Oifig an Stiúrthóra Ionchúiseamh Poiblí
Office of the Director of Public Prosecutions

Office of the DPP
Privacy Policy for Job Applicants

February 2026

Table of Contents

1. Purpose

1.1 This privacy notice explains how the Office of the Director of Public Prosecutions (ODPP) collects, uses and processes your personal data as part of the job application process. It has been prepared to demonstrate the ODPP's commitment to protecting your privacy and to inform you about the information we handle in connection with your application. The ODPP is the "data controller," which means we are responsible for deciding how your personal data is used. We are committed to processing all personal data fairly, lawfully and carefully, and in full compliance with the GDPR.

1.2 This Notice explains:

- what personal information we collect about you,
- why we collect and process it,
- how and where the information is stored,
- who we may share it with, and
- what your rights are in relation to your personal data.

1.3 By submitting a job application to the ODPP, you confirm that you have read, understood and agree to the terms of this privacy notice.

2. Types of Information we collect

2.1 During the recruitment process, we may collect the following types of data from you:

Personal Data Category	Description
Contact Data	This may include a person's email address, phone number, postal address, other communication details.
Identification Data	This may include a person's name, citizenship, date of birth, PPSN number, driving licence, passport.
Professional Data	This may include profession, employment history, skills, experience, membership of professional bodies and verification document pursuant to same.
Education Data	This may include educational history, languages, degrees, certificates, diplomas and other qualifications.
Financial Data	This may include payments and bank details, tax information, current salary/salary scale details where applicable (i.e. when transferring from an existing public/civil service position).
Health Data	This may include health information including information about any disability or illness and whether

Personal Data Category	Description
	the interviewee requires special accommodation during the interview process.
Legal Data	This may include criminal record and citizenship checks undertaken where required as part of the application process including information required to establish right to work in Ireland (The Employment Permits Acts 2003 to 2014) equal opportunities data and reference/ background check data (may include criminal offence data).
Communications Data	This may include personal data included in communications with us over email, text, phone or letter.
Application Data	This may include personal data provided as part of an application for a permanent or contract position, including information about achievements or hobbies.
Position Data	This may include information on salary/rate of pay, working hours and job description.
Interview data	This may include interview notes and assessment results.
Emergency Contact Data	This may include the name and contact details provided by applicants in case of emergency.
Web data	This may include application timestamps, IP address and length of visit to the recruitment management system.

3. How does the ODPP plan to use your data

3.1 We collect and use your personal information for the management and administration of the recruitment process. We do this to manage our relationship with you effectively, lawfully and appropriately, and to protect your rights and interests as an applicant.

We use your information for purposes including:

- **Managing your application** and assessing your suitability for the role,
- **Communicating with you** throughout the recruitment process,
- **Making informed hiring decisions**,
- **Verifying the information you provide**, including carrying out reference or background checks where required,
- **Complying with our legal and regulatory obligations**,
- **Protecting our legitimate interests**, including managing and defending any legal claims, and
- **Improving our recruitment processes**.

3.2 If you are placed on a panel and are being considered for a position, the ODPP must complete a number of pre-employment checks before deciding whether you are suitable for appointment. These checks help us confirm that you meet all required standards for the role.

Before offering an appointment, the ODPP will carry out all necessary enquiries to assess your suitability and eligibility. These checks may include:

- **confirming your citizenship** (e.g. to ensure you meet statutory eligibility requirements),
- **assessing your health** (e.g. where required to determine fitness to perform the role or to consider requests for reasonable accommodation),
- **conducting Garda vetting and obtaining security clearance** (including where required for certain public service and criminal justice roles), and
- **obtaining and reviewing references** (to verify your employment history and suitability).

If any of these checks are unsatisfactory or cannot be completed, the ODPP reserves the right to:

- remove you from further consideration for appointment, or
- end your employment if an appointment has already been made.

4. What is the Lawful Basis for processing your personal data

4.1. The ODPP processes personal data of job applicants in accordance with the General Data Protection Regulation (GDPR) and the Data Protection Act 2018.

4.2 The ODPP has a legitimate interest in processing personal data during the recruitment process and in maintaining appropriate records in order to manage recruitment competitions. This includes assessing and confirming a candidate's suitability for a role, progressing applications, and making decisions on offers of employment. The ODPP may also process personal data where necessary to respond to, or defend against, legal claims arising in the context of a recruitment process.

