Data protection

This page is from APP, the official source of professional practice for policing.

First published 24 October 2014 Updated 17 October 2023
Written by College of Policing
24 mins read

Some links on this page are only available to authorised users who are logged on to the **Knowledge Hub** and are members of the **National Police Chiefs' Council (NPCC) Data Protection Knowledge Hub Group**.

Authorised professional practice (APP) on data protection has been produced to assist police forces in their statutory responsibility to comply with the **Data Protection Act 2018 (DPA)** and **UK General Data Protection Regulation (UK GDPR)**. The DPA replaced the Data Protection Act 1998 in 2018 and the UK GDPR replaced the EU GDPR in 2021 following the UK's withdrawal from the EU.

Data protection is a core requirement to support effective policing. It identifies the structures, responsibilities, policies and processes that must be in place to ensure consistency in the way the DPA and UK GDPR are applied throughout the police service.

The target audience for the APP is primarily officers, staff and others working for the police, information asset owners, senior information risk owners, senior managers, and chief officers in their capacity as controllers. A separate, more detailed **NPCC Data Protection Manual of Guidance** has been produced for police data protection professionals.

The APP helps create an environment across the police service in which compliance can be achieved, providing the policing business with professional guidance and assistance in interpreting the DPA and UK GDPR.

The APP covers police use of personal data for both law enforcement purposes and for supporting functions, such as those carried out by administration staff.

See also our briefing note about compliance auditing.

Data protection introduction

UK GDPR and data protection

The current legislation regarding data protection implemented in the UK in May 2018 and January 2021. It consists of two elements.

- The **UK GDPR**, which deals with the processing of personal data for non-law enforcement purposes, referred to as ‘general processing’ in this guidance.
- The **Data Protection Act 2018**, which, in addition to the UK GDPR specifically concerns the processing of personal data for law enforcement purposes in Part 3 of the DPA.

This dual requirement with differing regimes for general processing and law enforcement processing is more complex than the single approach contained within the Data Protection Act 1998.

Definitions

The DPA and UK GDPR define key terms which are simplified below. More detailed definitions can be found in the guidance issued by the **Information Commissioner** or within the legislation itself (DPA and UK GDPR).

Personal data

Personal data is any information which could be used on its own or combined with other information from within the police service or public domain to identify a living person.

Examples include a person’s name, address, phone number, email address, IP address, photograph or video recording.

If a person cannot be identified then data protection legislation does not apply. Anonymisation is a means of converting personal data into a form in which the individuals concerned are no longer identifiable – this is classed as anonymised data.

Data subject

This is the person to whom the personal data relates.

Examples include a suspect, offender, convicted person, witness, police officer, and police staff member.

Processing

This is an activity that personal data is subjected to.

Examples include the creating or obtaining, storing, accessing, amending, sharing, and deleting of data.

Law enforcement processing and law enforcement purposes

This is processing of personal data by the police and other competent authorities for law enforcement purposes, which are defined as: the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.

Competent authorities

These are organisations defined in **DPA Schedule 7** or any other body which has a statutory function for any of the law enforcement purposes. Police forces funded by the Home Office are classed as competent authorities.

General processing

For the purposes of this guidance this is processing of personal data which is not law enforcement processing, for example, HR and procurement.

Controller

This is the person who determines the purpose and means by which the processing of personal data occurs. Within the police service, the controller is the chief officer, namely, the chief constable of each force or, in the case of the Metropolitan Police or City of London Police, the commissioner.

Processors

Processors are individuals or organisations who process personal data for, or on behalf of, police forces.

Special category data

This is personal data which the UK GDPR states is more sensitive, therefore it needs more protection.

This is related to general processing and law enforcement processing and includes personal data about a person's:

- race
- ethnic origin
- politics
- religious or philosophical beliefs
- trade union membership
- genetics
- biometrics
- health
- sexual lifestyle or sexual orientation

Criminal offence data for general processing purposes

This relates to general processing and is a type of personal data related to criminal allegations, proceedings or convictions.

