poistphoiblí publicjobs

Data Privacy Statement

January 2026

I. Purpose and Scope

The purpose of this Privacy Statement is so that publicjobs can be clear and transparent about the information we collect about you, and how we will use that information.

The Privacy Statement sets out our approach to ensuring compliance with the principles of data protection (as outlined in the GDPR) for all data subject groups, and how we ensure the security of the data we process.

Throughout this Privacy Statement, 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 Statement 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.

The website www.publicjobs.ie is owned and operated by publicjobs. You can access most of the website without entering your personal data. However, you will need to provide some of your personal data when you are logging into the Oleeo system through our website. Information processed through the Oleeo platform is subject to both the terms of this Privacy Statement and the Oleeo privacy statement, available here.

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

2. Accessibility and Review

Policy Owners:	Sinéad Dolan, Data Protection Officer
Heads of Division:	Sinéad Dolan
Most recent review:	13/01/2026 #13
Approver and Approval date:	Sinéad Dolan 13/01/2026
Effective date:	01/01/2026

Next formal review date:	01/12/2027

3. Data Protection Officer Contact Information

The publicjobs Data Protection Officer is Sinéad Dolan

Telephone: 01 858 7576

Email: dataprotection.officer@publicjobs.ie

Address: Data Protection Officer, Chapter House, 26/30 Abbey Street Upper, Dublin I D01 C7W6

4. Candidate Privacy Statement

Legal Basis for Processing Data

Data provided by candidates as part of a recruitment competition

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. As the processing of personal data for this purpose is necessary to allow publicjobs to carry out this statutory function, Article 6(I) (e) of the General Data Protection Regulation (GDPR) and Section 71 (2) (a) of the Data Protection Act 2018 apply.

While the processing of personal data is supported by a statutory basis, candidates are not obligated, by either statute or contractual obligations, to provide any

personal data as part of a recruitment competition. However, failure to provide the personal data which is required to facilitate an effective assessment process will result in that candidate being removed from consideration for the role applied for.

Special Category Data required for assessments and appointments

Where a candidate requires reasonable accommodations as part of an assessment process, and/or requires such accommodations in the workplace (should they be appointed to a role), publicjobs is required to collect information from that candidate regarding their health or disability status in order to arrange the appropriate measures. The right for employees to be provided with reasonable accommodations is set out in the Employment Equality Acts, 1998-2015. The information collected for this purpose amounts to special categories of data as defined in Article 9 GDPR. Section 46 of the Data Protection Act 2018 provides a legal basis for the processing of "special categories" of personal data which is required to comply with employment law.

Under the Public Service Management (Recruitment and Appointments) Act 2004, publicjobs is required to comply fully with the Code of Practice published by the Commission for Public Service Appointments. It is publicjobs function to ensure that the standards of probity, merit, equity and fairness, consistent with the codes of practice are followed in the public interest in the selection of persons for appointments in the Civil Service and other public service bodies. In doing so, we are mandated to carry out all the procedures necessary to select suitable candidates for appointment. Under S.34(b) of the 2004 Act, publicjobs are mandated to carry out competitions in line with the Code of Practice while S.24(I) requires that the Code includes requirements relating to candidate suitability. In order to assess suitability under those grounds, publicjobs is required to carry out pre-employment checks, which will include such matters as Garda Vetting (and/or international police clearance, where relevant), health and character declarations, and evidence that

the individual is in a position to provide regular and effective service (collected by way of current and previous employer references).

The legal basis relied upon for processing the special category data outlined above is Article 9(2)(a) – explicit consent. This data is subject to a range of more stringent measures designed to safeguard the fundamental rights and freedoms of data subjects, including strict access controls, 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.

Candidates may withdraw or refuse consent to the processing of this data if they wish. However, candidates should note that refusing consent to this processing will impact their application in the following ways

- Refusing or withdrawing consent regarding information collected to provide reasonable accommodations will prevent publicjobs from being able to provide such accommodations.
- As publicjobs cannot appoint a person to a role without first conducting all necessary checks, refusing consent to carry out Pre-Employment Checks will result in your application being withdrawn from the competition.