4.3 The ODPP may also need to process your personal data where this is necessary for entering into an employment contract with you.

4.4. In certain cases, the ODPP processes personal data to comply with legal obligations. For example, the ODPP is required to verify a successful candidate's entitlement to work in Ireland before employment can commence.

4.5 The ODPP may process special categories of personal data where necessary for the purposes of carrying out obligations and exercising specific rights in the field of employment law. This may include information relating to disabilities in order to make reasonable accommodations for candidates during the recruitment process.

4.6 The legal basis for conducting Garda vetting and obtaining security clearance is to be found under Article 10 of the GDPR and section 55 of the Data Protection Act 2018.

4.7 Further information about GDPR lawful bases can be found at Appendix A and on the Data Protection Commission Website.

4.8 If you are appointed to a role, the legal basis for processing and retaining your HR records will be explained in full in the **ODPP Employee Privacy Notice**, which will be provided to you at the start of your employment.

5. How do we obtain your information

5.1 We may collect your personal information from a variety of sources, including:

- Information you provide during the recruitment process,
- Communications with the HR or recruitment team,
- Third parties, such as referees or organisations providing background checks (with your consent where required), and
- Information received through the **Garda Vetting** process.

6. Who can access your data (Data Sharing)

6.1 Data will only be shared on a **strict need-to-know basis** and only for purposes directly related to recruitment and appointment within the Office of the DPP. Your information may be shared with:

- the **recruitment team**,
- **competition board members** (internal and external),
- relevant **managers** involved in the recruitment and appointment process,
- **IT consultants** where access is necessary for their work,
- organisations carrying out **background checks**, including **An Garda Síochána National Vetting Bureau**, and
- **legal or regulatory authorities**, where required by law.

6.2 Please take care when deciding what information to include in your application. Only provide details that are **relevant to the position** you are applying for.

7. How long will we store your data

7.1 We keep your personal data only for as long as necessary to carry out the recruitment process or to meet legal or regulatory requirements. For unsuccessful candidates, the ODPP retains all recruitment data for **one year after the competition has ended**.

7.2 If you are appointed to a position, the personal data collected during the recruitment process will be added to your HR file (in both electronic and paper formats). This information will be retained for the duration of your employment. You will also receive a separate Employee Privacy Notice. This will explain how long different types of HR information are kept and access to specific retention periods for each category of HR data will be available to you.

7.3 The processing and retention of civil service HR data must also comply with the **National Archives Act 1986**, which may require certain records to be preserved.

8. How do we store your data – security measures

8.1 We are committed to protecting all personal data submitted to us. To prevent unauthorised access or disclosure, we use a range of technical and organisational measures designed to safeguard your information. These include security technologies and procedures that help protect your data from unauthorised access, use, or disclosure.

8.2 We take all reasonable steps to prevent security breaches involving the personal data we process. These measures include:

- secure servers and encrypted storage
- access controls and authentication
- staff training on data protection and security practices

8.3 Where we use external service providers to process personal data on our behalf, we ensure they also have appropriate technical and organisational measures in place. We have received assurances that these measures align with recognised standards, including controls set out in **ISO 27001**.

9. What are your rights under data protection law?

9.1 You have the following rights under data protection law, although some may be restricted in certain circumstances:

- **Right of access**: You can request a copy of the personal data we hold about you, along with information about how we process it.
- **Right to rectification**: If any of your personal data is incorrect or incomplete, you can ask us to correct or update it.
- **Right to erasure**: In certain situations, you can request that we delete your personal data.
- **Right to restrict or object to processing**: In some circumstances, you can ask us to stop using your data for specific purposes or object to how we are processing it.
- **Right to data portability**: In some cases, you can request that your personal data be transferred to you or to another organisation.
- **Right to withdraw consent**: If we are processing your data based on your consent, you may withdraw that consent at any time. Withdrawing consent does not affect the lawfulness of any processing carried out before you withdrew it.
- **Right to lodge a complaint**: You can make a complaint to the **Data Protection Commission (DPC)** if you believe your data protection rights have been infringed. Complaints may be submitted through the DPC website using their "Making a Complaint" process - Making a Complaint to the DPC.

