Oifig an Ard-Reachtaire Cuntas agus Ciste
Office of the Comptroller and Auditor General

Data Protection (Privacy) Policy

May 2024

1. Overview

The General Data Protection Regulation (GDPR) and the Data Protection Act 2018 give individuals (data subjects) the legal right to privacy in relation to their personal data. The GDPR and the Irish data protection legislation places obligations on data controllers including the Office of the Comptroller and Auditor General (the Office) collecting, holding and processing such data.

Personal data means data relating to a living individual who is, or can be, identified either from the data itself, or together with other data that is in, or is likely to come into, the possession of the Office. The Office may hold this data electronically or in manual files.

This policy outlines the purpose for which we collect personal data including the lawful basis for doing so, the type of personal data that we handle and the ways in which we collect, hold and process the personal data that we receive. It relates to personal data that we receive when data subjects contact us directly and personal data received by us indirectly, as outlined below.

In accordance with Article 37 of the GDPR, we have appointed a Data Protection Officer who advises us on data protection obligations, monitors compliance and is the first point of contact in dealing with data protection enquiries from individuals regarding the processing of their personal data and the exercise of their rights. The Data Protection Officer's contact details are set out in Section 9 below.

2. Why we hold and process personal data

As part of our day-to-day operations, the Office receives and holds personal data for a wide range of purposes

- ***Comptroller and Auditor General's statutory functions of audit, examination or inspection and the issue of disbursements from the Exchequer -*** in undertaking this work we access and test a variety of information to support findings and conclusions in our reports. We have a statutory right of access under Section 10 of the Comptroller and Auditor General (Amendment) Act 1993, to data held by public bodies where it is for the purpose of our audit and examination work. This data may contain personal information. The primary legal bases for processing in connection with our statutory functions are Articles 6(1)(c)[1] and 6(1)(e)[2] of the GDPR.

- ***Prescribed person under protected disclosure legislation -*** the Comptroller and Auditor General (C&AG) is a prescribed person under protected disclosures legislation for the receipt of disclosures relating to improper use of public funds and resources or matters concerning value for money in respect of entities that fall within his remit. We process personal data received in disclosures to the C&AG. The personal data may include name and contact details, details of the purpose of the contact and any other personal data provided by the discloser. The primary legal bases for this processing are Articles 6(1)(c)[1] and 6(1)(e)[2] of the GDPR.

[1] Compliance with a legal obligation to which the controller is subject.
[2] Performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

- ***Shared learning and good practice 'audit insights' events –*** we host audit insights events which share information on common recurring issues and examples of good practice identified through our financial audit and performance audit work. Personal data is provided to our Office by participants that take part in these events. This will generally include name and contact details and dietary requirements and access/facility requirements where appropriate. The legal basis for this processing is Article 6(1)(a)[3] of the GDPR.

- ***Administrative functions –*** *w*e hold and process personal data in relation to our current and former employees, suppliers, persons who make freedom of information requests and others with whom we communicate in carrying out our administrative functions. In general, the type of personal data that we process includes name and contact details, the company or organisation a person works for and other personal data that is provided to the Office during the performance of these functions. We have a separate personal data policy for staff which describes in detail the personal data held in that respect. The legal bases for processing personal information in connection with our administrative functions are Articles 6(1)(a)[3], 6(1)(b)[4], 6(1)(c)[1], 6(1)(e)[2] and 6(1)(f)[5].

3. How we handle your personal data

We fully commit to protecting your data as required under the GDPR and the Irish data protection legislation. We adhere to the key principles of data protection as set out in Article 5 of the GDPR, when processing your information. Personal data must be

- processed lawfully, fairly and in a way that is transparent to the data subject (lawfulness, fairness and transparency)
- collected, created or processed only for one or more specified, explicit and lawful purpose (purpose limitation)
- adequate, relevant and limited to what is necessary for those purposes (data minimisation)
- kept accurate and, where necessary, up-to-date (accuracy)
- retained no longer than is necessary (storage limitation)
- kept safe and secure (integrity and confidentiality).

We treat all personal data received as confidential and use such data only for the purposes that it was obtained. However, we may share data with third parties, such as other government departments or public authorities, when permitted or required by a specific legislative provision.

We ensure that information sought and retained is the minimum needed to fulfil our statutory functions and for administrative purposes.

---

3 Data subject has given consent.

4 Where the processing is necessary for the performance of a contract.

5 Legitimate interests of the Controller or a third party.

We retain data in accordance with National Archives legislation and our Records Management Policy which specifies the retention period for the records that we hold. The retention schedule for certain records series in the Office is set in certain instances by authorities outside of the Office.

