Data protection – definitions and elaboration

What the terms in this guidance mean and how they link to the ten principles.

First published 31 March 2023 Updated 15 May 2024
14 mins read

Data protection

Data protection is concerned with the lawful and fair use of personal data.

Personal data in the legislation means any facts or figures relating to an identified or identifiable living individual.

Personal data and other data obtained and placed on PNC and LEDS is processed to become policing, law enforcement and safeguarding information. (The data may also be subject to logging and auditing and archived to form part of other organisational information, such that used in performance or disciplinary activity.)

Data and information

The terms ‘data’ and ‘information’ are often used interchangeably (even in the legislation) but they can have specific meanings. For the purposes of the Code, the terms are both used in the following context.

- Data is a term often used for facts or figures that provide the source of information.
- Once the data is processed (organised, structured or presented), it can be considered a component of information, as in ‘police information’.

This echoes the responsibilities in law for the data supplied to the systems, the processing activity that creates a record, and the format of the stored information that can be accessed and eventually removed. In other words, information is data that has been processed in such a way as to be meaningful to the person who receives it.

The data may also be subject to logging and auditing and archived to form part of other organisational information, such that used in performance or disciplinary activity.

UK data protection regime

In relation to data processing, the Code is intended to support compliance with data protection legislation. The ICO regulates data protection in the UK and looks at adherence to the **UK data protection regime**.

Everyone who has access to personal data held on PNC or LEDS is required to use it according to the current legislative framework. The Code highlights the key requirements of the UK data protection regime, which is formed principally by the **Data Protection Act (DPA) 2018** and the UK General Data Protection Regulation (UK GDPR).

The DPA 2018 was amended in January 2021, following Brexit, when the UK GDPR came into effect as a UK law . The UK GDPR sets out the key principles, rights and obligations for most processing of personal data in the UK, except for law enforcement and intelligence agencies, which are covered by **Part 3** and **Part 4** respectively of the DPA 2018.

As of January 2024 the UK Government is seeking to reform the UK's data protection regime. A **Data Protection and Digital Information Bill** is under review in Parliament. The Bill does not comprise an extensive overhaul of the UK's data protection laws, but rather a set of clarifications and adjustments. It is not envisaged that PNC and LEDS user organisations that already comply with the UK's existing data protection laws will be required to take additional steps to comply with and resulting legislation, but further guidance may be issued once any amended law takes effect.

Other legislation such as the Human Rights Act 1998 and the Protection of Freedoms Act 2012 (PoFA) are also relevant and referenced within the responsibilities which underpin the Principles where appropriate.

Controllers and processors

Discussions about data ownership can be complex. The processing of personal data brings about responsibilities to those who are processing it – this may include creating, sharing, exchanging and changing personal data. For data protection purposes, the focus is on how the data is controlled and who controls it, that is, who determines the purposes and means of processing.

Controllers

Under data protection legislation, there must be a controller (or possibly joint controllers) for each processing operation and a single piece of personal data might be subject to multiple different processing operations.

The data 'controller' is defined in the UK GDPR as:

> *...the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.*

For law enforcement processing under Part 3 of the DPA 2018, the controller is the 'competent authority' that, alone or jointly with others, determines the purposes and means of the processing of personal data. A 'competent authority' includes the bodies specified in Part 3 of the DPA 2018 (**see other organisations**) or 'any other person if, and to the extent that, they have statutory functions to exercise public authority or public powers for the law enforcement purposes.

The data controller is the company or person who has the power to determine what happens to the personal data. It is the body with legal status. In the case of a company it would be the company itself, for example, McDonalds the company and not the chief executive of McDonalds. Likewise for a government department like the Treasury, it is the Treasury not the Chancellor of the Exchequer. However, in some organisations such as a police force it is the chief officer who carries that legal personality or responsibility.

The controller who determines the purposes and means of processing personal data will be the legal entity (organisation or person) accountable to the Information Commissioner for the storage, management and other processing of that personal data. Police forces have local systems that feed personal data to PNC and/or LEDS as national systems, where the chief officer is controller of the local system. For the shared systems of PNC and LEDS, there are more complex relationships.

Joint controllers

There are joint controller arrangements for PNC and LEDS as system that contains multiple processing operations depending on how data is processed for particular purposes. For most police forces using PNC and/or LEDS the NPCC has been appointed through a written agreement, made under section 22A of the Police Act 1996. This is a role delegated to the PNC/LEDS Portfolio holder, who is also IAO (see **Information assurance and security** and **Data protection roles**), to

act on behalf the joint controllers.

Organisations that supply data to either PNC or LEDS can either do so on the basis that they become a joint controller with others of that information once on PNC/LEDS, or they may be making a controller-to-controller data share. If they retain a copy of that personal data, they will of course remain responsible as the controller for that copy.

