

Privacy Notice for Cabinet Office Security Management Processing

This notice sets out how we will use your personal data, and your rights. It is made under Articles 13 and/or 14 of the UK General Data Protection Regulation (UK GDPR).

YOUR DATA

Purpose

The purposes for which we are processing your personal data are:

Dealing with security incidents and queries as they arrive in the dedicated security email inbox. These can range from adding colleagues to security inductions, through to managing security incidents/breaches.

Where an incident has occurred, the team may request specific follow-up information from an individual, or relevant stakeholders, to better understand the nature of the incident, with progress logged and managed via a tracker.

Specific processing purposes include:

- For cyber security, for example detecting and analysing unusual IT usage
- For dealing with security breaches or concerns
- To maintain an incident log
- For preventing or detecting fraud
- For managing employees
- For vetting purposes, e.g. updating the vetting team with security incident information
- For ensuring legal obligations and implications of overseas travel are managed
- Providing employees with IT access

The data

We will process the following personal data in the course of security investigations:

- Name of person reporting incident & any other individuals named

- Email address
- Date of birth
- Employment details
- Location data
- Audio or video recordings from on site security teams
- Photographs from on site security teams
- Job title or grade
- Telephone number
- Criminal allegations or convictions
- Security clearance
- Work and personal overseas travel plans
- We do not see vetting records, but we update the vetting team with relevant security incident information
- Emergency contact information

Legal basis of processing

The legal basis for processing your personal data is:

It is necessary for a public function, which is to ensure the security and integrity of Cabinet Office Assets, People and Estate.

Sensitive personal data is personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation, or criminal convictions. The legal basis for processing your sensitive personal data is:

Processing is necessary for reasons of substantial public interest for the exercise of a function of the Crown, a Minister of the Crown, or a government department; the exercise of a function conferred on a person by an enactment; or the exercise of a function of either House of Parliament. The task is to ensure the security and integrity of CO Security & Estate. The processing by us of personal data relating to criminal convictions and offences or related security measures is not carried out under official authority, but is authorised because:

Processing is necessary for the purposes of preventing fraud or a particular kind of fraud; and it consists of (i) the disclosure of personal data by a person as a member of an anti-fraud organization, (ii) the disclosure of personal data in accordance with arrangements made by an anti-fraud organisation, or (iii) the processing of personal data disclosed as described in sub-paragraph (i) or (ii).

Recipients

Your personal data will be shared by us with Google (official IT platform)

As your personal data will be stored on our IT infrastructure it will also be shared with our data processors who provide email, and document management and storage services.

If we have reason to believe criminal activity has taken place we will share personal data with the police.

Your personal data may be shared with onsite Security Teams, CO Fraud, HR, Cybersecurity, GSG Investigations, or the data protection team as part of any investigation carried out. Where it is revealed that an investigation relates to a member of staff in another government department, this will be referred onwards to the other government department's security team.

Retention

Your personal data will be kept by us for 5 years

YOUR RIGHTS

You have the right to request information about how your personal data are processed, and to request a copy of that personal data.

You have the right to request that any inaccuracies in your personal data are rectified without delay.

You have the right to request that any incomplete personal data are completed, including by means of a supplementary statement.

You have the right to request that your personal data are erased if there is no longer a justification for them to be processed.

You have the right in certain circumstances (for example, where accuracy is contested) to request that the processing of your personal data is restricted.

You have the right to object to the processing of your personal data.

INTERNATIONAL TRANSFERS

As part of this processing activity, your personal data may be processed in USA and a basis of Adequacy decision

As your personal data is stored on our Corporate IT infrastructure, and shared with our data processors, it may be transferred and stored securely outside the UK. Where that is the case it will be subject to equivalent legal protection through an adequacy decision, reliance on Standard Contractual Clauses, or reliance on a UK International Data Transfer Agreement.

COMPLAINTS

If you consider that your personal data has been misused or mishandled, you may make a complaint to the Information Commissioner, who is an independent regulator. The Information Commissioner can be contacted at: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF, or 0303 123 1113, or icocasework@ico.org.uk. Any complaint to the Information Commissioner is without prejudice to your right to seek redress through the courts.

CONTACT DETAILS

The data controller for your personal data is the Cabinet Office. The contact details for the data controller are: Cabinet Office, 70 Whitehall, London, SW1A 2AS, or 0207 276 1234, or you can use this [webform](#).

The contact details for the data controller's Data Protection Officer are: dpo@cabinetoffice.gov.uk.

The Data Protection Officer provides independent advice and monitoring of Cabinet Office's use of personal information.