do so.

Staff in support units have access to personal information on staff members (People & Culture and Finance Unit), candidates (IT), board members/assessors/invigilators (IT, Board Members Unit and Finance Unit) and suppliers (Finance Unit, any Unit involved in the procurement and management of the contract). 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 People & Culture must sign a Confidentiality Statement.

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

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

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

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

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

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

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

v) All personal data held by Oleeo is stored in geographically separate primary and disaster recovery data centres. Access to these data centres is strictly limited to designated Oleeo employees and only through Oleeo's internal network with all logins and actions logged.

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

vii) 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

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

ix) Anti-virus and anti-spyware software is installed on all computers and laptops

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

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

xii) 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

xiii) 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

xiv) Personal or sensitive data held on applications and databases with relevant security and access controls in place (e.g. STAR and Oleeo) 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.

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

xvi) For interviews or shortlisting exercises occurring in Chapter House, tablets may now be used for selection boards. This means that applications may be temporarily stored on ShareFile in preparation for the board meeting. The tablets must be stored securely in publicjobs, 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.

xvii) Where interviews or shortlisting exercises are conducted remotely, the same security measures regarding Sharefile must apply. Board Members must confirm that any copies of candidate applications, scoring sheets or other assessment data are not stored on their personal devices once the assessment process has concluded. Any hard copy papers containing personal data (such as interview notes) must be securely couriered to Chapter House on completion of the assessment process, and the Board Member must complete a cover sheet confirming that all papers have been returned. Failure to comply with this procedure constitutes an offense under the Data Protection Act 2018 and may result in appropriate actions being taken by publicjobs and/or the Data Protection Commission.

xviii) 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.
b. 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.
c. No confidential or sensitive corporate information should be accessed or transmitted over an unsecured public Wi-Fi network.
d. Passwords are enforced on smart phones and mobile devices and passwords used should be strong and secure as stated in the Information Security Policy
e. When portable computing devices or mobile phones are being used within a shared home environment, care must be taken to avoid unwitting disclosure of information, e.g. through overlooking or overhearing by unauthorised persons. **This includes by Alexa, Siri, or other virtual assistant technologies**
f. Staff are not permitted to access publicjobs' systems or use their work laptops in public spaces. This includes but is not limited to remote working hubs, coffee shops, or public transport
g. 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

h. Laptops must be physically secured if left in the office overnight; when out of the office, the device should be kept secure at all times. Work laptops must not be used for personal purposes.
i. Portable devices should never be left in an unattended vehicle
j. All laptops are regularly called in for AV updates and patches (immediate compliance with this is required) and all have full disk encryption; USB devices are centrally controlled, and restrictions are in place in relation to the use of USB devices; USBs are only used for non-confidential and non-personal information, e.g. public presentations).

Remote Access

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

Staff are expected to comply with this Code when accessing data remotely. If this work 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 publicjobs 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 publicjobs systems must be encrypted to the strongest standard available.

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

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

- Board members must be asked to sign a “Confidentiality Statement” before being given access to any paper files and must be briefed by the publicjobs Representative on the requirement for confidentiality at all stages of the process. Assessors/Invigilators must also be asked to sign a “Confidentiality

Statement" and be briefed by the relevant recruitment unit on the requirement for confidentiality.

- When interviewing in Chapter House, it is important that candidates and selection board members calling at reception are not allowed to view personal data on other candidates/other boards (this includes the names of other candidates) so care should be taken with the board folders to ensure they cannot be accessed, and care should also be taken when checking in candidates that they cannot view information on other candidates accidentally. This means such information should not be kept in a visible place at the reception desk
- When interviewing in Chapter House, all board papers must be taken from the board room when the board is finished, and the room must be locked if board papers are left unattended in the room at any stage.
- All board room keys must be handed into reception and the press where the keys are stored should be locked at all times when reception is unattended (e.g. overnight). The key to that press must be stored in a secure location.
- When assessing in Chapter House, care must be taken that candidates signing-in at test venues are not allowed to view personal data on other candidates (including names and candidate IDs).
- When assessing in Chapter House, 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 externally by a contractor who has in his/her contract agreed to the office's data protection procedures and ensure that the confidentiality of all personal data is protected.
- When in Chapter House and photocopying or printing personal information (e.g. application forms) care should be taken to ensure all copies are removed from the photocopying room.
- Personal and sensitive information must be locked away when not in use or at end of day (e.g. application forms, order-of-merits, confidential reports, etc.). This includes when working remotely.
- When assessing candidates remotely, all efforts should be made to ensure no paper records are created. **Board Members are not permitted to print copies of documents sent to them via Sharefile**; where this is unavoidable