Equality Monitoring Data

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 with regard to sensitive information; candidates can choose the option 'prefer not to say' if they do not wish to provide this 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 publicjobs' 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(I)(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 consent of the data subject is collected by way of their choosing to supply the information. Consent can be revoked at any point by changing or revoking their answers to these questions when submitting a new application through Oleeo. Any such data will be treated in strict confidence, with access to such information tightly controlled and minimised to include only those staff members who require access to this data as part of their role.

Equality monitoring data is stored on the candidate profile on STAR and is retained for as long as the candidate wishes to maintain an active account. Once the STAR platform has been shut down in March 2026, the equality monitoring data provided on that platform will not be retained, except in an anonymised form. 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.

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. Candidates can remove this information from their own profile and amending their details accordingly. There are no consequences for any candidate who wishes to withdraw consent to this processing.

Categories of Personal Data

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 publicjobs 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, publicjobs 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

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
- 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 applied for a competition, their profile details would automatically update the relevant sections of the standard application form.

When STAR is decommissioned in March 2026, any accounts which were created on STAR but are not connected to any competitions will be automatically deleted.

Oleeo Process

Personal data captured at registration stage on Oleeo is:

- Email Address
- First Name
- Last Name
- Password

When applying for a role, candidates will be asked to supply the following information on their Application Form:

- 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 process

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; however, should a person come under consideration for appointment further information will be requested directly from the candidate, via a Garda Vetting return, and from the candidate's referees.

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 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, PPSN and date of birth; (of this information, only the name is shared with the selection board). publicjobs is authorised to carry out public sector recruitment via the Public Service Management (Recruitment and Appointments) Act 2004, and all data requested is required to carry out this statutory function.

The types of data collected directly from candidates on the Application Form or when registering an account include the following:

- Name
- Address
- Contact Information
- PPS Number
- Citizenship/Visa Status
- Education History
- Employment History

Further data is collected to confirm that the candidate meets the essential requirements for the competition and for background checks, to confirm that the correct candidate is taking part in an assessment, 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. While this information is generally collected at the end of a competition, in certain circumstances (such as where the information forms part of the eligibility criteria, or for roles such as those recruited for under the TLAC process where checks must be carried out in advance of any candidate names being provided to the Minister for consideration) this information may be collected in advance of Interview. The types of data collected for this purpose includes:

- Security checks, Garda vetting and international police clearance certificates
- Employment and/or other references. Where publicjobs accepts references or statements of employment, verification of documents provided may take place at any stage, and publicjobs may follow up on these in more detail during a candidate's probationary period.
- 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) or appropriate Occupational Health authority (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 is 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 person's employment is held by (unless the candidate is successful in a subsequent competition, where a reference may be collected). A copy of the assignment notice is held by this Office for thirty years, before transfer to the National Archives.

Equality Monitoring Data

Candidates are also 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. The equality monitoring data collected by publicjobs includes the following:

- Date of Birth
- Ethnicity/Cultural Background
- Country of birth

- Citizenship
- Disability Status
- Gender Identity
- Sexual Orientation
- Religion or Faith
- Caring Status
- Civil Status

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 Committee, 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; PPS numbers 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, or to verify identity).

Recipients (or categories of recipients) of personal data

There are some occasions where, in order to fulfil its obligations, publicjobs must disclose personal data supplied by candidates to third parties.

Examples of legitimate disclosures specific to publicjobs are listed below:

- publicjobs use external selection board members and assessors, who may receive (or have access to) redacted versions of the candidate application form (leaving only the candidate name, application or ID number, educational and work history including answers to the capability questions which may be included on the form) 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 are required to sign a Confidentiality Agreement in advance of such data being shared. Application documents and, where relevant, assessments completed by candidates (for example presentations and written exercises which are assessed at Interview) are provided to Board Members primarily using Sharefile, a secure digital file sharing platform relied upon by publicjobs. Notes taken as part of an assessment are uploaded to Sharefile by the publicjobs representative on the Board. In some cases, where the publicjobs representative creates handwritten rather than typed notes, the blank version of these documents are sent to the representative via courier or register post and are returned to Chapter House in the same way.
- For TLAC processes, candidate application documents may be printed for the members of the Assessment Board. These papers will either be securely couriered or, where possible, printed by the TLAC secretariat on the day. All such hard copy paperwork will be destroyed securely as soon as the relevant assessment has concluded.
- 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, included as point 8 to this statement.
- 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 or Application ID number). The majority of assessment providers used by publicjobs are based in the UK, and the transfer of data is supported by appropriate safeguards such as sharing using a secure transfer method, encryption of data, and minimising the data sent. Further information regarding these suppliers is provided as part of the relevant familiarisation material shared in advance of the assessment.
- 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 shared in order to facilitate the investigation.
- Information is provided to the CMO or an appropriate Occupational Health expert, 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) or where publicjobs requires specialist support in relation to the provision of reasonable accommodations.