Governance

Introduction

A governance structure is in place across the service to ensure compliance with the DPA and UK GDPR. The following posts and measures form an important part of that structure. Further details for these can be found in the **NPCC Data Protection Manual of Guidance**. (This link is available to authorised users who are logged on to the **Knowledge Hub** and are members of the **NPCC Data Protection Knowledge Hub Group**).

Information Management & Operational Requirements Co-ordinating Committee (IMORCC)

The NPCC committee IMORCC is chaired by a chief officer. It oversees, among others, the following areas on behalf of the police service:

- data protection and freedom of information
- records management
- information assurance
- information sharing
- data quality
- disclosure and barring

IMORCC promotes compliance, consistency and a corporate approach across the service. It also assists chief officers in interpreting data protection in the police environment.

Chief officer ? controller

Each chief officer, as a controller, has a legal responsibility to ensure their force complies with the DPA and UK GDPR. They cannot delegate this legal responsibility.

In some cases, the chief officer may be the sole controller. In other circumstances, they may also be a joint data controller with one or more controllers. Where there are joint controllers, the DPA and UK GDPR require a written agreement setting out the nature of that relationship with regards to data protection.

Senior manager

The chief officer must designate an officer of NPCC rank or equivalent to:

- support and oversee the management of data protection matters
- ensure that force policies, procedures and guidelines reflect the requirements of this APP

The manager also performs the function of senior information risk owner (SIRO).

Senior information risk owner (SIRO)

By designating a SIRO, a police force demonstrates that there are measures in place, at senior level, to protect information held by the police force, including personal data. The SIRO has a range of key duties which are described within the **NPCC's SIRO Handbook**.

Information asset owner

An information asset owner (IAO) is responsible for all information in their business area.

An IAO has a range of responsibilities which are described within the **NPCC's IAO Handbook**.

Data protection officer

The DPO is a post required by the DPA and UK GDPR. Their primary role is to support their force's compliance with that legislation, and also to ensure that the data subjects' rights are upheld.

Further guidance on the DPO role can be found in the **NPCC Data Protection Manual of Guidance** and a **DPO role profile** has been published by the College of Policing.

All officers, staff and others working for the police

Every police officer, member of police staff, police community support officer, special constable, volunteer, processor, contractor and approved persons working for or on behalf of the police who have access to personal data are required to comply with the requirements of the DPA and UK GDPR, and any supporting local policy or procedure designed to help establish compliance.

Information Commissioner

The **Information Commissioner** is the UK's independent authority set up to uphold information rights in the public interest, promote openness by public bodies and data privacy for individuals.

The Information Commissioner can take enforcement action for non-compliance with the DPA and UK GDPR, which includes issuing monetary penalties.

Data protection training and guidance

The College of Policing and the NPCC have developed a suite of data protection-related training products for police officers, staff and others to undertake. These include:

- e-learning for information management (**operational** and **non-operational**)
- **foundation e-learning for data protection police professionals**
- modular training is delivered by the National Police Freedom of Information and Data Protection Unit (NPFDU) for data protection and FOI practitioners.
- annual update videos

Training should be refreshed or repeated annually, and records of training maintained as they are likely to be subject to inspection by the Information Commissioner.

The College has produced other APP related to Data Protection APP, namely, the Management of Police Information, Sharing Police Information, Freedom of Information and Information Assurance (Security).

The **NPCC Data Protection Manual of Guidance** contains detailed guidance, primarily for police data protection professionals (available to authorised users who are logged on to the **Knowledge Hub** and are members of the **NPCC Data Protection Knowledge Hub Group**). The Information Commissioner's website includes considerable **guidance on data protection matters**.

Data protection principles

Introduction

The DPA and UK GDPR each introduced six data protection principles for law enforcement processing and general processing respectively.

Both sets of principles are broadly consistent with one another. The most significant difference between the two regimes is that the law enforcement processing principles do not specifically make reference to transparency.

Whenever a police force processes personal data the law requires that the principles must be complied with, though there are some exemptions which mean in some circumstances parts of the principles do not apply.

A failure to comply with the principles is a breach of the DPA and/or UK GDPR and may lead to enforcement action by the Information Commissioner.

