Independent Office for Police Conduct
Swyddfa Annibynnol Ymddygiad yr Heddlu

Appropriate policy document

Schedule 1, Part 4, Data Protection Act 2018

Processing special category and criminal offence data for employment and related purposes

Who we are

The Independent Office for Police Conduct ("IOPC")[1] was established to oversee the police complaints system in England and Wales and maintain public confidence in it.[2] Our powers and duties are principally set out in the Police Reform Act 2002 ("PRA") and associated regulations. In order to fulfil our statutory remit we carry out independent investigations into alleged misconduct and deaths or serious injuries following police contact. We also determine appeals from local police investigations into a complaint. We use learning from our work to influence changes in policing with a view to promoting best practice. We do this by making public statements, outreach work with stakeholders, making organisational recommendations, carrying out research, analysis and collating statistics in order to produce and publish thematic reports

For further information on what we do, please visit our website.

What this policy does

This policy explains how and why the IOPC processes particularly sensitive personal data about you to administer our employment or contractual relationship with you and related activities, in accordance with the data protection principles set out in the General Data Protection Regulation 2016 (GDPR). Sensitive personal data can only be processed lawfully if it is carried out in accordance with this policy. IOPC staff must therefore have regard to this policy when carrying out sensitive personal data on behalf of the organisation.

[1] Formerly the Independent Police Complaints Commission. The IOPC was established on 8th January 2018.
[2] We also oversee the complaints system for other organisations, such as HMRC, the National Crime Agency, and the Gangmasters and Labour Abuse Authority.

Our approach to data protection

The IOPC is committed to an information assurance and data governance framework that is clear and accessible and which ensures that the collection and processing of personal data is carried out in accordance with the GDPR and the Data Protection Act 2018 (DPA). This information assurance and governance framework underpinned by a scheme of delegation and a decision-making framework ensuring that data protection is explicitly considered by our staff and senior leaders, including our Senior Information Risk Owner. We are further seeking to foster a culture of data protection by design and default by developing a business-wide data protection manual. This manual is planned to guide users through new processes, ensuring data protection is at the heart of the decisions we make.

The IOPC values openness and transparency, and we have committed to and published a number of policies and processes to assist data subjects and to explain how we handle personal data. These include a retention and disposal schedule and privacy notices which describe what information we hold, why we hold it, the legal basis for holding it, who we share it with, and the period we will hold it for.

The IOPC has built a network of Information Asset Owners who are responsible for ensuring that the information their department collects is necessary for the purposes required and is not kept in a manner that can identify the individual any longer than necessary. They are collectively responsible for ensuring that the IOPC Information Asset Register is kept up to date and accurately reflects the information the IOPC holds and the lawful basis for holding it. This network is supported by every member of staff undertaking mandatory data protection training each year and agreeing via a signed declaration that they will abide by the relevant legislation, that they understand the processes and policies the IOPC has in place to ensure that it is compliant, and that they understand how data protection fits into their job.

Due to the nature of work performed at the IOPC, the organisation often needs to share information with other parties. The IOPC has a suite of Information Sharing Agreements that govern the transfer of information between parties. In addition, the IOPC Information Asset Register clearly lays out the categories of recipients with whom information is shared.

The data protection principles

In summary, Article 5 of the GDPR states that personal data shall be:

- processed lawfully, fairly and transparently
- collected for specific and legitimate purposes and processed in accordance with those purposes

- adequate, relevant and limited to what is necessary for the stated purposes
- accurate and, where necessary, kept up-to-date
- retained for no longer than necessary; and
- kept secure.

Special category data and criminal offence data

Special category data

Personal data refers to any information by which a living individual can be identified. Individual identification can be by information alone or in conjunction with other information. Certain categories of personal data have additional legal protections when being processed. These categories are referred to in the legislation as “special category data” and are data concerning:

- health
- racial or ethnic origin
- political opinions
- religious or philosophical beliefs
- trade union membership
- genetic data
- biometric data
- sex life or sexual orientation

Criminal offence data

The processing of criminal offence data also has additional legal safeguards. Criminal offence data includes information about criminal allegations, criminal offences, criminal proceedings and criminal convictions.

Special category and criminal offence data we process about you

If we process personal information about you, you are a “data subject.” You might be:

- a current employee
- a previous employee
- a prospective employee

- agency staff
- an apprentice
- a consultant
- a student or intern
- a contractor
- a secondee
- an individual representing a 3rd party service provider supplier (for example a representative of our Occupational Health providers or of the administrators of our payroll).