- 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.
- For Medical Consultant Roles, a copy of the Pre-Employment Checks file, containing the information reviewed by publicjobs as part of that process, is shared with the HSE
- Where an appointment must be made by the Minister, details on successful candidates are shared with the relevant Department in order to facilitate the Minister making the decision. This process is also followed as part of State Board assessment processes.

International Data Transfers

Unless otherwise indicated, publicjobs holds candidate personal data within the GDPR region. Information provided through STAR is stored on secure servers within publicjobs. Once that system has been decommissioned, the remaining data will be ported to a secure Microsoft Fabric platform, hosted on the Azure cloud. This data will remain in EU data centres

Transfers to the United Kingdom

The United Kingdom holds an Adequacy Decision, as decided by the European Commission. On this basis, publicjobs transfers data to that jurisdiction, while also ensuring appropriate technical and organisational security measures are in place to protect the data transferred.

Information provided through the Oleeo platform is held on secure servers based in the UK. The processing of candidate personal data through Oleeo is supported by a robust privacy agreement, and appropriate technical and organisational

safeguards such as restricted access to the platform, the encryption of data and other robust mechanisms.

The majority of test providers which publicjobs relies upon for online testing are UK based, and candidate data is transferred to facilitate these assessments. The transfer of data is supported by appropriate safeguards such as sharing using a secure transfer method, encryption of data, and minimising the data sent.

Period for which Personal Data will be retained

The Record Retention Schedule sets out the retention period for all items of personal data kept and is provided as point 8 of this privacy statement. Necessary approval has been sought from the Director of the National Archives to destroy electronic and physical records, where relevant.

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. Information on the date a candidate was assigned to a post in a particular department or office is 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 assessment outcomes, assignment notice and any other relevant archival material is held by this Office for thirty years, before transfer to the National Archives.

All personal data not required to be retained for archive purposes are kept for three years. This includes candidate application forms. 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 application forms at any stage via their publicjobs profile. Importantly, candidates should note that if they delete their application form as part of an active competition, they will automatically be removed from that particular competition and will receive no further consideration.

Some data related to candidate performance in a competition (for example 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.

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 relating to candidates taking part in that competition, depending on the nature of the campaign and other factors such as how far a candidate may have progressed in the recruitment process. 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 on the competition file.
- 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 scored 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.
- If a candidate requests a formal Section 7 review or submits a Section 8 complaint as part of a recruitment process, a copy of the request and the outcome will be retained on the competition file.
- If a candidate raises a legal case as part of a recruitment competition, the file compiled by publicjobs as part of that case will be retained. This file will contain any submissions made by the candidate, any facts relating to the matters raised, relevant legal advice and the decision of the court/arbitration/mediation outcome

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

Automated Decision Making

publicjobs does not engage in automated decision making as part of any of our processes.

5. Selection Board Member, Assessor and Invigilator 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(I) (e) GDPR applies.

In order to ensure that the Selection Board has the experience and expertise required to assess candidates for a particular role, Board Members are required to supply publicjobs with some information regarding their career and educational history. Any Board Members, Assessors or Invigilators who are paid for their services must also supply information to facilitate these payments. As Board Members must provide this information in order to facilitate the fulfilment of their contract, Article 6(I)(c) also applies.

The provision of personal data is a contractual requirement for Selection Board Members, Assessors and Invigilators. Failure to provide the required information will mean that publicjobs is not in a position to assign you to any assessment processes.

Categories of Personal Data

The types of data held by publicjobs relating to Board Members, Assessors and Invigilators may include the following:

- Name
- Contact Information
- 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.
- Selection 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, Selection Board Members can indicate their availability on their profiles.

