Explanatory Framework for Adequacy Discussions

Section F: Law Enforcement

Overview

This section provides an overview of the UK's law enforcement data protection regime. It outlines principles, data subject rights, and obligations in the law enforcement context. It will cover the DPA 2018 and domestic application of EU law for data sharing, and detail relevant aspects of common law and legislation on police powers.

Introduction

This section provides an overview of the UK's law enforcement data protection regime. It is structured as follows:

- Part I sets out the wider context for law enforcement data processing, including the historical development of the policing model, and its legislative bases.
- Part II summarises key elements of the DPA 2018 for law enforcement processing, with a focus on principles and the rights of data subjects.
- Part III summarises key accountability and compliance obligations. These include data protection by design and default; security requirements; data protection officers; and data protection impact assessments.
- Part IV summarises provisions on international transfers in the law enforcement context.
- Part V sets out key oversight and enforcement mechanisms, including the ICO. More detail on the ICO and alternative redress routes is in Section G of this pack.

PART I: WIDER CONTEXT FOR LAW ENFORCEMENT DATA PROCESSING

Overview

In the UK, the law of the land comprises UK legislation, common law, Royal Prerogative, retained EU law, and the various international conventions that the UK has signed up to, such as the ECHR.

There are a number of factors that ensure high data protection compliance. Firstly, for decades the UK's law enforcement community has operated under a statutory requirement to treat all personal data in line with the data protection principles. This has been irrespective of whether the processing was in scope of European law.

Secondly, the law enforcement community have a number of checks and balances built into their processes. Staff are security cleared. For more sensitive processing such as searches of criminal records, these are recorded and can be audited.

Thirdly, law enforcement operates with internal governance structures, such as the National Police Chiefs' Council's Information Management & Operational Requirements Co-ordinating Committee (IMORCC), which oversees, amongst other things, police forces' data protection, records management, and information sharing. IMORCC promotes compliance, consistency, and a corporate approach across the service. It also assists chief officers of the different forces in interpreting data protection in the police environment. In addition, all law enforcement organisations must now have a Data Protection Officer who has a statutory obligation to assure data protection compliance and protection of the rights of data subjects.

Fourthly, the UK law enforcement community works closely with the UK Data Protection Authority: the ICO. Under the new data protection legislation, there is a greater requirement to do this. However, UK law enforcement have operated using this constructive working relationship for many years.

Lastly, in the event data breaches do occur, the ICO has the same powers to investigate as they do under the UK GDPR, with the same powers and levels of sanction. Moreover, a structured, independent appeals process is available.

At the core of the UK Law Enforcement structure are police officers and staff who serve in the territorial police forces. This comprises all of the 43 'Home Office' police forces across England and Wales, Police Service of Scotland, and the Police Service of Northern Ireland (PSNI). Their primary duty is the protection of life and property, preservation of the peace, and prevention and detection of criminal offences.

The work of these forces is complemented by national agencies, such as the National Crime Agency; and three specialist units – the British Transport Police, the Civil Nuclear Constabulary, and the Ministry of Defence Police.[1] Other public bodies that encompass diverse areas of public life, such as offender management and prosecuting authorities, along with more niche regulators such as the Food Standards Agency (FSA)[2], are also covered within the scope of law enforcement.

Together these organisations make up the "competent authorities" (as defined by the DPA 2018, see below) and enforce the law through their regulatory, investigatory, and prosecutorial powers. For example, the FSA and Food Standards Scotland work with local authorities to enforce food safety regulations. Their staff work in meat plants to check standards are being met. Similarly, Her Majesty's Revenue and Customs employ around 2000 Criminal Investigators who are responsible for investigating serious organised fiscal crime; and prosecutors across the UK make decisions on whether or not to charge the most serious criminal offences such as murder.

Given the wide-ranging nature of the organisations and the functions that would come within the umbrella of law enforcement in the UK, the section focuses primarily, though not exclusively, on the UK policing since they are the primary 'users' of the law enforcement data processing regime.