9.2 Further information about your data protection rights is available HERE.

10. Will you be subject to profiling or automated decision-making?

10.1 You will not be subjected to profiling or automated decision-making.

11. Transfers outside the European Economic Area

11.1 Your personal information will not be transferred, stored or processed outside the European Economic Area ("**EEA**").

12. Where can you get further information?

12.1 For questions related to the HR process contact recruitment@dppireland.ie.

12.2 If you wish to exercise your data protection rights, or if you have any questions or complaints about how your personal data is used, you can contact the **Data Protection Officer (DPO)** for the Office of the DPP by email at: data.protection@dppireland.ie or by post:

Data Protection Officer,
Office of the DPP,
Infirmary Road,
Dublin 7
D07 FHN8

12.3 The contact details for the supervisory authority in Ireland is:

Data Protection Commission,
6 Pembroke Row,
Dublin 2,
D02 X963,
Ireland.
Tel: +353 1 765 0100 or +353 1800 437 737

Appendix A: Lawful Bases for Processing Personal Data (Recruitment)

1. Consent (Article 6(1)(a))

We may process your personal data where you give clear, specific, informed, and unambiguous consent. Consent is used only where:

- you are genuinely free to agree or refuse, and
- you can withdraw consent at any time without negative consequences.

Where these conditions cannot be met, we will rely on another lawful basis.

2. Necessary for a Contract (Article 6(1)(b))

We may process personal data where necessary:

- to take steps at your request prior to entering an employment contract, or
- to administer an employment contract once in place.

This includes evaluating applications, progressing candidates through recruitment stages, and taking steps required before an offer is issued.

3. Legal Obligation (Article 6(1)(c))

We process personal data where required to comply with our legal obligations. Relevant legislation may include:

- the Public Service Management (Recruitment and Appointments) Acts 2004 and 2013
- the Employment Equality Acts 1998–2015

This basis applies where the law requires us to collect, use, or retain information during recruitment.

4. Legitimate Interests (Article 6(1)(f))

Public authorities cannot rely on legitimate interests for their core statutory functions. However, as employing staff is not a core function of the ODPP, this basis may be used for certain recruitment and employment-related activities, including:

- receiving, reviewing, copying and storing applications, CVs, references, interview notes
- routine HR administration such as emergency contacts, payroll data, pension information, and performance-related records

5. Task Carried Out in the Public Interest / Exercise of Official Authority (Article 6(1)(e))

The ODPP may process personal data where it is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the ODPP.

This lawful basis is relied upon in particular for **vetting and suitability assessments**. This includes processing personal data for the purposes of including conducting Garda vetting and related background checks.

Processing Special Category Data (Article 9)

Special category data includes information on racial/ethnic origin, political opinions, religious/philosophical beliefs, trade union membership, genetics/biometrics, health, and sexual orientation. We process such data only where an Article 9 basis applies and where necessary for recruitment or employment purposes.

Key bases include:

1. Explicit Consent (Article 9(2)(a))

Used where you have clearly and deliberately agreed (e.g., in writing) to the processing of sensitive data.

2. Employment and Social Protection Law (Article 9(2)(b)[1])

Processing may be required to meet obligations in employment, social security, or social protection law, including:

- equal opportunities monitoring
- providing reasonable accommodations
- verifying work eligibility
- meeting health and safety requirements

3. Legal Claims (Article 9(2)(f))

Processing may occur where necessary for the establishment, exercise, or defence of legal claims or where courts act in a judicial capacity.

4. Substantial Public Interest (Article 9(2)(g))

Used where processing is necessary for statutory functions carried out in the public interest, including public safety, regulatory duties, or compliance obligations.

Criminal Convictions and Offences (Article 10 GDPR)

Information relating to criminal convictions or offences is processed only where authorised by law. The legal basis for conducting Garda vetting and obtaining security clearance is provided for under Article 10 of the GDPR and section 55 of the Data Protection Act 2018, which gives further effect to Article 10 of the Regulation.

[1] See also section 46 of the Data Protection Act 2018, which gives further effect to Article 9(2)(b) of the GDPR in Irish law.