(e.g. where a publicjobs Rep must hand-write the notes of the assessment), the relevant papers will be brought to the home of that Board Member via a secure courier or registered post. The publicjobs Rep must store all papers in a lock box or other secure location inaccessible by other members of the household. No papers should be left out or visible to other household members. Once the assessment process has completed, the Board Member or publicjobs Rep must complete a cover sheet and advise publicjobs that the papers are ready for collection. A courier will collect the papers from the home of the Board Member and return them securely to Chapter House

- Where a Board Member has printed papers or taken 'rough work' notes as part of a process which would normally be shredded in the publicjobs Offices, these papers must either be securely couriered to publicjobs for secure destruction, or, if feasible and appropriate, burned. **Disposing of these papers through any other means, including using a home shredder, will constitute a breach of these guidelines and may be considered an offence under the Data Protection Act 2018.**
- Access to paper records and files containing personal data is restricted only to those staff with business reasons to access them. Files are stored off-site in secure storage, or in our Records Management Room when not in use; files in use are stored in locked tambour Units within the section to which they relate. Only the Records Management Unit, the Business Support Unit and the Facilities Unit have access to the Records Management Room. Requests for files stored off-site should be sent to the Records Management Unit, who will request and release same to the relevant Unit. The name of the person to whom the file is released will be recorded. All files retrieved from Iron Mountain must be returned, in the same or a better state of organisation as they were received, as soon as the necessity for access to the files has concluded.
- Access to files containing personal data will be monitored 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 publicjobs:

- Personal information should not be sent to other external parties unless it is absolutely necessary and complies with the GDPR; you must check with a senior manager before sending any personal information to persons outside of publicjobs.
- Personal information should only be sent externally by email if the email is encrypted, and customers should be informed that they should not send in personal information by email unless absolutely unavoidable (such as at Pre-Employment Checks); the disclaimer at the bottom of office emails advises customers of this.
- When recruitment takes place on the Oleeo platform, all personal information exchanged should occur on that platform
- The fax must never be used for transmitting documents containing personal data.
- You should ensure that the data will be delivered only to the person to whom it is addressed 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 publicjobs 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. When frequent transfers of data to a named State Body or Department are required, a Data Sharing Agreement as outlined in the Data Sharing and Governance Act should be applied. To support data transfers, publicjobs 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: -
    - 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 publicjobs);
    - named contacts in each organisation responsible for the data;
    - the frequency of the proposed transfers;
    - an explanation of the requirement and legal basis for the transfer;
    - the transfer method that will be used (e.g. Secure FTP, Secure email, etc);
    - the encryption method that will be used;
    - the acknowledgement procedures on receipt of the data;
    - the length of time the information will be retained by both the third party and publicjobs (the Retention Schedule);

- Confirmation that the information will be secured to at least the standard that PAS applies, and in line with the requirements of data protection legislation
- confirmation as to the point at which the third party will take over responsibility for protecting the data (e.g. on confirmed receipt of the data);
- the method of secure disposal of the transfer media and the timeline for disposal;
- the method for highlighting breaches in the transfer process or other data protection breaches by the third party;
- 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;
- 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;
- 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.
- Particular attention should also be paid to data transfers outside the EEA; such transfers should only occur with Management Board approval, and with advice sought from the DPO

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

2. CCTV Policy

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

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

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

- Preventing or investigating interference with property, or harm to persons in the Office
- Ensuring the safety and security of assessment material or the assessment process
- Health and safety
- Helping investigates any complaints involving harm to persons or interference with property.
- Where applicable and appropriate, to respond to a Subject Access Request

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 publicjobs in relation to the assessment process. This will be determined on a case-by-case basis and will only form part of the review process where strictly relevant and necessary.

To protect the privacy of staff and customers and the integrity of our assessment material, the use of any other type of recording equipment is not permitted in Chapter House.

Security and Retention Arrangements

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

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

CCTV footage extracted as art of a Subject Access Request will be redacted, and the footage released will be stored for seven years in redacted form.

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

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

Data Protection

CCTV footage will not generally be provided as part of a Subject Access Request response, as the data is not stored long enough to generally be extracted as part of such a request. Where a data subject specifically requests access to such data, and if the request is made within the retention period of that data, it may be possible to provide the data subject with a redacted copy of the relevant footage. The footage will be redacted to ensure only the

relevant data subject is identifiable, and the redaction will be carried out by an expert in this area (who may be a third-party), who will be required to agree to appropriate confidentiality agreements before the raw footage is provided to them.