The Principles and Historical Development of the Policing Model

To understand how the police forces in the UK operate today, it is worth reflecting on their historical development. The *'Peelian Principles'*, which were probably developed by the first Commissioners of the Metropolitan Police Charles Rowan and Richard Mayne, led to the development of the British model of "policing by consent". The Principles included the following:

- Police must secure the willing cooperation of the public in voluntary observance of the law to be able to secure and maintain the respect of the public;
- Police, at all times, should maintain a relationship with the public that gives reality to the historic tradition that the police are the public and the public are the police; the police being only members of the public who are paid to give full-time attention to duties which are incumbent on every citizen in the interests of community welfare and existence.[3]

[1] The special forces are respectively sponsored by the Department for Transport, the Department for Business, Energy and Industrial Strategy and the Ministry of Defence. The BTP have jurisdiction across the railways of Great Britain, whilst the CND and MOD police have powers that span the UK.

[2] The Food Standards Agency has responsibility for England, and Northern Ireland. The Scottish equivalent is Food Standards Scotland.

[3] This shapes the police force inspection framework in England and Wales taken by Her Majesty's Inspectorate of the Constabulary and Fire and Rescue Services (HMICFRS). This framework is appropriately called 'PEEL' – standing for Police Efficiency, Effectiveness and Legitimacy and is available at: https://www.justiceinspectorates.gov.uk/hmicfrs/police-forces/integrated-peel-assessments/

The model of "policing by consent" operates on the basis that the power of the police comes from the common consent of the public, as opposed to the power of the state. Such consent is not provided by particular individuals but is based on public approval of the existence, actions and behaviour of law enforcement authorities, and on their ability to secure and maintain public respect and trust.[4]

A vital component of public consent is the protection of civil liberties, which the police must obtain while balancing the need to ensure public security. UK authorities are constantly vigilant to maintain public security whilst upholding the principle of respect for privacy. Part 3 of the DPA 2018 strengthens the rights and protections of data subjects, while ensuring that the law enforcement agencies can continue to process personal data to prevent and investigate crime, bring offenders to justice, and keep communities safe.

Legislative Bases of the Policing Model

There are two types of law in the UK which together make up the UK legal framework:

- **Legislation**: The UK legislature consists of the UK Parliament (in Westminster, London), the Scottish Parliament, the National Assembly for Wales and the Northern Ireland Assembly. They are responsible for passing primary legislation (Acts of Parliament) and delegating and approving secondary legislation (typically more detailed rules).
- **Common Law:** Sometimes also known as customary law, or judge made law, common law is created by the judiciary through the decisions in the cases they hear. The defining feature of the common law is that it is based on precedent and is underpinned by the principle of *stare decisis* (standing by decisions of higher courts). The conclusions the judges reach are normally recorded as court judgments, and collectively these form part of the common law. In practice, this means a judge presiding over a case will check to see if a similar situation has come before a court previously. If a precedent was set by a court of equal or higher standing, the judge will in most instances follow the decision.

UK legislation provides a comprehensive framework for the powers, scope and limits of police force activity. It is important to note that the UK has three separate legal systems: one each for Scotland; England and Wales[5]; and Northern Ireland. This reflects its historical origins.

Devolution has provided for the transfer of some powers from the Westminster Parliament to the Welsh Assembly in Cardiff, the Northern Ireland Assembly in Belfast and the Scottish Parliament in Edinburgh. UK Parliament will not normally legislate on matters that are

[4] This is one reason why UK police forces are not routinely armed.
[5] England and Wales share the same legal system.

within the legislative competence (i.e. jurisdiction) of the Scottish Parliament, the National Assembly for Wales or the Northern Ireland Assembly without the relevant devolved legislature's consent. Whilst data protection is a reserved matter and the UK DPA applies across the UK, policing is an example where policy is devolved. As such, there is often similar, but different, legislation applicable to policing in England and Wales; Scotland; and Northern Ireland.

Acts of Parliament

Over the past 25 years, the UK Parliament has passed a number of key pieces of legislation which relate to the powers of law enforcement agencies in the UK. Most of this legislation has been subject to amendment, since it was originally passed to keep the law up to date with modern developments. Some of the key pieces are below to give an indication of other legislation – aside from the DPA 2018 – that provide for information management requirements.

Perhaps most important is the Police and Criminal Evidence Act 1984 (PACE)[6] (England and Wales) which sets out the key powers of police officers in England and Wales including:

- stop and search;
- arrest;
- detention;
- investigation;
- identification; and
- interviewing of detainees.

Similar legislation exists in Scotland by virtue of the Criminal Justice (Scotland) Act 2016[7] and in Northern Ireland by virtue of the Police and Criminal Evidence (Northern Ireland) Order 1989[8] (SI 1989/1341).