4 How do we collect personal data

We collect personal data from a number of sources.

Audited bodies data

A primary source of evidence for fulfilling the C&AG's statutory functions are the records of audited bodies, enquiries from administrators, inspections and third party confirmations. Personal data may be obtained as part of this statutory function. Examples include payroll data, grant payments and payments by public bodies under various schemes, taxpayer records. We request that data provided by audited bodies is anonymised, where possible, by removing details such as names, dates of birth, addresses and personal public service numbers. Where possible data will be held on the audited body's system or transferred securely by the audited body to the Office using either the on premise secure file transfer system (File Cloud) or the Government collaboration platform (the HIVE). Data received will be retained on the Office's ICT network in accordance with our Information and Data Security Policy.

Phone / video calls to the Office

We do not record or retain recordings of phone conversations or video calls. Voicemails received by the Office may be retained. During the course of a phone/video call, we may record personal data received during the call in the form of notes.

Emails

All emails received by us are saved and can be forwarded to relevant employees / units of the Office as required with the sender's email address remaining visible. It is the sender's responsibility to ensure the content of their emails does not infringe the law. Unsolicited unlawful material, together with the details of the sender, may be reported to An Garda Síochána and/or other relevant authorities and further emails from such recipients may be blocked.

Post

All post which we receive is scanned and forwarded to the relevant employees / units of the Office to which the matter relates. Original hard copy versions of post items are filed and retained in accordance with the retention periods set in the Office's Records Management Policy.

Social Media

We operate a social media account on the LinkedIn platform to support our functions. Messages or posts received on this social media platform are viewed by us but the personal data contained in the messages/posts is not logged or stored other than on the relevant social media platform, and no further processing of such personal data is carried out by us.

CCTV

We operate closed-circuit television (CCTV) at our Dublin Office located at 3A Mayor Street Upper, Dublin 1. CCTV recordings are deleted by the Office after one month. If the recordings identify an issue, that recording will be retained in the context of an investigation of the issue.

Website

We respect the privacy of all users of our website and have a policy that outlines the use of cookies. Our website uses cookies only for functionality and monitoring website performance. It does not use any third party or persistent cookies.

5. When do we share personal data with others

We are obliged to protect the confidentiality of all information given to us. We fully commit to safeguarding data given to us from use or disclosure, except as provided for by law.

We may share your data with third parties when permitted or required by a specific legislative provision to do so, where the sharing of the personal data is necessary for the performance by the Office of its functions and where third parties are providing services for us. All transfers will be done within the requirements of the data protection legislation.

For the purposes of the GDPR and the data protection legislation, processing of personal data by contractors on behalf of the Office does not constitute disclosure.

6. Processing outside the European Economic Area (EEA)

The Office will not ordinarily transfer personal data outside of the European Economic Area or third countries. In the event that this position changes, we will comply with our obligations under Article 46 of GDPR by adopting one of the appropriate measures approved by the Data Protection Commission and the European Commission to ensure that such transfers are lawful.

7. Keeping your personal data safe

We are obliged under a wide range of legislative and administrative provisions to protect the confidentiality of official data. This includes the protection of records against unauthorised access, unnecessary use, alteration, destruction or disclosure. We take our obligations very seriously and strive to ensure that we maintain the privacy of personal data.

We employ high standards of physical and technical security to protect the confidentiality of your personal data. All staff are aware of the standard of data security expected of them. Staff access rights extend only to the data necessary to carry out their appointed duties.

We will hold accountable any employee found to be in breach of the data protection rules.

We demonstrate our accountability for data protection and compliance with our obligations under data protection legislation by

- having appropriate policies and procedures around data protection, information security, access control and records management
- an information security management system certified to ISO 27001
- ensuring internal audits are carried out of our information security management
- the appointment of a data protection officer
- ensuring employees are aware of their responsibilities under GDPR
- providing induction and regular awareness training and guidance and having an Information Security Forum in place to oversee the information security and data protection processes in the Office.

8. Your rights under GDPR

Under GDPR, you have a right to

- information (e.g. the purpose(s) for processing your data)
- access information (e.g. data which we have about you)
- rectification of your personal data
- erasure ('right to be forgotten')
- restriction of processing
- data portability and to object to processing
- not be subject to automated individual decision-making.