In simplified form, the principles require:

1. lawfulness, fairness (and transparency in the case of general processing)
2. purpose limitation
3. data minimisation
4. accuracy
5. storage limitation

6. integrity and confidentiality (security)

In addition, police forces must ensure they demonstrate compliance with the six principles.

More information on the principles can be found on the **Information Commissioner's website** or in the legislation (DPA and UK GDPR). Detailed guidance is also available in the **NPCC Data Protection Manual of Guidance**.

First principle – lawfulness, fairness (and transparency)

For law enforcement processing this principle requires the processing to be:

- necessary for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security
- targeted and proportionate and not carried out if it is possible to reasonably achieve the purpose by alternative, less intrusive means
- fair to data subjects, but only where doing so would not prejudice law enforcement purposes – fairness requires being clear and open with data subjects about how their information is used, in keeping with their reasonable expectations

In addition, for law enforcement processing, where sensitive processing occurs it must be strictly necessary, it must meet a **DPA Schedule 8 condition**, and an appropriate policy document must be in place to demonstrate compliance, safeguards and processes.

For general processing, this principle requires the police:

- to identify valid grounds (known as a 'lawful basis') for collecting and using personal data
- to ensure a **UK GDPR Article 6(1)** condition is met
- to ensure that it does not do anything with the personal data in breach of any other laws
- to use personal data in a way that is fair, meaning it must not be processed in a way that is unduly detrimental, unexpected or misleading to the data subjects concerned
- to be clear, open and honest with people from the start about how their personal data will be used

If general processing involves special category data, a **UK GDPR Article 6(2)** special processing condition must be met. Additionally, if the processing involves criminal offence data, it must comply

with **UK GDPR Article 10**.

Second principle – purpose limitation

For law enforcement processing, this principle requires the processing to be:

- for a defined law enforcement process
- specified, explicit and legitimate
- compatible with the original reason and justification for processing

For general processing this principle requires the police:

- to be clear about what the purposes for processing are from the start
- to record the purposes as part of their documentation obligations and specify them in privacy information for individuals
- to only use the personal data for a new purpose if either this is compatible with your original purpose, or if consented to by the data subject, or there is a clear basis in law to do so

Third principle – data minimisation

For law enforcement and general processing this principle requires the personal data to be:

- adequate – sufficient to properly fulfil the stated purpose
- relevant – has a rational link to that purpose
- limited to what is necessary – the police will not hold more than is needed for that purpose

Fourth principle – accuracy

For both law enforcement and general processing this principle requires:

- all reasonable steps to be taken to ensure the personal data is not incorrect or factually misleading
- the personal data to be updated in certain circumstances, depending on what it is being used for
- to correct or erase incorrect or misleading personal data as soon as possible where reasonable
- the police to carefully consider any challenges to the accuracy of personal data

In addition, for law enforcement processing, as far as possible:

- a distinction must be made between personal data that is based on fact and that which is based on opinion or assessment; and
- where relevant, a distinction is made between different categories of data subjects such as suspects, convicted persons, victims, witnesses and others

Fifth principle – storage limitation

For both law enforcement and general processing this principle requires:

- personal data not to be retained for longer than it is needed
- the police to consider, and be able to justify, how long personal data is retained for, depending on the purposes for holding that information
- a policy setting standard retention periods wherever possible, to comply with documentation requirements
- periodic review of the personal data held, and erasure or anonymisation when it is no longer needed
- careful consideration of any challenges to the retention of personal data. Individuals have a right to erasure if that information is no longer needed

In addition, personal data can be kept for longer if the police are only keeping it for public interest archiving, scientific or historical research, or statistical purposes.

Sixth principle – integrity and confidentiality (security)

For both law enforcement and general processing this principle requires appropriate security measures to be in place to protect the personal data held. ‘Appropriate security’ includes ‘protection against unauthorised or unlawful processing and against accidental loss, destruction or damage’.

The Information Commissioner has produced **guidance on security**.

Accountability

The ‘accountability principle’, as it is termed by the Information Commissioner, requires the police to have appropriate measures and records in place to be able to demonstrate compliance with the data protection principles.

Data breach

A data breach is defined by the DPA and UK GDPR as a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed. This includes breaches that are the result of both accidental and deliberate causes.

