

Processing

This term covers almost any conceivable use of data, from the moment the data is obtained, to the method of recording, disclosing and destroying the data. Due to the fact that the data protection legislation covers manually recorded data, this means that nearly all uses of personal information are subject to the legislation.

It covers:

- Viewing
- Using
- Altering
- Arranging
- Browsing

Please note:

Browsing of information other than for an official policing purpose is an offence. This means that police staff are authorised to use computer systems and to view data, solely in order to discharge their official duties. The use of computer systems for the sake of 'interest' is deemed unlawful. For example, a police officer coming on duty who views incidents / occurrences on Niche or ControlWorks of police attendance in relation to his / her duties does not commit an offence, but someone who views incidents / occurrences just to see what has happened out of personal interest does.

Data

This term covers not only information processed, or which is intended to be processed, by means of computers or other automatic devices, but also manual/ physical records.

This includes any structured set of information which is organised either by reference to individuals or by criteria relating to individuals so that specific details about a particular person may easily be selected from that system. For the police and other public bodies, this also includes manual unstructured information, whether centralised in one location or dispersed across BCUs.

Personal Data

This relates to data from which it is possible to identify a living individual, either directly from that information or from additional information which is in (or likely to come into) the possession of the Controller.

Therefore, personal data includes data such as:

- Audio/Sounds;
- Images (including video);
- Personal information held in manual files.

Data Protection Impact Assessments (DPIAs)

When considering using a new system to process personal data; where new technology is used; or where you are processing data in a new way; it is now a mandatory requirement to conduct a DPIA. This allows any data protection concerns to be identified and the risks to be managed effectively before employing the new processing methods. This also allows the force's Data Protection Officer and, where necessary, the Information Commissioner's

Office (ICO) to have an oversight of any new processing within the Force to ensure compliance with legislation.

Computer Security

In view of the force's heavy reliance on data processing systems, the confidentiality, security and accurate processing of data are of considerable importance. To help maintain equipment, systems and data in a sensibly controlled and secure environment, a number of requirements must be observed.

Police officers and support staff are reminded that employees shall not disclose or use to their private advantage any information which they may acquire in the course of their duties and which is not available generally to the public.

A list of basic guide-lines to conform to in relation to security is listed below:

- Active terminals must not be left unattended;
- Passwords must not be shared;
- Passwords should be changed regularly;
- Unauthorised use of user identifiers is expressly forbidden.

For full details on compliance issues in relation to security matters, please refer to the Force Information Security Policy, or contact the Force Information Security Officers on extension 70926/70927 or via email:

INFOSEC@south-wales.pnn.police.uk

This leaflet is to alert you to your personal responsibilities under the Data Protection Act 2018 and the GDPR and also your personal responsibilities for computer/information security.

Who to contact for advice:

The Data Protection Officer and the Data Protection team are situated at Police Headquarters, Bridgend. They deal with ALL data protection enquiries, ALL Subject Rights Requests (including Subject Access Requests), ALL personal data breaches and notification changes along with the notification of ALL new systems. The office is also responsible for keeping abreast of changes relating to data protection matters and advises the force on actions required to be taken in relation to comply with the Act.

If you have any queries, or are not sure what advice to give, then contact the Data Protection Officer or a member of the Data Protection Team:

Ext: 20621 / 20622

Email: DataProtection@south-wales.pnn.police.uk

Post: Data Protection,
Data Management and Disclosure Unit,
1st Floor, South Wales Police Headquarters,
Cowbridge Road,
Bridgend,
CF31 3SU

SOUTH WALES POLICE

An Introduction to the Data Protection Act 2018 and General Data Protection Regulation (GDPR)

OFFICIAL

What Is Data Protection?

Data Protection legislation has grown out of public concern about personal privacy in the face of rapidly developing computer technology. It provides rights for individuals and demands good computer practice when handling information about people. By ‘protecting’ data we mean ensuring that personal data about an individual is processed in accordance with legal requirements in order to protect the rights of the individual.

What does this cover?

The legislation deals with information about living individuals which is either stored on computer or is kept in a structured manual file. It works in two ways:

- Giving individuals certain rights – access to their personal data; and
- Requiring those who record and use personal information on computer or in a relevant filing system (manual records) to be open about that use and to follow sound and proper practices.

General Processing

Part 2 of the Data Protection Act 2018, which applies the EU GDPR legislation within the UK, relates to the processing of personal data **excluding** personal data processed for the purpose of law enforcement or national security.