A record of the Selection Board Member name, capacity with which they served on the Board and most recent job title is retained on the Board Report and retained indefinitely for National Archive purposes.

Selection Board Members are reminded every two years that we hold their personal data, and that they can update this information at any time. Selection Board Members have access to update this information themselves, through their Oleeo profile.

Recipients or Categories of Recipients

The name and, in some cases, the most recent job title of a Selection Board Member is shared with the candidates who will be assessed by that Board in advance of the assessment.

Names of Selection Board Members, and the extent of their services for publicjobs may be disclosed if asked for as part of a Parliamentary Question or a valid access request. No sensitive personal data would be disclosed as part of these processes.

All Board Reports, which will contain the name and previous or current occupation of the Selection Board Member, are included in the competition file and transferred to the National Archives after thirty years.

There are some administrative reasons why Selection Board Member, Assessor or Invigilator data is shared with third parties. These cases include:

- Selection Board Member names and contact information may be shared with any third-party supplier hosting trainings on behalf of publicjobs
- Information required to process payments is recorded on Megapay. the publicjobs financial system and hosted on a secure cloud system.
- Where a Selection Board Member consents for their details to be passed to another public service body for the purposes of Interviewing on their behalf, publicjobs will facilitate this transfer using Sharefile, our secure file sharing system.

International Data Transfers

Unless otherwise indicated, publicjobs holds Selection Board Member personal data within the GDPR region. Information held on the STAR system is stored on secure servers within publicjobs. Once that system has been decommissioned, the remaining

data will be ported to a secure Microsoft Fabric platform, hosted on the Azure cloud. This data will remain in EU data centres.

Transfers to the United Kingdom

The United Kingdom holds an Adequacy Decision, as decided by the European Commission. On this basis, publicjobs transfers data to that jurisdiction, while also ensuring appropriate technical and organisational security measures are in place to protect the data transferred.

Information held on the Oleeo platform is held on secure servers based in the UK. The processing of Selection Board Member, Assessor and Invigilator data through Oleeo is supported by a robust privacy agreement, and appropriate technical and organisational safeguards such as restricted access to the platform, the encryption of data and other robust mechanisms.

Period for which Personal Data will be Retained

All Selection Board Member, Assessor and Invigilator personal data is retained indefinitely, to facilitate the continued use of that individual as part of various assessment processes. If you wish for this information to be deleted, you can contact publicjobs to arrange for same. Please note that when your information is removed from the system, it will no longer be possible for publicjobs to book you for future assessments, or to pay you for any assessments which remain outstanding at the time of the deletion.

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 relating to Board members who

are utilised as part of that competition. The types of personal data relating to Selection Board Members which may be held on the competition file are as follows;

- The Selection Board Member Name and current or most recent Job Title will be retained on all Board Reports
- Where a candidate has submitted a request for review, details of the Board will be included in the review response which is retained on the competition file.
- Where a legal case is taken relating to a Board, all information relevant to that case will be retained as part of the legal file. This may include Board documents, correspondence exchanged, and evidence or statements provided by the Selection Board Member as part of the case.

Automated Decision Making

publicjobs does not engage in automated decision making as part of our processes.

6. Staff Privacy Statement

Legal Basis for Processing Data

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 required in order facilitate the fulfilment of the staff member's contract of employment. Failure to provide the personal data required to facilitate your employment contract will mean that your contract cannot be put into place, and therefore you will not be employed by publicjobs.

The information provided is used by People & Culture (including Learning & Development) to complete any duties required of employers in relation to employees,

and by the Finance Unit in order to make payments to staff. The data is collected and held for employment and HR management purposes, to comply with our legal obligations as a civil service employer and to protect our legitimate interests as an employer. The legal bases relied upon for this processing are Article 6(I)(b), Article 6(I)e) and Article 6(I)(f).

A small amount of staff member's personal data, such as their name and contact information, may be processed as part of any competition or other business activity which they may be involved in, in order to facilitate the effective management of said process. The legal basis relied upon for this processing is Article 6(I)(e).