PACE and the devolved equivalents provide safeguards[9] and limitations to these powers. Since their enactment, they have been subject to further amendments, for example, to ensure compliance with the Human Rights Act 1998. Part VI of PACE requires the Home Secretary to issue Codes of Practice.[10] The 'PACE Codes' (A-H) provide for the exercise of these powers in an operational context in England and Wales, in a way that protects the rights of the public, ensures fairness to individuals, and is compatible with the British model of policing by consent.

[6] https://www.legislation.gov.uk/ukpga/1984/60/contents
[7] http://www.legislation.gov.uk/asp/2016/1/contents/enacted
[8] http://www.legislation.gov.uk/nisi/1989/1341/contents
[9] See also Sections 16, 18 and 32 of PACE.
[10] https://www.gov.uk/guidance/police-and-criminal-evidence-act-1984-pace-codes-of-practice#pace-codes-of-practice

Section F: Law Enforcement

In Scotland, the Criminal Justice (Scotland) Act 2003[11], along with common law, provide a robust retention schedule for the taking, retaining and deleting of samples and profiles of both victims and suspects of crime.

The Protection of Freedoms Act 2012 (PoFA)[12] was brought in in response to the 2008 judgment of the European Court of Human Rights in the case of *S and Marper v UK*[13]. In this case, the court ruled that the blanket retention of DNA profiles taken from innocent people posed a disproportionate interference with the right to respect for private life, in violation of Article 8 of the European Convention on Human Rights. The judge commented favourably on the Criminal Procedure (Scotland) Act 1995 and PoFA was enacted across England and Wales. PoFA, like the Criminal Procedure (Scotland) Act, aims to strike a balance between protecting the freedoms of those who are innocent of any offence whilst ensuring that the police continue to have the capability to protect the public and bring criminals to justice.

Some of the principle UK Law Enforcement Agencies are also subject to the Investigatory Powers Act 2016[14] and Regulation of Investigatory Powers Act 2000[15]. These regimes are covered in detail in Section H of the pack and will not be covered here.

Whilst not specific to law enforcement – UK Law Enforcement are required to act consistently with the European Convention on Human Rights (ECHR). The Human Rights Act 1998[16] (HRA) gives effect to certain rights contained within the ECHR in domestic law (the 'Convention rights', as defined in Section 1 HRA). The HRA provides that all public bodies must act compatibly with those ECHR rights, and individuals can rely on those Convention rights when bringing claims in domestic courts. As a result, law enforcement agencies must ensure compliance with the ECHR. For example, when processing data, they must comply with the right to respect for private and family life, ensuring any interference with this right is permissible with the convention right.

Similarly, the Equality Act 2010[17] legally protects people from discrimination in the workplace and in wider society. The Act introduced the Public Sector Equality Duty which means that public bodies (not specifically law enforcement) must consider all individuals when carrying out their day-to-day work – in shaping policy, in delivering services and in relation to their own employees.

---

[11] http://www.legislation.gov.uk/asp/2003/7/contents
[12] http://www.legislation.gov.uk/ukpga/2012/9/contents/enacted
[13] http://www.bailii.org/eu/cases/ECHR/2008/1581.html
[14] http://www.legislation.gov.uk/ukpga/2016/25/contents/enacted
[15] http://www.legislation.gov.uk/ukpga/2000/23/contents and the Regulation of Investigatory Powers (Scotland) Act 2000 (http://www.legislation.gov.uk/asp/2000/11/contents)
[16] http://www.legislation.gov.uk/ukpga/1998/42/contents
[17] http://www.legislation.gov.uk/ukpga/2010/15/contents. In Northern Ireland, the equivalent legislation is the Northern Ireland Act 1998; http://www.legislation.gov.uk/ukpga/1998/47/section/75

It also requires that public bodies have due regard to the need to eliminate discrimination, advance equality of opportunity and foster good relations between different people when carrying out their activities. In practice, equality, diversity and human rights are critical for UK Law Enforcement, in order to secure the trust and confidence of the communities they serve.

Police Powers Under Common Law

The core duty of the police service is to protect the public and detect and prevent crime. This duty is established in **common law** (precedents set by decisions of the courts), and the police have common law powers to execute these duties[18]. They also have specific powers set out in legislation which help them to carry out their duties.

In the UK, every sworn police officer will hold the 'Office of Constable'. This means the police officer will have the legal powers of arrest and control of the public. The Office of Constable means that he or she will have access to the powers available to a constable, regardless of rank. All police officers have a duty to keep the peace and preserve and prevent all offences against people and property.