Law Enforcement Processing

Part 3 of the Data Protection Act 2018 relates to the processing of personal data for the purpose of law enforcement, i.e. the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, which might include the safeguarding against and the prevention of threats to public security

Data Protection Principles

Personal data must be:

- 1 processed lawfully, fairly and in a transparent manner;
- 2 processed for specified, explicit and legitimate purposes and not to be processed in a manner incompatible with those purposes;
- 3 adequate, relevant and limited to what is necessary for the purposes for which they are processed;
- 4 accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data are not inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
- 5 kept in a form that identifies individuals for no longer than is necessary;
- 6 with appropriate security safeguards in place.

Individuals’ Subject Rights

The legislation gives individuals (Data Subjects) rights which can be enforced by the courts or by the Information Commissioner. The individual rights include:

The right to be informed

Individuals have the right to be informed about the collection and use of their personal data. This is often referred to as Privacy Notices or Fair Processing

Notices. The Data Subject should be informed of the purposes we are processing their personal data, our retention periods for that personal data, and who it will be shared with.

The right of access – Subject Access Requests (SARs)

The right of access, commonly referred to as subject access, gives individuals the right to obtain a copy of their personal data as well as other supplementary information. It helps individuals to understand how and why you are using their data, and check you are doing it lawfully.

An individual is generally only entitled to their own personal data, and not to information relating to other people (unless they are the focus of that information or they are acting on behalf of someone, or where it is information which they would clearly already be aware of).

Individuals may request copies of any personal data held about them, e.g. occurrences, body worn video footage, emails, officers pocket note books, etc. It is important to note that this includes any opinions that staff or officers have recorded about the individual, therefore any opinions should be clearly discernible from facts.

There is generally no fee for these requests. If someone has requested a copy of their personal data, you should complete the Subject Access Request (SAR) Quicklink on Bob, or on officers’ mobile devices. This will send the request to the Data Protection team in the Data Management and Disclosure Unit, who will respond to the request.

The right to erasure (AKA The right to be forgotten)

Individuals have the right to have personal data erased. This is also known as the ‘right to be forgotten’. The right is not absolute and only applies in certain circumstances.

Any such requests should be referred to the Data Protection team.

The right to rectification

Individuals have the right to have inaccurate personal data rectified. An individual may also be able to have incomplete personal data completed – although this will depend on the purposes for the processing. This may involve providing a supplementary statement to the incomplete data.

Any such requests should be referred to the Data Protection team.

The right to complain to the Information Commissioner’s Office (ICO)

Should an individual not be satisfied by the way South Wales Police has processed their data, or feels their rights have been infringed, they may contact the supervisory body for the UK – the Information Commissioner’s Office (ICO). Contact details can be found at: www.ico.org

The Data Subject may exercise their rights in writing or verbally. For example, this could be in an email, a paragraph in a letter, a message on social media, or approaching an on duty officer or member of staff in person. In general, the force has 1 month to comply with the request, but this period may be extended in some circumstances.

Personal Data Breach Reporting

It is now mandatory to report significant breaches to the ICO within 72 hours of them being identified by the organisation. Don’t delay in reporting as this could have an impact on meeting the statutory deadline which would result in a further breach in compliance with the DP legislation. Reports can be submitted via the Breach Reporting Quicklink on Bob, or via the tool on officers’ mobile devices.

Must record all potential personal data breaches – no matter the severity, e.g. an email containing someone’s personal data sent to the wrong email recipient internally may not seem like a problem, but this should be reported. If a significant number of similar breaches were to occur in a short space of time it could highlight a systemic failing.

Offences

Anyone who knowingly or recklessly uses, obtains, discloses or transfers personal data without the authorisation of the Controller is committing a criminal offence. The Chief Constable as Controller can be prosecuted and also the individual concerned can be held personally liable. The maximum penalty for an offence under the Data Protection Act 2018 and the GDPR is currently set at 20 million Euros (approx. £17.5 million) or 4% of annual global turnover, whichever is greatest.

The Information Commissioners Office has powers of inspection, in order to assess whether organisations are complying with the Data Protection principles.

The Data Protection principles have been used as the basis for the development of the guidance on the MoPI (Management of Police Information). The guidance was written as a direct result of the Bichard Inquiry which found flaws in the way the Police Service gathered, managed, used and shared information.

Effective policing depends on efficient information management and this guidance sets out a framework for the management of police information. As the vast majority of information held for a policing purpose is personal information, then compliance with the Data Protection legislation is essential for compliance with MoPI.

Key offences under the Data Protection Act 2018 are:

- Unlawfully obtaining personal data;
- Unlawfully retaining information without the authorisation of the Controller;
- Unlawfully selling personal data;
- Unlawfully offering personal data for sale;
- Re-identification of depersonalised data without the authorisation of the Controller;
- Unlawfully obtaining personal data by requiring someone to exercise their Right of Access in connection with employment or the provision of services (Enforced Subject Access).