Categories of Personal Data

Personal data is collected on all staff members in order to maintain an accurate record of their service, to manage performance, 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 and, where relevant, postal address
- Contact information
- PPSN
- Date of Birth
- Grade and Job Title
- Salary details
- Details of overpayments and repayment plans
- Personal payroll history (pay, overtime, allowances, reduced pay periods, strike days, other unpaid leave)

- Superannuation details
- Bank Account information (accessible by PSSC only)
- Marital status
- Emergency contact information (Next of Kin)
- Details of Leave (including annual leave, sick leave etc.). This information is also stored on the flexi clock system.
- Where sick leave has been certified, a copy of the certificate
- Where supporting documentation is supplied as part of a leave application, a copy of the supporting documentation
- Civil Service career history
- Pension Entitlement
- Eforms on employee schemes availed of, such as Cycle to Work or Travel Pass, and supporting documents
- Training records
- ePMDS records
- eProbation records

A Personnel File is also opened for you, held internally, that contains the following over the course of your employment:

- Name
- Address
- PPSN
- Phone Numbers
- publicjobs assignment notice
- Grade
- Contracts of Employment
- Signed Official Secrets Act and Code of Standards and Behaviour
- Spouses and Children's Forms

- Pensions related information
- Signed Agreement Forms following promotion
- Disciplinary Documentation
- Information regarding Awards received
- Chief Medical Officer Reports and correspondence
- Rental and other references which a staff member may request during the course of their employment
- Requests for transfers and how they are processed
- Records of meetings with managers or HR
- Personal Emergency Egress Plan
- Details of workplace accommodations
- Medical referrals
- Pensions related correspondence including purchased service, added years, transferred service
- Maintenance or Attachment Orders
- Resignation/termination letter
- Retirement related correspondence
- CSEES referrals
- Pregnancy Risk Assessments

Additional personal information is stored on other general HR or Finance files (electronic or physical), and this includes:

- Applications for Refund of Fees
- Health and Safety related training details and certification
- Attendance lists from training courses and awareness sessions
- Completed Skills Audit Forms and such details stored on spreadsheets
- Requests for internal mobility
- Correspondence with PeoplePoint re staff changes

- Details of long service awards
- Exit forms
- Attendance at wellness programme events
- Sick leave statistics
- Promotion sequences
- Seniority lists
- Statistics of staffing levels (including starters and leavers per year) and fte details
- Details of workplace accidents
- Travel and subsistence claims
- Travel for work details
- Organisation of Working Time Act reports
- Staff emails
- Pensions Statements
- Disability Census returns
- Attendance records on flexi system
- CCTV records
- Photograph (you can update this at any stage by contacting HR)
- Bullying and Harassment case files
- Legal files where staff take a case against PAS
- Disciplinary case files
- Ethics in Public Office returns
- Induction details and record of follow-up meeting
- Details of ergonomic checks of your workstation
- Career break information
- Worksharing information

Should a staff member apply to an internal competition for promotion, the competition file may contain:

- A copy of the staff members CV and Personal Statement
- Interview Notes
- Assessment Scores and summary comments
- Place on the Order of Merit
- If the staff member requests a review, any information relevant to the review process will be retained

Finance Unit also open a salary file for all staff (and set all staff up on the financial management software system to allow for payments such as T&S) which contains the following:

- Name
- Address
- PPSN
- Bank Account Details
- Tax records

This information is used by the People & Culture and Learning & Development teams 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.

Recipients or Categories of Recipients

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

publicjobs may also share data with the Chief Medical Officer and the Employee Assistance Officer as the central providers of occupational health and employee supports for the Civil Service.

When a staff member joins the organisation, an account will be set up in their name on the systems they will require access to in order to carry out their role. These systems may include:

- A Microsoft account will be set up for all staff, which will include the creation of an outlook email address and work phone number. As well as this contact information, this account will record the staff members name and job title. This account is used to access a number of other systems, as part of our Single Sign On procedures.
- An Oleeo staff profile will be created for all staff required to use that platform. This will record the staff members name and work email address.
- Staff details, as outlined in the sections above, will be provided to the NSSO in order to set up a PeoplePoint account.
- All staff will be registered on Capella, our desk booking system, in order to book a desk for in-person workdays. This account is accessed through Microsoft.
- All staff will be provided with a Softworks account in order to clock in and manage their flexi-time. This system has access to the name and work email address of staff.
- Staff requiring access to our financial systems, including Unit 4 and Megapay, will have a profile created on those systems. This system has access to the name and work email address of staff.
- publicjobs will provide your name and contact details to trainers publicjobs has sourced to provide training to you (or through One Learning).