These arrangements, and the data-sharing permissions accorded, are captured in the written access agreements, issued by the joint controllers (through the NPCC). There may also be scenarios where controller-to-controller shares take place, for example, where one organisation extracts data from PNC or LEDS for their own use. In such cases, there should be controller-to-controller agreements in place.

While some non-policing bodies may also be controllers due to the way in which they interact with the systems, others will be processers.

Processors

A processor is therefore a person or organisation that processes personal data of a controller or controllers under their instructions for the purposes and means determined by that controller or controllers. Not all processing operations will involve a processor. Organisations that process personal data on PNC and/or LEDS, for the joint controllers, will be party to a data-processing contract (DPC), or other appropriate written agreement, between themselves and the joint controllers.

Some data sets, such as vehicle insurance details, will simply be provided by external organisations to the joint controllers for reference. The responsibilities outlined in this document may fall between the organisations that are controllers and those that are processors.

The NPCC (acting on behalf of the joint controllers through the information asset owner – see **information asset owner**) will also ensure that current controller and joint-controller agreements (JCAs), and memoranda of understanding (MOUs) are in place for all controllers (as appropriate), and that DPCs are in place for all processors.

ICO guidance has more information on the relationships outlined in data protection legislation: **controllers, joint controllers and processors**. Each force and many of the other organisations

will have a data protection officer who provides expert advice and guidance in assisting controllers and processers with legal compliance.

Further legislation and guidance

Controllers are accountable for ensuring compliance with data protection legislation for personal data that is obtained from PNC and LEDS. The management of that personal data must follow defined policy and procedures. Key pieces of legislation govern what data can be recorded, the standard it must be recorded against, how that data can be used and how it should be managed.

As well as the legislation that forms the data protection regime, there is other legislation which impacts on data management, such as the Criminal Procedure and Investigations Act 1996 and the Protection of Freedoms Act 2012.

Other key pieces of policy or guidance include the **Police Information and Record Management Code 2023**. This sets out seven principles for effective police information management. This Code has replaced the Management of Police Information (MoPI) Code of Practice 2005. It broadens the applicability of the original MoPI Code beyond records that contain police operational information to include police corporate information.

For the purposes of PNC and LEDS, the operational data that is recorded is also covered by the PIRM Code. Controllers are always accountable for compliance with data protection legislation.

Data protection roles

There are several roles referenced in this guidance document. The responsibilities that support adhering to the principles of the Code are applicable to both systems and are assigned in a simplified manner.

This reflects layers of organisational structure, which are:

- chief officer
- manager
- systems user

A systems user is a particularly broad category that could refer to a specific role, such as data inputter, or to a data user, such as a frontline officer entering data during a shift.

Some governance roles are mandated by the data protection legislation. These were discussed further in terms of systems governance later.

Senior information risk owner

This is a mandated role within each police force. The senior information risk owner (SIRO) determines and sets the force appetite for risk, within the accepted national boundaries, and considers information risk from a business – rather than technical – perspective. For PNC and LEDS there is a National SIRO.

Information asset owner

The information asset owner (IAO) has strategic responsibility for ensuring that information assets are secured and managed appropriately. For PNC and LEDS there is a National IAO.

Data protection officer

A data protection officer (DPO) is a specialist in data protection, who provides advice and guidance on compliance with the legislation. Each force will have a DPO, and there are also DPOs at national level for PNC and LEDS.

Data processing

Under the DPA 2018, ‘processing’ is the activity that personal data is subjected to, including creation, storage, sharing and other activities. This includes data processed for law enforcement, safeguarding and wider policing purposes (see **Policing, law enforcement and safeguarding purposes** in this guidance).

Data processing, as defined in the DPA 2018, is:

> *an operation or set of operations which is performed on information, or on sets of information*

Broadly speaking, data processing is the collection, creation, storage and application of data to produce meaningful information. Data processing legislation provides examples of activities that might constitute data processing, such as:

- collection, recording, organisation, structuring or storage
- adaptation or alteration
- retrieval, consultation or use
- disclosure by transmission, dissemination or otherwise making available
- alignment or combination
- restriction, erasure or destruction

Purpose limitation

The UK data protection regime differentiates some of the rules that apply to authorities processing personal data for law enforcement purposes. That comes under part 3 of the Data Protection Act 2018 (DPA 2018), which is separate from the UK GDPR regime. The principles of the Code reflect data protection principles, rights and obligations and it is important to understand the principles for both law enforcement processing through PNC and LEDS and processing for other purposes (for example, safeguarding or human resources reasons).

One essential area to consider is purpose limitation. Personal data collected for a law enforcement purpose should not be processed for another purpose unless it is authorised by law. The **UK GDPR** sets out the regime for data such as that processed on PNC and LEDS, for other purposes, including wider policing purposes, such as community and educational activity and safeguarding responsibilities, where there is no accompanying law enforcement purpose. (The intelligence services, and those processing personal data on their behalf, are not subject to the UK GDPR or the law enforcement provisions of the DPA. Instead, they must comply with Part 4 of the DPA.)