The IOPC collects and retains special category and criminal offence data where it is necessary for your prospective, current or previous employment with the IOPC and related functions. We will also collect and retain this data where you carry out work with us or provide your services to us under any other contractual arrangement. We use this data in order to fulfil our obligations to you as our employee and any legal obligations we may have as an employer or under our contractual arrangement. We will also share this data with relevant third parties where necessary (please see the section "Who we share your data with" below).

We will collect your personal data from a number of different sources including: you, your family members, your referees, previous or current educational establishments you have attended or are attending, your previous or current employer, a health care provider and / or an occupational health provider, your GP, your agency, your Union, the police, security agencies, government departments, the College of Policing, third party service providers (including providers for our recruitment platform, our internal HR function IT systems and the administration of our childcare voucher scheme), Civil Service Learning and other providers of learning management systems or training, the Disclosure and Barring Service (DBS), Disclosure Scotland, your bank, HMRC and your pension provider.

The special category data we collect and process about you may include, but is not limited to, the following: medical information (e.g. for the purposes of carrying out reasonable adjustments under the Equality Act 2010, risk assessments and the application of our sickness policy); your race or ethnic origin and/or your religious beliefs and sexual orientation (e.g. for equal opportunity monitoring, when compiling statistics and conducting analysis for the purposes of the Equality Act 2010 or responding to a request under the Freedom of Information Act 2000). Where possible we will anonymise your data.

We also process information provided by your trade union for the purpose of administering your subscription via the payroll.

As part of an enhanced security clearance required for some employees we may obtain and process special category data regarding your personal relationships.

The IOPC does not keep a comprehensive register of the criminal convictions or cautions of prospective or current staff. However, as part of our pre-employment processes each individual will be subject to security clearance that will include obtaining information regarding any criminal convictions or cautions both from you and from third-parties. The IOPC will retain this information during the period of your employment and afterwards in certain circumstances.

Employment and related purposes

The employment and related purposes for which we will process special category and criminal offence data include:

- to maintain accurate employment records
- to provide references
- for recruitment and selection purposes (including your right-to-work and residence status)
- to operate the payroll (including the reimbursement of expenses), administer your pension and any other benefits as appropriate, this will include processing information such as your salary, dependents, government identifiers such as your national insurance number and your bank account details
- to make reasonable adjustments for prospective and current employees and to obtain occupational health advice
- to keep a record of your contact details (including emergency contact details)
- to carry out pre and post-employment vetting procedures including a DBS check and other security clearance procedures
- for monitoring staff use of IOPC systems in accordance with our security policies, including access to premises, computer and telephone use and reporting data breaches or suspicious activities where appropriate
- for monitoring IOPC premises (including by CCTV) for the purposes of protecting the IOPC and its workforce against injury, theft, legal liability fraud or abuse
- to facilitate, maintain accurate records of and ensure compliance with IOPC workplace management policies (including sickness, annual leave and other types of leave, poor performance, disciplinary, grievance, whistleblowing and information security)
- to operate and keep a record of other types of leave such as maternity leave and adoption leave
- for investigating serious complaints made against IOPC staff. Such complaints are managed by the IOPC's Internal Investigations Unit (IIU).[3]
- to monitor staff compliance with the IOPC Code of Conduct, Conflicts of Interest Register and Hospitality and Gifts Register

[3] In accordance with the IPCC (Staff Conduct) Regulations 2004

- to monitor attendance at and participation in work-related training events in-house, externally and online (for example via the Civil Service Learning website)
- to monitor recruitment and performance-related data such as objectives, comments, feedback, skills and competencies, work related qualifications and other information relevant to the Personal Development Records of staff
- to produce relevant statistics and conduct analysis for compliance with equality legislation
- to monitor and report on equal opportunities
- to make appropriate disclosure for the purposes of employment and other related legal proceedings
- to promote the IOPC through promotional videos and literature
- to perform our contractual obligations with third party suppliers and service providers

The legal basis for processing your special category and criminal offence data

Contract and legal obligation

If you are an employee we will collect and process your special category or criminal offence data, including providing it to third parties, where it is necessary to do so for the performance of our employment contract with you or where we have a legal obligation to do so (for example making reasonable adjustments in accordance with the Equality Act 2010).[4]

If you carry out work with us or provide your services to us under any other contractual arrangement we will collect and process your special category or criminal offence data, including providing it to third parties, where it is necessary to do so for the performance of that contract.