As the role of a police constable is a creature of the common law, constables will owe the public a common law duty to prevent and detect crime. That duty reflects a corresponding common law power to take steps in order to prevent and detect crime[19]. Thus, in *R (Catt) v Association of Chief Police Officers* [2015] AC 1065 [7] Lord Sumption JSC observed "[a]t common law the police have the power to obtain and store information for policing purposes, i.e. broadly speaking for the maintenance of public order and the prevention and detection of crime". The breadth of the police's common law powers and obligations was further recognised by the court in *Rice v Connolly:*

> "*it is part of the obligations and duties of a police constable to take all steps which appear to him necessary for keeping the peace, for preventing crime or for protecting property from criminal injury. There is no exhaustive definition of the powers and obligations of the police, but they are at least those, and they would further include the duty to detect crime and to bring an offender to justice."*

In *R (Catt) v Association of Chief Police Officers* [2015] AC 1065 the Supreme Court also considered the lawfulness of collecting and retaining personal information of an individual who had demonstrated against the operation of an arms manufacturer on a "domestic extremism" database. In relation to the police's power to obtain and hold that information Lord Sumption held that:

---

[18] See House of Commons Library Briefing, Introduction to Police Powers, 11 September 2019 < https://researchbriefings.files.parliament.uk/documents/CBP-8637/CBP-8637.pdf

[19] see Rice v Connolly [1966] 2 QB 414 *per* Lord Parker CJ at 419B

> "*At common law the police have the power to obtain and store information for policing purposes, i.e. broadly speaking for the maintenance of public order and the prevention and detection of crime. These powers do not authorise intrusive methods of obtaining information, such as entry on private property or acts (other than arrest under common law powers) which would constitute an assault. But they were amply sufficient to authorise the obtaining and storage of the kind of public information in question on these appeals."*

This is not an unqualified power. It only permits the police to process data if it is for a policing purpose. Furthermore, it also does not authorise processing that would be in contravention of the data protection legislation. This means that where police constables process data, they do so within the constraints of the law; for example, where PACE provides specific requirements, the police must abide by them. Part V ("Oversight") of this section has further detail on PACE.

Detailed guidance is available to officers when processing data using common law powers[20]. This is made publicly available on the College of Policing website[21]. Moreover, Section 39 of the Police Act 1996 gives the Home Secretary the power to create Codes of Practice.

In 2005, the then Home Secretary issued a Code of Practice on the Management of Police Information (MoPI). The Guidance recognised the need for a common approach across the police service and allows police forces to share information in a way that was not previously possible. Speaking at the time, the then Home Secretary said:

> *"Information is the lifeblood of policing, and effective and consistent processes for managing information flows are therefore at the heart of effective policing.*
>
> *The Guidance on Management of Police Information sets out, for the first time, detailed processes for the collection, recording, evaluation and actioning, sharing and review, retention and ultimately deletion of police information, supporting the business of policing and compliant with the law."*

Chief Constables (in their capacity as controllers) are the primary audience for the guidance, but it is equally applicable to records managers and others directly involved in the management of police information and has been designed to be accessible to all police officers and police staff. The guidance refers to all information, regardless of the medium in which it is stored.

---

[20] The Authorised Professional Practice (APP) on the Management of Police Information
[21] https://www.app.college.police.uk/information-management-index/

Section F: Law Enforcement

The MoPI Code ensures that there is broad consistency between forces in the way information is managed. This not only encourages effective use of available information within and between individual police forces and other agencies, but also the fair use of data.

MoPI sets out the principles governing the management of information (including personal data) which the police service may need to manage and use. It Includes guidance on a range of processing activities such as:

- Collection and Recording: accurate assessment and timely analysis of information.
- Evaluation: Police information undergoes evaluation appropriate to the policing purpose for which it was collected and recorded. All police information is evaluated to determine provenance, accuracy, continuing relevance to a policing purpose and what action, if any, should be taken.
- Common process for managing police information: Information comes from various sources and is received in different ways. As a result, it may be necessary to link information collected for one policing purpose to information collected elsewhere for a different purpose.
- Retention, Review, and Disposal: The review of police information is central to risk-based decision making and public protection. Records must be regularly reviewed to ensure that they remain necessary for a policing purpose and are adequate and up to date.