The **DPA s 67** and **UK GDPR Article 33** require police forces to report serious data breaches to the Information Commissioner within 72 hours of identifying them. Where the breach is likely to result in a high risk of adversely affecting data subjects' rights and freedoms, it is also required to inform those individuals without undue delay (**DPA s 68**).

Police forces must have measures in place to manage data breaches.

Once identified, any potential data breach and/or security incident must be reported in line with force policy and procedure so that it can be managed. In most police forces data breaches are required to be reported to the supervisor of the person identifying the data breach, the data protection officer and/or information security officer. The latter usually manages the breach.

If the breach occurs within a third-party, and concerns information provided by the police under information sharing or data processing arrangements, the breach should still be reported to the data protection officer.

Reporting to the Information Commissioner is a responsibility of the data protection officer.

The Information Commissioner has published guidance on **data breach management** and additional detailed guidance for police data protection professionals is contained within the **NPCC Data Protection Manual of Guidance**.

Data subject rights

Introduction

The DPA and UK GDPR secure the rights of data subjects in relation to the processing of their personal data. As these rights can be exercised verbally (as well as in writing) officers, staff and others should ensure they can recognise a rights request and forward it to the unit within their force

in charge of processing them.

The most frequently exercised rights are those of access and erasure of personal data. These and others are described below.

Police forces have a month to respond to rights applications so it is crucial that the details of such applications are forwarded promptly to ensure the request is processed as soon as possible.

The Information Commissioner has published guidance on **information rights** and detailed additional guidance for police data protection professionals is contained within the **NPCC Data Protection Manual of Guidance**. Police forces, staff and others should ensure they are familiar with their force's own policies and procedures relating to rights applications.

There are exemptions and restrictions within the DPA and UK GDPR which police forces can consider prior to a request being processed. For example, personal data would not be released to a data subject under the right of access if doing so would prejudice law enforcement or the rights and freedoms of another person.

The rights are listed below.

General processing rights

The **general processing rights** are:

- information to be provided where personal data is collected from the data subject (**UK GDPR Article 13**)
- information to be provided where personal data has not been obtained from the data subject (**UK GDPR Article 14**)
- right of access by the data subject (**UK GDPR Article 15**)
- right to rectification (**UK GDPR Article 16**)
- right to erasure ('right to be forgotten') (**UK GDPR Article 17**)
- right to restriction of processing (**UK GDPR Article 18**)
- notification obligation regarding rectification or erasure of personal data or restriction of processing (**UK GDPR Article 19**)
- right to data portability (**UK GDPR Article 20**)
- right to object (**UK GDPR Article 21**)

- automated individual decision-making, including profiling (**UK GDPR Article 22**)

Law enforcement rights

The **law enforcement processing rights** are:

- information for data subjects (**DPA s 44**)
- right of access by the data subject (**DPA s 45**)
- right to rectification (**DPA s 46**)
- right to erasure or restriction of processing (**DPA s 47**)
- rights under section 46 or 47: supplementary (**DPA s 48**)
- right not to be subject to automated decision-making (**DPA s 49**)
- automated decision-making authorised by law: safeguards (**DPA s 50**)
- exercise of rights through the Information Commissioner (**DPA section 51**).

Freedom of Information Act 2000

The right of access should not be confused with the right to request information under the Freedom of Information Act 2000.

The former permits an application by a data subject to their personal data.

The latter permits, in most cases, an application by individuals to non-personal data, though in some exceptional circumstances personal data relating, for example, to senior officers and staff, may be disclosed. For further information see **APP on freedom of information**, and Information Commissioner guidance on the Freedom of Information Act 2000.

Privacy by design and by default

Data protection by design and by default

DPA s 57 and **UK GDPR Article 25** require police forces to integrate data protection requirements in every aspect of their processing of personal data. This process is known as data protection by design and default.

This means that from the time of deciding that processing will occur, and at the time it occurs, the police force must devise and implement appropriate technical and organisational measures

necessary to ensure the processing complies with the DPA and UK GDPR, including the rights of data subjects.