Consent

As a prospective employee (prior to you entering into a contract of employment with us) we will only collect and process your special category or criminal offence data on the basis of your explicit consent to do so. You can withdraw your consent at any time. However, if you do withdraw your consent or refuse to provide the data required for the recruitment process we may not be able to progress your application properly or at all.

As a current employee there may be occasions where it is necessary to seek to your explicit consent to process your special category data. For example where you request and use a Personal Security Device which has the capacity to relay information about your health to the third party service provider of such devices your consent will be required.

Whenever we want to process your data by consent, prior to giving your consent you will

[4] Article 6(1) (b); Article 9(2)(b); Article 10 GDPR. Section 10(5) and Part 1 (1), Schedule 1 DPA 2018.

be provided with a consent form. This will explain:

- what you are being asked to agree to and why
- how your data will be used
- the names of any third party controllers that will be relying on the consent;
- your right to withdraw your consent at any time;
- the process through which you can withdraw your consent
- who to contact if you have any concerns about the use of your data

Necessary for the performance of a task carried out in the public interest

It is important us that we employ the right individuals to carry out certain roles within the business. This may mean on occasion we will ask an expert, not employed by the IOPC, from a particular field, for example IT, security, or finance, to sit on an interview panel in order to help make a decision on the expertise of the candidates at interview. We believe that it is necessary to have such experts used in this way as it ensures that we employ the right individuals to help aid and facilitate the carrying out of our tasks as a public authority.

Equal Opportunity Monitoring

Special category data may be processed by us where it is necessary for the purposes of identifying or keeping under review the existence or absence of equality of opportunity or treatment between groups of people specified in Schedule 1, Part 2, paragraph 8(2) of the Data Protection Act 2018. This processing will be with a view to enabling equality to be promoted or maintained and is not carried out for the purpose of measure or decisions with respect to a particular data subject. Such processing will not be carried out where consent has been declined or you have given notice that you do not wish your data to be processed for these purposes. It will only be carried out where it is not likely to cause substantial damage or distress to an individual. Any data used for this purpose will be anonymised.

Legitimate Interests

There are some circumstances where we will process special category data on the basis that the IOPC has a legitimate interest in doing so. For example, when we collect information about who to contact in an emergency and CCTV monitoring is used in workplace premises. We consider that ensuring we have contact details in the event of an emergency involving our staff and safeguarding the security of our premises and the information held in them are legitimate interests.

We will always seek to balance our legitimate interests with the fundamental rights and freedoms of data subjects.

Who we share your personal data with

For the employment and related purposes set out above we will need to share your special category and criminal offence data with third parties. The categories of persons we share your data with are:

- our payroll provider
- our pensions provider
- work-related benefit providers (for example the administrators of our childcare voucher scheme)
- HMRC and other government departments
- public bodies
- Interview panels
- our healthcare provider and / or our occupational health provider
- your bank (for example when you ask us to assist with a mortgage application)
- Disclosure Scotland and The Disclosure and Barring Service (for the purposes of security and other vetting procedures)
- the IOPC's Internal Investigations Unit (IIU)
- employment agencies
- third-party suppliers and service providers (e.g. the providers of our Personal security Devices and our internal HR function IT systems)
- the public (for example for the purposes of transparency the IOPC will publish relevant details of senior staff from its Hospitality and Gifts Register and Conflicts of Interests Register)

We are also required to share your data with a third party where there is a legal obligation to do so. We share information with other public bodies and government departments in order to facilitate the exercise of their statutory or other public functions. The categories of persons we share your data with are:

- coroners
- the Crown Prosecution Service
- courts and tribunals
- public bodies (for example, the College of Policing)
- the Information Commissioners' Office
- police forces and other law enforcement agencies
- regulatory bodies or ombudsmen including HMICFRS, HMIP, and the Health and Safety Executive
- professional advisers, experts and consultants

Automated decision making

Our recruitment process includes some automated decision making whereby specified responses to questions such as your right to live and work in the UK will result in your

application being automatically terminated.

How we keep your data secure and how long we keep it for

The IOPC deploys a wide range of Technical and Procedural controls in order to protect the personal data it holds and processes. These controls are deployed after an Information Risk Assessment and under the oversight of a duly constituted Information Assurance Governance Committee (Security Working Group) Chaired by the Head of Information Technology (IT) Security. Residual Information Risk is accepted on behalf of the IOPC by the Senior Information Risk Owner.