The guidance also recognises that the police service creates a plethora of records during the delivery of policing, and it is these records that the guidance is primarily trying to manage by setting the minimum standards for processing activities. They are, however, not mandatory and there are occasions when individual police forces may deviate from them for a variety of technical, operational and organisational reasons. Even in these scenarios, forces **are still required to comply with the requirements of Part 3 of the DPA 2018**.

Furthermore, Part 3 of the DPA 2018 is a comprehensive regime to govern data processed for law enforcement purposes. This means that, even when the police use their common law powers to process data, they do so within the limits imposed by the DPA 2018.

A decision to perform any sort of data processing - particularly using common law powers – must comply with the requirements of MoPI, and balance the rights of the individual against those of the public in general or any specific member or members of the public. This includes contemplating the impact of processing on the private life of the individual involved, whilst taking into account any adverse effect processing might have on the avoidance or detection of crime.

Section F: Law Enforcement

Although MoPI does not apply to Scotland, under the Code of Practice, the Scottish Police Services Authority are required to establish an Information Management Strategy[22], complying with guidance and standards issued under the MoPI Code. The resultant Strategy is very similar to the MoPI. The PSNI are not required by law to follow MoPI; however, they endeavour to voluntarily adopt the principles within their law enforcement processing.

By way of contrast, the National Crime Agency cannot rely on common law powers. It is a creature of statute and therefore must operate within the confines of the legislation that established it – the Crime and Courts Act 2013[23]. Under Part 1 of the Act, the NCA has a function in respect of tackling serious and organised crime, and a wider criminal intelligence function in respect of all types of crime.[24]

Its activities in relation to serious and organised crime include tackling the importation/supply of drugs and firearms; human trafficking; sexual abuse; high-end money laundering; organised immigration crime; and tackling cybercrime. By virtue of this legislation, NCA officers may be designated with the powers and privileges of a constable and the law enforcement powers of an officer of Revenue and Customs, an immigration officer and a general customs official. This enables them to effectively fulfil their broad functions and deploy techniques that are not available to the police.

The suite of powers which are exercisable by NCA officers enable them to do a range of things crucial to any criminal investigator including gaining entry to property, searching (people and premises), seizing goods, detaining and arresting suspects and executing warrants. This will result in processing the personal data of victims, witnesses and suspects, as the police do.

In addition, the NCA has a power to provide assistance to foreign governments, and overseas bodies carrying out functions of a public nature. For the purposes of the discharge of any function of the NCA, it may enter into arrangements for co-operating with other persons (in the United Kingdom or elsewhere). These functions and the information gateway in Section 7 of the Act permit the NCA officers to exchange data with their international counterparts subject to compliance with the DPA 2018.

PART II: THE CURRENT REGIME - DPA 2018

This section contains information on:

[22] https://www.nrscotland.gov.uk/files/record-keeping/public-records-act/element3-SPSAStrategy.pdf
[23] In Northern Ireland, the equivalent legislation is the Northern Ireland Act 1998; http://www.legislation.gov.uk/ukpga/1998/47/section/75
[24] The NCA requires the permission of the Lord Advocate to act in Scotland.

- the development of the law enforcement data processing framework and background to the 2018 reforms
- key elements of the UK's law enforcement data protection framework. This includes scope; definitions; principles; rights; and restrictions. Other obligations and provisions on international transfers are covered in Parts III and IV of this section.

Development of the Law Enforcement Data Processing framework

The UK has placed great significance on ensuring the correct balance between the rights of the data subject and the operational effectiveness of our law enforcement community. It has historically been at the forefront of data protection. As far back as the 1970s, it began taking steps to address the gap in the governance of personal information.

- The Younger Committee on Privacy[25] established ten principles for the handling of personal data that were to influence data protection statutes in Europe.

- In 1984, the UK's first Data Protection Act[26] became law, drawing on the principles contained in the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS No. 108)[27]. Although narrow in focus – it only applied to personal data stored on a computer – it instilled data protection standards across the board, including for law enforcement processing.

- In 1995, the European Union passed the Data Protection Directive (95/46/EC) which brought in a common standard for data protection throughout the European Union. This was transposed into UK law by the Data Protection Act 1998[28]. Although the Directive did not apply to data processing for law enforcement purposes, the then Government extended it to cover all processing of personal data[29] in the UK in order to create a single data protection regime.

  As a result, law enforcement agencies in the UK were required to comply with the provisions of the Act. The DPA 1998 set out the rights of data subjects, alongside a number of exemptions to those rights[30] including for crime and taxation. It established the post of Information Commissioner and provided them with a number of powers of enforcement.