Data protection by design is ultimately an approach that ensures police forces consider privacy and data protection issues at the design phase of any system, service, product or process and throughout their lifecycle. Data protection by default requires police forces to ensure that they only process the data that is necessary to achieve the specific purpose of that processing.

Consequently, officers, staff and others considering introducing new systems, services, products or processes involving the processing of personal data must begin considering data protection requirements at the earliest stage of their initiative.

Data protection impact assessments (see the next section) are a means of considering data protection requirements in a structured manner.

The Information Commissioner has published guidance on **data protection by design and default** and detailed additional guidance for police data protection professionals is contained within the **NPCC Data Protection Manual of Guidance** (available to authorised users who are logged on to the **Knowledge Hub** and are members of the **NPCC Data Protection Knowledge Hub Group**).

Data protection impact assessment (DPIA)

DPA s 64 and **UK GDPR Article 35** require police forces to undertake a data protection impact assessment (DPIA) where either law enforcement or general processing is likely to result in a high risk to the rights and freedoms of individuals.

For general processing, DPIA's are mandatory in some circumstances, including where:

- there is systematic, extensive and automated profiling of data subjects
- the processing is on a large scale involving special category data or criminal offence data
- the processing involves systematic monitoring of public spaces on a large scale.

The data protection officer must be involved in the process of creating DPIAs.

DPA s 65 requires police forces to consult with the Information Commissioner where, having conducted a DPIA, the DPIA identifies high risks to data subjects which have not been mitigated.

The Information Commissioner has published guidance on **data protection impact assessments** and detailed additional guidance for police data protection professionals is contained within the **NPCC Data Protection Manual of Guidance**.

Use of processors

For law enforcement processing, whenever a police force uses a processor to process personal data for, or on behalf of the police force, DPA s **59** and **60** require that the processor can only be used if they guarantee to implement the technical and organisational measures necessary to ensure the processing is compliant with the law. A processor must not engage with another processor without authorisation from the police force. There is also a requirement for the processor to be governed by a contract or other legal act, which is binding on the processor with regard to the police force.

For general processing, whenever a police force uses a processor to process personal data for, or on behalf of the police force, **UK GDPR Article 28** requires that a written contract is in place between the two parties. The contract is important so that both parties understand their responsibilities and liabilities. UK GDPR sets out what needs to be included in the contract. If a processor uses another body (namely, a sub-processor) to assist in its processing of personal data for a police force, authority for this must be given by the force. The processor must also have a written contract in place with the sub-processor.

Records of processing activities

For law enforcement processing and general processing, **DPA s 61** and **UK GDPR Article 30** respectively require police forces to create, regularly update and maintain written records of their processing of personal data. These are known as records of processing activities (RoPA) and must include processing purposes, data sharing and retention. The records must be made available to the Information Commissioner on request. Similar obligations apply to processors working on behalf of police forces.

The RoPA must include for each information asset:

- the police force's name and details (and where applicable those of other controllers, their representative and data protection officer)

- the purposes of the processing
- the description of the categories of individuals and categories of personal data
- the categories of recipients of personal data
- details of transfers to third countries including documentation of the transfer mechanism safeguards in place
- retention schedules
- a description of technical and organisational security measures

The RoPA may also serve as police forces' information asset registers.

Logging

For law enforcement processing **DPA s 62** requires any automated processing systems (any IT database) to include logs for at least the following processing actions:

- collection
- alteration
- consultation
- disclosure (including transfers)
- combination
- erasure

The intention behind logging is to monitor and audit processing, and to know which third parties personal data has been shared with, so that these third parties can be informed of changes to the information should the need arise. Logging also enables police forces to monitor systems for inappropriate access and/or disclosure of personal data, to verify the lawfulness of any processing, and to ensure the integrity and security of personal data.

No equivalent obligation applies to general processing.

Information sharing and disclosure of information

The College of Policing has produced **APP for information sharing**. In addition, the Information Commissioner's Office (ICO) has published a **data sharing code of practice**, which is designed to help ensure any sharing of personal information is compliant with the DPA and/or UK GDPR.

Enforcement

The Information Commissioner has produced **guidance on its enforcement powers** and regularly publishes outcomes of its enforcement activity, including monetary penalties.