The name, contact information and job title of staff members who are responsible for administrating recruitment competitions may be shared with candidates and Board Members who are involved in those processes, as part of the general correspondence and communications which may be issued during those competitions.

Names and contact information of staff members may be disclosed if asked for as part of a Parliamentary Question or a valid access request. No sensitive personal data would be disclosed as part of these processes.

If you apply for a competition run by the publicjobs, we will provide your sick leave record and performance information at the final stage of the recruitment and selection process, on request from the relevant Clearance and Assignments Unit.

International Data Transfers

Unless otherwise indicated, publicjobs holds staff member personal data within the GDPR region. Information held on the Microsoft platform is stored on secure servers within publicjobs or hosted on a secure Azure cloud. This cloud data will remain in EU data centres.

Transfers to the United Kingdom

The United Kingdom holds an Adequacy Decision, as decided by the European Commission. On this basis, publicjobs transfers data to that jurisdiction, while also ensuring appropriate technical and organisational security measures are in place to protect the data transferred.

Information held on the Oleeo platform is held on secure servers based in the UK. The processing of staff data through Oleeo is supported by a robust privacy agreement, and appropriate technical and organisational safeguards such as restricted access to the platform, the encryption of data and other robust mechanisms.

Period for which Personal Data will be Retained

The information on the HRMS is retained indefinitely and is updated as changes occur (e.g. grade change, salary changes). The HRMS is a secure system which only People & Culture staff and PeoplePoint has access to. The Department of Public Expenditure and Reform, the C&AG and the CSO have permission to run general reports in relation to issues such as staff numbers, absence levels, etc. but these reports do not allow them to see any personal information. You can view and update much of your own information through the PeoplePoint system.

The timeframe for retention of staff data is set out in the overall Civil Service Retention Schedule, as follows:

- The information which is stored and retained on your personnel file is used to ensure an accurate record of your employment is maintained and the information is retained to assist with any issues which might arise in relation to your service (e.g. at retirement age in relation to the payment of the appropriate pension entitlements). This file is kept in People & Culture in a lockable cabinet (the room is also locked when no HR staff are present) and should you transfer to another department/office the file will be passed on to them. As per the overall Civil Service Retention Schedule, the personnel file is retained for 100 years or for the life of the last beneficiary, whichever is longer.
- Similarly, individual staff pension files are retained for 100 years or for the life of the last beneficiary, whichever is longer.
- Any files which are created or held by line managers relating to the management of an employee are retained for two years.
- Internal competition files will be held for the lifetime of the competition panel plus one year for employment law purposes. The list of successful candidates will be retained indefinitely.

- Files relating to disciplinary processes resulting in an oral warning are retained for 6 months following the date of warning.
- Files relating to disciplinary processes resulting in a written warning are retained for 12 months following the date of warning.
- Files relating to disciplinary cases which result in an action being taken, including the termination of employment, are retained for 6 years following the conclusion of the disciplinary action or the termination of employment, whichever is first.
- Files relating to disciplinary cases where children or vulnerable adults are involved are retained for 25 years following the conclusion of the disciplinary process.
- The Salary File is retained in the Finance Unit in a lockable cabinet (the room is also locked when no Finance Unit staff are present). Only Finance Unit and staff involved in the set-up of payments have access to the financial management software system. This information is retained for the length of your employment in publicjobs, plus seven years (for audit and accountability purposes).

You are entitled to review and update the information which is held on you in any of the above systems. We would encourage you to ensure that when your contact details, emergency contact details, or other personal details change, that you update your PeoplePoint record accordingly (and People & Culture and/or Finance Unit, if appropriate) so that the details stored on you are at all times up to date.

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 may contain certain personal data relating to staff members who

are involved in administrating that competition. The types of personal data relating to staff members which may be held on the competition file are as follows;

- Where a staff member signs off on an assessment outcome, their name signature will be retained on that document.
- Where a candidate has submitted a request for review which relates or involves a particular staff member, that person's name and job title may be included in the review response, which will be retained on the competition file.
- Where a legal case is taken against publicjobs, all information relevant to that case will be retained as part of the legal file. This may include staff member details, correspondence exchanged, and evidence or statements provided by the staff member as part of the case.