- In 2008, the then Government transposed the Council Framework Decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters (the 'Framework Decision').

---

[25] https://api.parliament.uk/historic-hansard/lords/1973/jun/06/privacy-younger-committees-report
[26] http://www.legislation.gov.uk/ukpga/1984/35/pdfs/ukpga_19840035_en.pdf
[27] https://www.coe.int/en/web/data-protection/convention108-and-protocol
[28] http://www.legislation.gov.uk/ukpga/1998/29/contents
[29] Except for processing by private individuals for domestic purposes
[30] including for crime and taxation

This was through the Criminal Justice and Data Protection (Protocol No.36) Regulations 2014[31], which applied to law enforcement within the scope of EU law and included implementation of the tools and databases to facilitate the mutual exchange of information to assist in criminal apprehension, investigation, prosecutions, or confiscation of the proceeds of crime.

As a result, once the 2014 Regulations came into force, organisations processing data for law enforcement purposes had to comply with the requirements of the DPA 1998 and, when processing personal data for cross-border law enforcement purposes, Part 4 of the 2014 Regulations.

The DPA 1998 continued to govern all aspects of the processing of personal data for domestic law enforcement purposes, as well as the processing of personal data by law enforcement agencies which was not for law enforcement purposes (for example for their own internal record-keeping, administration, personnel records, etc). The 2014 Regulations applied in circumstances outside the reach of the DPA 1998 – for example when co-operating with an overseas Competent Authority – but the provisions were broadly consistent with the DPA 1998.

More recently, the UK has played a key role in shaping the data protection landscape, including its participation in the development of the Law Enforcement Directive (LED). UK Home Office officials actively participated in DAPIX working group discussions to develop the Council position. The UK produced non-papers on specific issues and provided real-life examples to discussions to help ensure that the LED would work effectively and appropriately in the law enforcement environment.

Moreover, the UK was one of the first countries to fully transpose the directive into domestic law. For the UK, applying the new data protection legislation is therefore about more than simply meeting its international obligations. It is a further step in its long-term commitment to protecting personal data and is fundamental to how the UK strikes a balance between respecting the privacy of the individual and effectively utilising the powers of the police to investigate and tackle crime.

The LED has primarily been transposed into UK legislation through Part 3 of the DPA 2018. Part 3 will be considered further in the following section.

Background to 2018 Data Protection Reforms

[31] https://www.legislation.gov.uk/ukdsi/2014/9780111122723

Section F: Law Enforcement

The EU GDPR does not apply to the processing of personal data by "competent authorities[32] " for 'law enforcement purposes'. Instead, alongside the EU GDPR, the European Parliament and Council adopted the Law Enforcement Directive (LED – Directive (EU) 2016/680)[33].

Unlike the EU GDPR, the LED is not directly applicable EU law, and so the UK was required to transpose it into UK domestic legislation. The scope of the LED is provided for in Article 1 and concerns the processing of personal data by competent authorities for the law enforcement purposes.

When the UK transposed the LED, it went further than the Directive required by extending the data protection standards set out in Part 3 to all processing by law enforcement agencies for law enforcement purposes, not just law enforcement processing which falls within the scope of the LED/EU law. This was welcomed by operational users domestically, as it enables them to apply a single set of standards to the majority of their processing and is consistent with the approach the UK took in the DPA 1998.

In Part 3 of the DPA 2018, the UK 'copied out' the LED wherever possible and deviated only to elaborate where such elaboration was necessary to reflect UK-drafting style, clarify the legal effect of a provision, or to give effect to bespoke provisions. Deviation from 'copy-out' was only used where necessary and permitted by the LED or where it was necessary to cover matters outside EU law which are not covered by the LED (such as additional provisions on national security).

Scope and Definitions

Part 3 of the DPA 2018 provides a bespoke regime, tailored to the needs of the police, prosecutors and other law enforcement agencies (referred to as 'competent authorities' by the DPA 2018).

This regime protects the rights of victims, witnesses, and suspects while ensuring law enforcement agencies can continue to effectively tackle crime and other threats to community safety, both at home and abroad. Data protection, supported by legislation such as the Protection of Freedoms Act 2012 and the Police and Criminal Evidence Act 1984, is ingrained in the everyday work of the law enforcement agencies.

