Swyddfa Annibynnol Ymddygiad yr Heddlu
Independent Office for Police Conduct

Appropriate Policy Document

Schedule 1, Part 4, Data Protection Act 2018

Processing special category and criminal offence data for the purposes of investigations, appeals and our other core functions.

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[3]. In order to fulfil our statutory remit we:

- independently investigate deaths and serious injuries following police contact and the most serious and sensitive allegations of misconduct against those working for the police. This includes officers, staff, special constables and contractors providing services to the police. Where appropriate this can be a criminal investigation
- oversee investigations carried out by police forces into allegations of misconduct against those working for the police (where we have decided not to investigate them independently)
- direct police forces to hold misconduct proceedings for a person/s working for the police, where appropriate
- determine appeals from members of the public who are not satisfied with the way the police have dealt with their complaint
- use learning from our work to influence changes in policing and promote best practice. We do this through outreach work with stakeholders, making public statements, making organisational recommendations, carrying out research and collating statistics in order to produce and publish thematic reports

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

[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.
[3] The key regulations that govern what we do are the Police (Complaints and Misconduct) Regulations 2012 and Police (Conduct) Regulations 2012.

What this policy does

This policy explains how and why the IOPC collects, processes and shares particularly sensitive personal data about you in order to carry out our functions, 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 processing on behalf of the organisation.

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

The IOPC collects, processes and shares special category and criminal offence data where it is necessary in order to carry out our functions. If we process personal information about you, you are a "data subject." Below is a non-exhaustive list of categories of data subjects who we might process information about:

- complainants
- subjects or suspects (i.e. those whose conduct is under investigation)
- witnesses
- interested persons[4]

[4] An "interested person" is usually a family member of a person who has died or been seriously injured following police contact but may be anyone who the IOPC deems to have a sufficient interest in the matter under investigation.

- victims or survivors
- members of the public (i.e. who contact us with a general enquiry or whom we might speak to during the course of an investigation but who are not witnesses)
- an individual acting on behalf of a police force or any other data subject
- medical professionals
- a police and crime commissioner or equivalent or a member of his/her staff

We collect and retain special category and criminal offence data that is relevant to the matters we are investigating, the determination of an appeal or to any of our functions described above. We will share this data with third parties where necessary (please see the section "Who we share your data with" below).

We will collect your special category and criminal offence data from a number of different sources including: you, your family members, victims or survivors, witnesses, interested persons, subjects and suspects, members of the public, the police and other law enforcement agencies, courts and tribunals, security agencies, government bodies and agencies and medical professionals.

We use special category and criminal offence data obtained during our investigations and appeal work in our strategic work including research and statistical analysis. We also use it to seek feedback from those affected by our work to help us make improvements. Where possible, we anonymise data. We include personal data in our public statements when it is in the public interest to do so.

We also obtain and process this data for other statutory and legal obligations including, but not limited to:

- responding to data subject requests under data protection legislation
- responding to Freedom of Information Act requests
- in connection with our duties under the Equality Act 2010
- in connection with our duties under Environmental Information Regulations

We may also process your special category or criminal offence data if you are not directly involved in a particular investigation, but we come into contact with you for any other reason that is related to our functions, as set out above.

The IOPC does not keep a comprehensive register of criminal convictions. However, owing to the nature of our investigations we often generate, or are provided by third parties with, data about criminal allegations, offences, proceedings and convictions.

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

As a public body it is necessary for us to process your special category and criminal offence data in order to fulfil our functions under the PRA. These functions are carried out in the public interest.[5] We will only process it where it is necessary owing to a substantial public interest arising from maintaining public confidence in the police complaints system.[6]

[5] Article 6(1)(e) GDPR; section 8 DPA 2018;
[6] Article 9(2)(g) GDPR; s.10 and part 2 (6) schedule 1, DPA 2018.

Processing for the purposes of law enforcement[7]

When we conduct an investigation for the purposes of law enforcement (for example, a criminal investigation) the IOPC is a "competent authority" under the Data Protection Act 2018. In these situations, we must process your special category and criminal offence data in order for to fulfil our statutory functions under the PRA[8]. Where we process this data it will be because:

- it is necessary to do so owing to the substantial public interest that arises from us carrying out our functions under the PRA to maintain confidence in the police complaints system
- of the wider public interest in securing the prevention, investigation and prosecution of criminal offences
- we are under a duty to provide the police or other law enforcement agencies with this data to enable them to investigate a suspected offence

Special category and criminal offence data processed for dual purposes

There may be circumstances when it will be necessary to process all types of personal data for both law enforcement and non-law enforcement purposes. For example, there may be an investigation into several allegations of misconduct only some of which are potentially criminal. Personal data which we obtained for a law enforcement purpose may also be used in disciplinary investigations, proceedings and unsatisfactory performance proceedings. These purposes are authorised by the PRA and associated regulations.

Who we share your personal data with

We are required to share your data with third parties where we have a legal obligation to do so. We also 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 special category and criminal offence data with are:

- the College of Policing
- coroners
- the Crown Prosecution Service
- courts and tribunals
- government bodies
- the Information Commissioners' Office
- police forces and other law enforcement agencies
- the Criminal Case Review Commission
- regulatory bodies or ombudsmen including HMICFRS, HMIP, the Health and Safety Executive, the General Medical Council and the Nursing and Midwifery Council
- professional advisers, experts and consultants

We share special category and criminal offence data with complainants, interested persons, subjects/suspects in our investigations and with stakeholders where it is necessary to do so for the proper performance of our functions under the PRA.

[7] Law enforcement is defined in Part 3, chapter 1, s.31 Data Protection Act 2018 as: *"the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties including the safeguarding against and prevention of threats to public security."*

[8] Part 3, chapter 2 (35) (5) DPA 2018.

Automated decision making

Currently, the IOPC undertakes no automated decision making in relation to your personal data.

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, including your special category and criminal offence 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 FOI and DP page on the website.

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 call us 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 subject to revision. Please visit our website to check for any updates.