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

3. Records Retention Schedule

Type of File / Record	What is included on File / Record	Retention Period
Competition File	See Competition File Checklist	Indefinite – transfer to National Archives
Rough Work	Board members notes not forming part of the official record (i.e. not the notes taken by PAS Representative)	Destroy once board report has been prepared
Reasonable Accommodation Information	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 relating to candidates' assessments retained indefinitely Photocopies of Medical Reports and details of disability etc. retained for 3 years; candidates will be reminded every three years that publicjobs is retaining this data and may consent to us holding this for a further three years
Equal Opportunities Data	Information gathered in relation to specific grounds from the Equality legislation.	Indefinitely (in anonymised form) STAR: On profile indefinitely; may be deleted by the candidate Oleeo: Saved on Application Form for three years
Scripts, Presentation Exercises, Work Sample Tests and other written assessments	Candidates' identity (ID, name, email address etc.), candidates completed assessment	Three years, or for one year after the panel is exhausted, whichever is longest

Type of File / Record	What is included on File / Record	Retention Period
	Assessors notes from exercise (Assessor Report Form, notes, comments and scoring sheets)	Assessment outcomes (scores/OOM) are retained on the Competition File indefinitely
Video Interviews & Remote Proctoring records	The video record of the assessment	Panel length plus one year
Online Tests (verbal, numerical, SJTs etc.)	Candidate name and number; candidates' responses to each question for some tests, candidates' scores	Full data retained for length of panel Historical data is anonymised and retained indefinitely (by ASU)
Personality Questionnaires	Reports based on responses provided by candidates	Two years
Verbal References	Record of all verbal references provided	Three months or, where a panel is formed, the lifetime of the panel
Executive Assessment Reports	Report of candidate's executive assessment if called for final interview	Three months
Hospital Consultant Referee Report	Reports on training and relevant experience	1 year
Template documents	Standardised documents saved to the eHub, other	Indefinite (on eHub)
Documentation collected from candidates who are ultimately unsuccessful	Copies of certificates/proof of eligibility and IDs; honesty statements/Declarations	Destroy immediately once final Board Report signed

Type of File / Record	What is included on File / Record	Retention Period
Other Competition Documents	Non-essential correspondence, Application Forms, all other Competition Documents not otherwise listed on this Schedule	Three years
Feedback Requests	All requests and responses issued in relation to assessment feedback	Three years or length of panel plus One year, whichever is longest
Review Requests	Request Received, response issued, Review Trackers Research conducted/correspondence surrounding review,	Indefinite Three years
Clearance & Assignments: Candidate File	As per Candidate File Checklist	Three years
Clearance & Assignment Masterfile	File containing full panel information for all competitions with a panel in place	Indefinite
Clearance & Assignment – other files	Any records held by Clearance & Assignment Teams not otherwise listed	Three Years
Website Registration / Profile Information	Username, Candidate I.D., Title, Name, Address, Phone Number(s), Email Address, Postal Address, Date-of-Birth, Highest Qualification, Career Level, Special Needs,	Information to be retained indefinitely. Candidates will have the option to delete their profile.

Type of File / Record	What is included on File / Record	Retention Period
	Job Alerts, Job Category, Job Subcategory	
STAR and Oleeo Information – non personal	All non-personal information held on STAR and Oleeo	Indefinite
STAR Information – personal	Candidate Applications Candidate Profile Information, including message board messages Assessment details and scores	Three years Indefinite (may be deleted by the candidate except where forms part of a competition file) Indefinite (National Archives)
Oleeo Information - Personal	All personal information on Oleeo (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)	As STAR

Type of File / Record	What is included on File / Record	Retention Period
Board Member / Assessors / 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 – may be deleted upon request
Suppliers	Tax Clearance Certificate Electronic Format, via ROS; Company name, address and contact details; bank account information; records of all payments made	Indefinite
Parliamentary Questions	Question asked, response submitted and any supporting material	3 years
Correspondence from TDs	Question asked, response submitted and any supporting material	3 years
Personnel Files	Name, address, PPNS, contact numbers, sick leave record and medical documents, civil service	Sent to new organisation on transfer or retained indefinitely for pension purposes

Type of File / Record	What is included on File / Record	Retention Period
	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.	
Microfiche details for former staff and other legacy systems	Name, address, contact numbers, sick leave record	Indefinite for pensions purposes
Staff Census Forms	Disability status of staff on an annual basis – self declaration	Three years
Ethics in Public Office Returns	Returns received from all relevant PAS staff / members of the PAS Board	15 years
Legal Files	Records of legal problem (notification of case, correspondence and records showing investigations), legal advice sought and received, outcomes	Indefinite – Transfer to National Archives;