The regime takes a flexible, risk-based approach, which puts the onus on each organisation to consider and justify how and why it uses data. This has implications for individual users too but there are justifications. For example, data about a victim captured as part of an ongoing criminal investigation could be used if there is an immediate need for support and welfare from other emergency or local support services, such as health and social services. System users should consult their data protection officers if they have concerns about what constitutes being ‘authorised by law’.

Key differences between UK GDPR and DPA

The following table summarises some of the key differences between processing under UK GDPR and Part 3 of the **DPA 2018**. More information about managing the individual rights of a data subject is contained in the next section of the guidance.

Question	UK GDPR	Part 3 DPA 2018
What data processing does it apply to?	Most processing of personal data, known as general purposes processing. Processing by law enforcement bodies for general purposes, such as human resources.	Processing of personal data for law enforcement purposes. There are additional rules that apply to 'sensitive processing' of some specified types of particularly sensitive data.
What are the key principles?	• Lawful, fair and transparent. • Purpose limitation. • Data minimisation. • Accuracy. • Storage limitation. • Integrity and confidentiality. • Accountability.	• Lawful and fair. • Purpose limitation. • Data minimisation. • Accuracy. • Storage limitation. • Integrity and confidentiality.

Question	UK GDPR	Part 3 DPA 2018
What are the rights of a data subject?	• The right to be informed. • The right to access. • The right to rectification. • The right to erasure. • The right to restrict processing. • The right to data portability. • The right to object. • The right not to be subject to automated decision-making.	• The right to be informed. • The right to access. • The right to rectification. • The right to erasure. • The right to restrict processing. • The right not to be subject to automated decision-making.

Question	UK GDPR	Part 3 DPA 2018
What exceptions or exemptions may apply?	Exceptions available: • The individual already has the information. • Providing the information would be impossible. • Disproportionate effort. • Would have an impact on the objectives of the processing. • Required by law to obtain or disclose the data. • Subject of a professional secrecy obligation. Exemptions – there are several different exemptions detailed in Schedules 2 to 4 of the DPA 2018. They depend on the purposes for processing personal data.	As for UK GDPR, plus: • Avoid obstructing an official or legal inquiry. • Avoid prejudicing prevention, detection, investigation or prosecution of criminal offences. • Protect public security. • Protect national security. • Protect the rights and freedoms of others.
What organisations can process data?	Applies to any organisation that handles personal data.	Only applies to competent authorities (those specified in Schedule 7 of the DPA 2018, or those that have a statutory function or public powers) processing for criminal law enforcement purposes.

Impact assessment

One of the requirements under the UK data protection regime is that the organisation must produce a Data Protection Impact Assessment (DPIA) where data processing is likely to result in a ‘high risk’ to the rights and freedoms of individuals. This is defined in the UK GDPR and outlined **ICO guide to data protection** and producing a DPIA is considered good practice for any major project which requires the processing of personal data.

On an organisational level, DPIAs play a key role in ensuring that any innovative processing that draws upon data from either PNC or LEDS is both necessary and proportionate.

There is an overarching DPIA for LEDS (produced in 2020 with a revision expected in 2024) and there will be separate DPIAs for each of the LEDS products. As it has been recognised that there is no existing DPIA for PNC, that is also in development as of April 2024.

Connecting organisations such as police forces will also produce their own DPIAs, reflecting their local systems as well as their access to PNC and LEDS.

These documents are useful for organisations as they:

- describe the nature, scope, context and purposes of the processing of data within PNC and LEDS
- assess necessity, proportionality and compliance measures relevant to both systems
- identify and assess risks to individuals; and identify any additional measures to mitigate those risks

Equality impact assessments

Whilst not a requirement derived from the data protection regime, equality impact assessments (EIA) also ensure that further processing does not discriminate against those with a protected characteristic. One of the commitments of the **College of Policing Race Action Plan** is the use of the new national approach to improve and promote consistency in the recording, analysis, monitoring and publication of data on police powers and the effective use of that data at force level to tackle inequalities. Recording standards currently differ between forces.

There will be an EIA for LEDS published in 2024.

Child Rights Impact Assessment

In 2021 of the United Nations Committee on the Rights of the Child General Comment No. 25 called for consideration of children's rights in relation to the digital environment. The Digital Futures Commission advocated the feasibility and benefits of child rights impact assessment (CRIA) as one means of embedding children's best interests in a digital world.

Child rights impact assessment (CRIA) is a tool for looking at decisions, practice, policy or legislation and identifying and measuring their effect on children and young people. A CRIA is considered good practice in examining impacts to be predicted, monitored and, if necessary, avoided or mitigated.

There will be a CRIA for LEDS published in 2024.

Tags

Information management