



Privacy Notice – Counter Fraud & Investigation

GIAA takes your privacy seriously

The Government Internal Audit Agency (GIAA) is committed to protecting personal data. This Privacy Notice sets out why and how we collect, use and look after the personal data we collect when providing counter fraud and investigation services. It applies to personal data provided to GIAA, both by individuals themselves and by others. We may use personal data provided to us for any of the purposes described in this privacy statement or as otherwise stated at the point of collection.

About us

GIAA is an executive agency of His Majesty's Treasury, providing assurance and advisory services across government.

Our services involve delivering a risk-based programme of internal audit and assurance activity that culminates in an annual report and opinion on the adequacy and effectiveness of the organisation's

framework of governance, risk management and control.

Counter fraud services

We also provide specialist services. GIAA Counter Fraud and Investigation (CF&I) is recognised as a trusted provider of independent, professional and cost-effective counter fraud services across UK Government. Our objectives are to support organisations in enhancing the consistency and quality of their counter fraud response and undertake independent criminal and civil investigations into suspicions of fraud by staff, contracted employees and providers of services to UK Government.

Our services support organisations in reducing their risk of fraud and protects against the loss of public funds.

Collecting personal data

Personal data means any information concerning an identified/identifiable living person. CF&I collects, uses, stores and transfers some personal data when providing counter fraud and investigation services to our



customers. Our policy is to only collect personal data necessary for the purposes of delivering counter fraud and investigation activities.

Where we need to process personal data to provide our services, we ask customers to provide the necessary information to the relevant data subjects regarding its use. Our customers may also refer to relevant sections of this privacy notice if they consider it appropriate to do so.

The types of personal data processed by CF&I in relation to counter fraud and investigation services include:

- Personal details - e.g., name, date of birth, National Insurance Number and gender;
- Contact details - e.g., email address, telephone number, and office location; and
- Job details - e.g., role, grade, and employee number).
- Discussion of potentially fraudulent or other criminal activity

For certain counter fraud activities, CF&I may process special categories of personal data that involve us processing data revealing racial or ethnic origin, religious or philosophical beliefs, sexual orientation, or genetic

or biometric data. It is possible that criminal offence data could also be processed.

Usually, we collect personal data from our customers, shared service Providers, or other third parties. We may also ask you to provide data about yourself by filling in hardcopy forms or online, submitting certain documentation, or by corresponding with us by phone, e-mail or otherwise. For counter fraud services we may, additionally, collect personal data from you at an interview. These interviews may be audio recorded to enable the production of accurate summary of the interview.

Using personal data

CF&I uses personal data when providing services for the following purposes:

- Counter fraud services – these services require us to process personal data to deliver investigations and counter fraud activities.

The lawful basis for this is the performance of tasks in the public interest.

- Administering and managing our



services – we may process personal data to administer and manage the Agency's business.

This may include:

- managing our relationship with current and prospective customers;
- developing and improving our services;
- maintaining and using our IT systems and website

The lawful basis for this is the pursuit of legitimate interests to administer, manage and develop our business and services.

- Undertaking quality assurance activities – we may process personal data when monitoring our counter fraud services or for quality assurance purposes.
The lawful basis for this is the pursuit of legitimate interests to ensure the quality of our services.
- Providing information about CF&I and/or GIAA - we may process personal data when developing content to illustrate our services e.g., promoting our services to current and prospective customers, or attendance at business related events.

The lawful basis for this is the pursuit of legitimate interests to promote GIAA and its services.

- Complying with law – CF&I will retain records, which may contain personal data, where there is a legal requirement to do so. This may include, for example, to support the relevant authority in criminal investigations.

The lawful basis for this is legal obligation or the pursuit of legitimate interests to meet our regulatory or professional obligations.

- Benchmarking and analysis – CF&I may use information, received when providing counter fraud services, for other lawful purposes. This includes data analysis and providing insights at a cross-government level. We de-identify any personal data prior to using the information for these purposes.

The lawful basis for this is the pursuit of legitimate interests to help our customers understand the cross-government fraud landscape.



Protecting personal data

CF&I has policies, procedures and training in place covering data protection, confidentiality and security. We regularly review these measures to prevent personal data from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed.

Sharing personal data

We may use other organisations to help us deliver our Services as agreed with customers on an engagement-specific basis. Third-party service providers will only process your personal data for specified purposes and in accordance with our instructions.

CF&I does not normally require your personal data to be transferred outside of the UK. If we do, we will put in place sufficient, appropriate safeguards to ensure the security of the data.

We may disclose your personal information to third parties if we are required to do so by law – for example, by court order, or to prevent fraud or other crime; or to protect the rights, property, or safety of our staff and/or the wider public.

Retaining personal data

We keep personal data in line with our retention policy for counter fraud records. This means such records are generally deleted or destroyed in controlled manner after three years. Interview recordings, will also be destroyed after three years, except for any recorded to compact disc which are generally only retained for 12 months from the date of the investigation closure. Additionally, we may need to retain some personal data longer for legal, regulatory or professional purposes, e.g., investigations or work involving the examination of a long-term contract.

Your rights

Individuals have certain rights over their personal data and controllers are responsible for fulfilling these rights. We provide information about these rights when they are available and how to exercise them below.

You have the right to request:

- information about how your personal data is processed;
- a copy of your personal data;
- correction of anything inaccurate in your personal data;



- erasure of your personal data if there is no longer a justification for us storing or processing it; and
- restriction of the processing of your personal data in certain circumstances.

You can also raise an objection about how your personal data is processed. If you have a request or objection, contact our Data Protection Officer (DPO).

Contacting us

Contact our Data Protection Officer (DPO) if you:

- wish to make any of the requests described above;
- have questions about anything in this document; or
- think that we have misused or mishandled your personal data.

You can also make a complaint to the Information Commissioner, who is an independent regulator.

Information Commissioner's Office

Wycliffe House

Water Lane

Wilmslow

Cheshire SK9 5AF

caserwork@ico.org.uk

Telephone: 0303 123 1113

Text phone: 01625 545860

Monday to Friday, 9am to 4:30pm

Changes to this policy

We may update this Privacy Notice from time to time. Any changes will apply to you and your data immediately. If these changes affect how we process your personal data, GIAA will publish this on the website.

Data Protection Officer
Government Internal Audit Agency
10 Victoria Street
London
SW1H 0NN
Correspondence@giaa.gov.uk