The controls are aligned to the ISO27001 Information Assurance Standard and Information Risks are assessed according to the ISO27005 International Standard. Controls include but are not limited to:

- Mandatory annual Information Security Training for all staff
- Acceptable use of IT equipment and systems defined in Security Operating Procedures signed by all users of IOPC systems
- Role Based Access Controls, limiting IOPC system users to only access those systems necessary for them to perform their duties
- Identity and Access Management through Human Resources hiring and reference polices, including HMG Security Clearances. External access to IOPC systems is governed by two-factor authentication and is only granted to new employees or contractors after security checks and a security briefing by specialist IT Security staff
- Strong defences of the IOPC core IT system (e.g. Firewalls, Malware Detection & Defence)
- Encryption of Data both at rest and in transit across dedicated IOPC networks where appropriate
- Monitoring and / or logging of digital and user activity into, within and out of IOPC systems
- Deployment of Information Security Tools (e.g. Data Loss Prevention, Mobile Device Management, Secure External Email)
- Assurance of IOPC Technical Security Architecture by Independent 3rd party partners
- Independent Accreditation of IOPC Systems; contractually enforced
- Requirement for all 3rd party IOPC Data Processors to be certified against the ISO27001 Standard or, where appropriate, the NCSC ‘Cyber Essentials’ framework
- Annual and ad-hoc IT Health Checks and Penetration Tests by independent CHECK certified test teams; with follow-up treatment of identified vulnerabilities
- Robust procedures for the reporting of any data or potential data breaches.

The IOPC reviews and revises these controls as part of ongoing Security Improvement Plans

The IOPC has a retention and disposal schedule which lists the data we hold and how long we hold it for. To find out how long we keep your data please see our Corporate and Operational Retention & Disposal Schedules.

Your rights in relation to the data we hold

Data protection legislation provides you with a number of rights relating to your personal data. These rights are subject to some specific exemptions. Your rights may include:

- the right to access your data
- the right to have your data corrected if it is wrong or incomplete
- the right to request restrictions to the processing of your data
- the right to object to your data being processed
- the right to have your data erased
- the right to be informed about how your data is processed
- rights relating to automated decision making and data portability

You should keep us informed of any changes to your information so that we can be confident that the data we hold about you is accurate.

To understand more about these rights are and how to exercise them please see our webpage.

Our Data Controller and Data Protection Officer

Our data controller is the Director General. The data controller has overall control of the purpose for which and the manner in which we obtain and process personal data and who must ensure that this is done in accordance with the data protection principles.

The IOPC also has a designated Data Protection Officer and a Freedom of Information and Data Protection Team. This team is responsible for:

- facilitating data subject rights and making key decisions such as whether the applicant has a right to access the data requested
- supporting an Information Assurance Board, chaired by the organisation's SIRO, in holding the organisation to account for its data protection practices
- leading cooperation with the Information Commissioner's Office for the organisation
- deciding whether a data protection impact assessment is needed where a change in business processes is proposed and advising to ensure compliance with relevant data protection laws
- responding to concerns from the public in relation to how the IOPC processes personal data
- advising whether any proposed data processor would be data protection compliant

- carrying out investigations into any data breach within the business and recommending appropriate changes to ensure best practice methods are adhered to
- providing independent advice to the organisation on its data protection obligations and reporting instances where the DPO advice has not been followed to senior management

If you have any queries or concerns about exercising your data rights or the way in which we collect, handle or process your data, please contact the team either via the contact us page of our website or by emailing dpo1@policeconduct.gov.uk.

Alternatively you can contact our switchboard on 0300 020 0096 between 9am and 5pm, Monday to Friday.

Your right to complain to the Information Commissioner

If you are unhappy with any aspect of the way in which we have processed your personal data, you have the right to make a complaint to the Information Commissioner's Office:

Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF
www.ico.org.uk
Tel: 0303 123 1113
casework@ico.org.uk

Feedback or complaints about our service or staff

If you want to give us feedback or make a complaint about our service or staff please contact our Internal Investigation Unit either through the contact us page of our website or by emailing IIU@policeconduct.gov.uk.

Alternatively you can contact our switchboard on 0300 020 0096 between 9am and 5pm, Monday to Friday or leave a voicemail message at any time on 0207 166 3261.

Review of this policy

This policy will be regularly reviewed and may be revised. Please visit our website to check for any updates.