Type of File / Record	What is included on File / Record	Retention Period
FOI	FOI request and request for review (if appropriate); acknowledgement(s), response(s) from publicjobs, copies of all associated documents; all correspondence with the Information Commissioner	7 years unless the case has gone to the Information Commissioner; Information Commissioner files/Legal Advice files retained indefinitely and transferred to National Archives
Subject Access Requests	Subject access requests and responses	3 years unless escalated to DPC; DPC investigation files retained indefinitely and transferred to National Archives
Data Breach Files	all correspondence with the Data Protection Commissioner; all investigations into data breaches	Indefinite- transfer to National Archives
Policy Files	Documentation in relation to any policy decisions made by publicjobs and any discussions around those decisions (including with regulatory bodies etc.)	Indefinite – Transfer to National Archives;
Procurement Files	As per Procurement Checklist on Intranet	7 years
Finance Files	Staff Salary Files	Indefinite for pension purposes

Type of File / Record	What is included on File / Record	Retention Period
	Fees and Travel Expenses for Board Members and Board of PAS	7 years
Administrative Files - Informal	Records of meetings and documents provided to meetings carried out as part of non-decision-making groups (e.g. team meetings), draft documentation	3 years
Administrative Files – Formal	Records of meetings and documents provided to of decision-making groups (e.g. publicjobs Board documentation, Management Board documentation, Senior Management meeting documentation, Recruitment Operations meeting documentation, Leadership Team documentation, Internal Audit Committee documentation Risk Management Group etc. etc.)	Indefinite – National Archives
Complaints (outside review process)	Request received; acknowledgement; response issued and all associated research	3 years unless file contains legal advice; Legal Advice files retained indefinitely and transferred to National Archives

Type of File / Record	What is included on File / Record	Retention Period
General Correspondence (emails and letters)	Query and response	3 years in Unit directories; 7 years on mailmeter
CCTV Footage	All footage captured on CCTV	30 days unless forms part of SAR
Google Data Analytics/Matomo data used to help analyse how users use Publicjobs.ie. These 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
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
Email Correspondence	All emails received and sent	Stored in Mailmeter for 7 years; available through Outlook for 1`year
Correspondence / Meetings with the Department of	Records of non-campaign specific correspondence and meetings with D/PER	Indefinite

Type of File / Record	What is included on File / Record	Retention Period
Public Expenditure and Reform		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

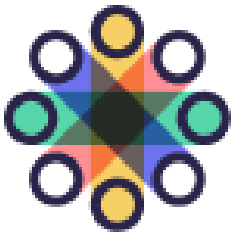
4. Competition File Checklist and Data Retention Guidelines

When a competition is deemed to have 'closed' or the panel has been exhausted, competition files must be prepared for transfer to the National Archives and Put Away until it is time for that transfer.

Competition files will be stored for 30 years before being transferred to the National Archives to be permanently stored there. The following Guidelines apply to Competition Files;

- Only completed and final versions of documents are included in the competition file (no draft or incomplete versions)
- The Competition File Checklist includes all possible assessment stages which are required to be sent to the National Archives; however, it is expected that not all stages listed below will form part of every competition
- All competition documents that are not listed below are not included in the Competition File, and you should refer to the Retention Schedule to identify how long these records should be retained. These documents may include Application Forms, Board Member or staff contact information, checklists, statistical information, draft or template documents etc.
- Important letters, emails and other pertinent information should be stored in the competition file; this means that important emails should be saved in an 'important correspondence' folder within your competition directory or retained on the Competition File built on Oleeo. Letters or other correspondence which was received or sent in hard copy should be stored with hard copy interview notes, and the RMS number of the box where they are contained should be recorded in your Competition File. Important correspondence should be understood as any correspondence with a material impact on the recruitment process

If you are unsure if the data you are recording forms part of the competition file, you can ask your Team Data Champion or contact the Records Management Team who will be able to assist.



poistphoiblí
publicjobs

Competition File Checklist

Planning Stage

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.)