The DPA and UK GDPR place a responsibility on police forces to **cooperate** with the Information Commissioner. The Information Commissioner in their role as regulator will often approach a police force after receiving complaints regarding compliance with the DPA and UK GDPR.

Consequently, the Information Commissioner has powers to compel a police force to:

- provide information to the Information Commissioner as a consequence of an information notice being served on the police force
- comply with instructions contained within an information order served on the police force by the Information Commissioner
- comply with an assessment notice served on the police force by the Information Commissioner
- comply with an enforcement notice served on the force by the Information Commissioner

The Information Commissioner also has powers of entry and inspection on/of police premises.

It is a criminal offence to destroy or falsify information sought by the Information Commissioner under an information notice or assessment notice.

The Commission has the power to serve penalty notices on police forces where they fail to comply with the DPA and/or UK GDPR. There are two levels of penalty which apply in differing circumstances according to the nature of the non-compliance.

- The higher maximum amount is £17.5 million or four per cent of a police force's annual budget, whichever is the greater amount.
- The standard maximum amount is £8.7 million or two per cent of a police force's annual budget, whichever is the greater amount.

Criminal offences

Introduction

The DPA sets out **criminal offences** that may be committed by individuals. Those offences apply to both general processing and law enforcement processing. The offences are:

- breach of confidentiality by the Information Commissioner (**DPA s 132**)
- destroying or falsifying Information and documents etc. (**DPA s 148**)
- unlawful obtaining etc. of personal data (**DPA s 170**)
- re-identification of de-identified personal data (**DPA s 171**)
- alteration etc. of personal data to prevent disclosure to data subject (**DPA s 173**)
- enforced right of access (**DPA s 184**)

The **NPCC Data Protection Manual of Guidance** has additional detail on all of the offences.

The offences of particular relevance to officers, staff and others working for police forces are examined in greater detail below.

Destroying or falsifying information and documents (DPA s 148)

Where the Information Commissioner has issued an information notice or an assessment notice against a police force it is an offence to destroy or otherwise dispose of, conceal, block or (where relevant) falsify it, with the intention of preventing the Information Commissioner from viewing or being provided with or directed to it.

Unlawful obtaining of personal data (DPA s 170)

It is an offence for a person knowingly or recklessly to obtain or disclose personal data without the consent of the controller (ie, the chief officer), or to procure the disclosure of personal data to another person without the consent of the controller, or after obtaining personal data, to retain it without the consent of the person who was the controller in relation to the personal data when it was obtained.

Alteration of personal data to prevent disclosure to data subject (DPA s 173)

It is an offence to alter personal data to prevent its disclosure following the exercise of a right of access or right to data portability application.

Enforced right of access (DPA s 184)

It is an offence for an employer to require employees or contractors, or for a person to require another person who provides goods, facilities or services, to provide certain records obtained via right of access applications as a condition of their employment or contract. It is also an offence for a provider of goods, facilities or services to the public to request such records from another as a condition for providing a service.

Related offences

The following are related offences that may be considered when dealing with offences under the DPA.

- Unauthorised access to computer material (**Computer Misuse Act 1990 s 1**).
- Unauthorised access with intent to commit or facilitate commission of further offences (**Computer Misuse Act 1990 s 2**).
- Unauthorised acts with intent to impair, or with recklessness as to impairing, the operation of a computer (**Computer Misuse Act 1990 s 3**).
- Misconduct in a public office (common law).
- Conspiracy (**Criminal Law Act 1977 s 1(1)**).
- Conspiracy to pervert the course of justice (**Criminal Law Act 1977 s 1(1)**).
- Breach of confidence (common law).
- Altering records with intent to prevent disclosure (**Freedom of Information Act 2000 s 77**).
- Fraud by false representation (**Fraud Act 2006 s 2**).
- Fraud by abuse of position (**Fraud Act 2006 s 4**).

Primary links to legislation:

- **Data Protection Act 2018**
- **UK GDPR**

Primary links to the Information Commissioner's Law Enforcement Guidance:

- **guide to law enforcement processing**

Primary links to the Information Commissioner's UK GDPR Guidance:

- **guide to the UK GDPR**

Tags

Information management