The Register of pensionable officers is retained for 30 years, before transfer to the National Archives.

Automated Decision Making

publicjobs does not engage in automated decision making as part of any of our processes.

7. Data Protection Rights Applicable to All Data Subjects

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 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 – information which is required to defend a legal case, or which is required to be retained for the National Archives (including information confirming appointment to a state body) cannot be deleted)
- To request to restrict the processing of their personal data, or to object to its processing
- The right to lodge a complaint regarding how your personal data has or will be processed, either with publicjobs and/or 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 falling within the scope of the above description, including all requests for access to 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 is 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.

Subject Access Requests can be made by emailing or messaging the recruitment team you are engaging with, or by emailing dataprotection.officer@publicjobs.ie

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.

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.

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.

8. publicjobs 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 publicjobs 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,	Records relating to candidates' assessment retained indefinitely, in an anonymised form. Photocopies of Medical Reports and details of

Type of File / Record	What is included on File / Record	Retention Period
	accommodations agreed, competitions applied for	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 Assessors notes from exercise (Assessor Report Form, notes, comments and scoring sheets)	Three years, or for one year after the panel is exhausted, whichever is longest Assessment outcomes (scores/OOM) are retained on the Competition File indefinitely

Type of File / Record	What is included on File / Record	Retention Period
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	I year
Template documents	Standardised documents saved to the eHub, other	Indefinite (on eHub)

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

Type of File / Record	What is included on File / Record	Retention Period
	competitions with a panel in place	
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, Job Alerts, Job Category, Job Subcategory	Information to be retained indefinitely. Candidates will have the option to delete their profile.
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	Three years Indefinite (may be deleted by the candidate except where forms part of a competition file)

Type of File / Record	What is included on File / Record	Retention Period
	Assessment details and scores	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
Selection Board Member / Assessors / Questionnaires and Details	Contact details (title, name, phone number(s), email address; postal address); service on selection boards;	Indefinite – may be deleted upon request

Type of File / Record	What is included on File / Record	Retention Period
	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.	
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	Sent to new organisation on transfer or retained

Type of File / Record	What is included on File / Record	Retention Period
	documents, civil service career history, salary and superannuation details, contracts, record of annual and other types of leave or work-life balance; PMDS ratings; training records; live disciplinary or other investigation related documentation; merit awards, next-of-kin information, education and qualifications records.	indefinitely for pension purposes
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 publicjobs staff / members of the publicjobs Board	15 years

Type of File / Record	What is included on File / Record	Retention Period
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.
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	Indefinite- transfer to National Archives

Type of File / Record	What is included on File / Record	Retention Period
	investigations into data breaches	
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 Fees and Travel Expenses for Board Members and Board of PAS	Indefinite for pension purposes 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.	Indefinite – National Archives

Type of File / Record	What is included on File / Record	Retention Period
	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.)	
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
General Correspondence (emails and letters)	Query and response	3 years in Unit directories; 7 years on mailmeter
Microsoft Teams Chat	Informal, internal communications which do	I month

Type of File / Record	What is included on File / Record	Retention Period
	not involve making business decisions and which do not constitute important correspondence	
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 interact with publicjobs.ie. These analytical tools use 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.	Files need to be kept indefinitely but identifiers removed once analysis is complete

Type of File / Record	What is included on File / Record	Retention Period
	training scores or manager/supervisor ratings	
Email Correspondence	All emails received and sent	Stored in Mailmeter for 7 years; available through Outlook for I year
Correspondence / Meetings with the Department of Public Expenditure and Reform	Records of non-campaign specific correspondence and meetings with D/PER	Indefinite Information relating to specific campaigns should be retained indefinitely on competition files
Correspondence / Meetings with Local Government Management Authority (LGMA) and the County and City Managers Association (CCMA)	Correspondence / Meetings with LGMA and CCMA	Indefinite Information relating to specific campaigns should be retained indefinitely on competition files
Correspondence / Meetings with Clients	Correspondence / Meetings with Clients	Indefinite

Important Note:
publicjobs refers to Public Appointments Service established under the Public Service Management (Recruitment and Appointments) Act 2004-2013.