Final, agreed Information Booklet

Confirmation of invasive procedures EPP (Hospital Consultants Unit Only)

Proposed Interview panel nominations (agreed and signed)

Testing

All candidate test scores

Order of Merit following the Assessment

Shortlisting and Sifting (including one way Video Interviews)

Copy of ineligible message issued through STAR

Shortlisting guide and briefing documents (including guidance documents given to the Board in advance of the Assessment)

Shortlisting Board Report, containing:

Public Appointments Service Representative's Report

Signed Confidential Report

List of Candidates/Candidates' Assessments at Shortlisting

Agreed Shortlisting Criteria (may be in the publicjobs Rep Report)

Signed Confidentiality & Conflict of Interest Forms

Information Booklet

Order of Merit

Copy of non-shortlisted message to candidates

Copy of message calling candidates to next stage

All important correspondence relating to the Shortlisting & Sifting exercise(s)

Preliminary / Main Interviews and Associated Assessments (Including Irish Interviews)

Interview Guide and other briefing/guidance material provided to the Board before the assessment(s)

Interview Board Report, containing:

Public Appointments Representative's Report

Signed Confidential Report

Signed Report from Presentation Exercises/Other related Tests

Marking Sheet

Candidates Assessments (Interview Notes)

Signed Confidentiality & Conflict of Interest Forms

Information Booklet

Order of Merit

Copy of message to unsuccessful candidates

Copy of message to successful candidates

All important correspondence relating to the Interview stage(s)

Assignment

Ministerial Sanction

Recommendation Letters/Copy of Provisional Recommendations

5. Candidate File Checklist (Pre-Employment Checks)

All Clearance and Assignment Files should be retained for three years, except where the information forms part of a legal file (where it should be retained indefinitely). The Ministerial Sanction, Provisional Recommendation and Assignment Notice should be extracted from the Candidate File and stored as part of the Competition File. The Clearance file should contain the following;

Pre-Employment Checks 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) (a copy should be retained on the Competition File)

Assignment notices to candidate (a copy of this should be retained on the overall competition file)

6. Privacy Statement

I. Candidate Privacy Statement

Data Controller: Public Appointments Service (publicjobs), Chapter House, 26-30 Abbey Street Upper, Dublin 1

Data Protection Officer: Sinéad Dolan, dataprotection.officer@publicjobs.ie

Information processed through the Oleeo platform is subject both to the terms of this Privacy Statement and the Oleeo Privacy Statement, available here.

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. publicjobs is mandated by statute (under the Public Service Management (Recruitment and Appointments) Act 2004) 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 publicjobs 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.

Categories of Personal Data Concerned

Personal data is collected on all candidates for competitions run by publicjobs 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.

publicjobs 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 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 the information currently collected. These audits are conducted on an ongoing basis by a nominated staff member for the Data Protection Officer. The findings are reviewed by the Risk Management Group, who report to the Management Board.

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

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

Recipients or Categories of Recipients

Examples of legitimate disclosures specific to publicjobs 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 publicjobs;
- National Archives disclosures are set out in the Retention Schedule and 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 publicjobs; only the minimum amount of personal data is disclosed to allow them to fulfil their functions as data processors (name, email address and publicjobs 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, submits a complaint to the Data Protection Commission 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;

- publicjobs 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 publicjobs has concerns in relation to a candidate's suitability for appointment on health-related grounds (as the CMO provides the occupational health service for publicjobs);
- 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.

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

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

A record of candidate participation in a competition will be retained for archiving purposes where that candidate has successfully completed any stage of the assessment process.

Your responsibility

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

Subject Access Requests

publicjobs 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 publicjobs are entitled to ask 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. publicjobs 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

publicjobs 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 publicjobs updated or corrected (if the individual believes that any information held is incorrect/incomplete).

2. Selection Board Members, Assessors & Invigilators Privacy Statement

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. publicjobs 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 any additional information which is required to make any payments to you. We also retain information on your training and experience where this is provided by us, and where you advise us of any additional training you have completed elsewhere. This includes online training, face-to-face training and follow-up workshops attended by you. A record of all assessments which you have been a part of is also retained for National Archive purposes.

Recipients or Categories of Recipients

Names of board members/suppliers and the extent of their services for publicjobs may be disclosed if asked for as part of a Parliamentary Question or relevant access request. No sensitive personal information is disclosed as part of these processes.

All Board Reports (which will contain the name and previous or current occupation of the panel members) are transferred to the National Archives after thirty years.

Period for which personal data will be retained

All 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 publicjobs holds on you at any stage. We would encourage you to ensure that when any of your details change you notify publicjobs, or update your own profile on Oleeo, so that the information stored on you can be kept up to date.

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

publicjobs 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 publicjobs are entitled to ask 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. publicjobs 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.

publicjobs 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 publicjobs updated or corrected (if the individual believes that any information held is incorrect.

Where you have served as a Board member as part of an assessment which is related to a Subject Access Request submitted by a candidate, the information contained on the Board Report may be supplied to that candidate as part of the response. Your contact information, including email address, will never be supplied to a third party without your explicit consent.