Section 60(3)(c)(iii) of the 2018 Act provides for a restriction on the exercise of these rights where personal data has been received indirectly for the exercise of our statutory functions. This is to ensure that the C&AG is not materially restricted in his ability to carry out his statutory and constitutional functions.

9 Making a subject access request

As a data subject you have the right to request access to your personal data. You can make an access request by contacting our Data Protection Officer using the contact details below. To help us provide your data and deal with your request more quickly, you should include sufficient details so that we can identify you.

Data Protection Officer

Data Protection Officer
Office of the Comptroller and Auditor General
3A Mayor Street Upper
Dublin 1
D01 PF72

Phone: (01) 863 8600

Email: dpo@audit.gov.ie

How soon will you receive a reply?

We will deal with your request promptly and issue a response as soon as possible. The GDPR and the Irish data protection legislation require us to issue a response within one month of receipt of the request.

We can extend the time to respond by a further two months if the request is complex or we have received a number of requests from you, but we must still let you know within one month of receiving your request and explain to you why the extension is necessary.

Can someone make an access request on your behalf?

Yes. You can ask someone else to request data on your behalf, for example, a friend, relative or solicitor. We must have your authority to do this. This is usually a signed letter authorising the person to write to us for your data and/or receive our reply.

Can we, as the data controller, ask you for clarification on your request?

Yes. Where we, as the data controller process a large quantity of information concerning you, we can request clarification from you on the information or processing activities that you want access to or information on.

Can you obtain all data held about you?

No, not always. The GDPR and Irish data protection legislation allows us to withhold personal data in certain circumstances.

Under Article 12(5) of the GDPR, where an access request is ‘manifestly unfounded or excessive’, we may, where appropriate, refuse to act on a request.

Article 15(4) of the GDPR provides a general limitation on the exercise of the right of access to information by providing that the right to obtain a copy of the personal data undergoing processing should not negatively impact ('adversely affect') the rights and freedoms of others. The Office will however, endeavour to comply with any request insofar as possible whilst ensuring adequate protection for the rights and freedoms of others.

Article 23 of the GDPR also allows for data subject rights to be restricted in certain circumstances and Section 60(3)(c)(iii) of the Data Protection Act 2018 allows us to withhold personal data where the data is kept for the performance of the statutory functions of the Comptroller and Auditor General.

Further details on restrictions of the right to access can be obtained from the Data Protection Commission website

10. Appealing a refusal

You can appeal against a refusal for access to your data directly to the Data Protection Commission. Before doing so, we recommend that you contact us to establish the circumstances and to indicate your intention to appeal to the Commission.

11. Rectifying your personal data

We make every effort to ensure that your personal data is accurate and up to date.

If you think that your personal data is inaccurate or incomplete you can contact our Data Protection Officer in writing or by email using the contact details in Section 9 above, to have it corrected or supplemented. You should set out clearly the personal data involved and the reasons why you consider it to be inaccurate and or incomplete.

Once we have confirmed that the personal data to which the request relates is inaccurate, we will rectify the data without undue delay but no later than one month after the date on which the request was received.

All employees of the Office have access to their personal data held by the National Shared Services Office which they themselves can access and update to ensure its accuracy.

12. Making a complaint

If you have concerns in relation to the manner in which we handle your personal data or if you would like to report that a data breach has occurred, you can contact our Data Protection Officer using the contact details in Section 9 above. We will investigate the matter fully and notify you of the outcome of the investigation when it is completed.

If you are dissatisfied with how we handle your personal data you also have the right to raise your concerns with the Data Protection Commission as the Irish supervisory authority. The Data Protection Commission can be contacted in the following ways

- ***Data Protection Commission website***
  www.dataprotection.ie

- ***By post***
  Data Protection Commission
  21 Fitzwilliam Square South
  Dublin 2
  D02 RD28

13. Our data protection code of practice

We have a Code of Practice for the Protection of Personal Data in place which is made available to all staff and is also available on our website.

14. Enquiries about data protection

If you have any enquires concerning data protection in the Office, you can contact our Data Protection Officer who will be happy to assist you, contact details in Section 9 above.

15. Data controller contact details

The Office is the data controller for the personal data that it processes. You can contact the Office in a number of ways which are set out on the contact page of our website.

16. Changes to our Data Protection (Privacy) Policy

This Data Protection (Privacy) Policy is reviewed annually by the Office's Information Security Forum.

17. Related Documents

The following legislation is linked to this policy:

- Regulation (EU) 2016/679 (General Data Protection Regulation)
- Data Protection Act 2018.

Last review date: *May 2024*
Next review date: *May 2025*