The meaning of 'competent authority' is defined in Section 30 of the Act. There are two ways in which a controller may be a competent authority:

[32] These are organisations that have a statutory function for one of the law enforcement purposes. Some of the key competent authorities are listed under Schedule 7 of the DPA 2018.
[33] This repealed the Council Framework Decision (2008/977/JHA) – the previous EU measure addressing cross-border processing of law enforcement data.

- by appearing in Schedule 7 of the DPA 2018; or
- by carrying out a statutory function for a law enforcement purpose.

All UK Government Departments are included in Schedule 7. This means, for example, the Home Office (HO) is a competent authority for the purposes of Part 3. Non-ministerial Government Departments and other organisations, such as the Commissioners for HMRC, are also listed in Schedule 7 where appropriate.

Others, such as local authorities which are not named in Schedule 7 may still be a competent authority if they have a legal power to process personal data for law enforcement purposes.

Example 1:

A local authority processes personal data as part of a trading standards prosecution. Local authorities are not listed in Schedule 7; however, the local authority is carrying out a statutory function and prosecuting is a law enforcement purpose (see below).

Section 222 of the Local Government Act 1972 permits local authorities to take prosecutions in the interests of the inhabitants for their areas. In this instance, the local authority would be operating as a competent authority.

Competent authorities do not include those carrying out private prosecutions; nor does it include the intelligence services as they are governed by Part 4.

'Law enforcement purposes' is defined in Section 31 of the Act as '*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'.*

When determining whether processing is for a law enforcement purpose, it is important to assess whether the '**primary** purpose' of the processing is law enforcement. It must therefore be more than incidental to the processing.

In some circumstances, crimes will be detected, even though there is no intention to carry out law enforcement action. It is important to reflect on the wording within Section 31 which says the processing has to be carried out 'for the purpose of' law enforcement.

If a law enforcement action is not contemplated at the time the processing takes place, it is unlikely the processing will be more than merely incidental to law enforcement and it **cannot** therefore be done under Part 3.

Example 2:

A foreign national seeks to enter the UK as a visitor by confirming he will leave within the required 6 month period. On closer inspection, the Border Force Officer finds evidence to suggest he is planning to stay in the UK. Using deception to enter the UK is a criminal offence; however, the officer administratively removes the individual in line with Home Office policy rather than pursuing a criminal prosecution. The officer's role requires her to process personal data.

Although the officer in the above example has detected a crime, this still remains incidental to her primary purpose: to identify and administratively remove offenders. The processing of personal data therefore takes place under Part 2 (general processing).

There will be instances in which data is collected for a purpose other than law enforcement, and the circumstances change in that the data is later used for a law enforcement purpose. In most of these situations, it will be clear when the primary purpose changes as specialist teams will take over the case; for instance, Fraud Units or Prosecution Teams.

Example 3:

HM Passport Office (HMPO) receives an application for a new passport. During the process, they carry out standard checks to ascertain the genuineness of the application and discover potential fraud. They pass the case to their specialist fraud unit.

The application in the above example is initially processed under the general processing provision (Part 2). Even though as part of their standard checks they are looking for fraudulent applications, this remains part of the general processing, since detecting crime is not the 'primary purpose' of processing a passport application.

Once the potential fraud is detected and it is handed to the specialist fraud unit, the primary purpose of the processing changes. This is made clear by the fact the primary function of a fraud unit is to detect and prevent crime. At this point, Part 3 (law enforcement) applies.

Data collected and processed in accordance with Part 3 may also sometimes be further processed under Part 2 to assist in the formulation of policy or operational planning. The regime which applies will depend on the primary purpose for any further processing.

The section below provides further definitions found in Part 3 of the DPA 2018. The UK has, as noted copied out the LED wherever possible. The list below represents where the UK has diverged or expanded on that provided for in the LED but still remained within the spirit of

the legislation. This is included here to aid understanding of the Act. Sections 3 and 205 of the DPA 2018 include definitions of other expressions used in Part 3:

- Controller: this is either the competent authority which, either alone or jointly, determines the purposes and means of the processing of the personal data, or one which is required to do so by virtue of an enactment. This has the same practical effect as the LED definition.

- Processor: this is identical to the definition under Article 3(9) of the LED, except that it clarifies that an employee of a controller is not a processor and uses the term 'person' in lieu of 'natural or legal person, public authority, agency or other body'. This latter change reflects the fact that the term 'person' is defined as "includ[ing] a body of persons corporate or unincorporate" under Schedule 1 of the Interpretation Act 1978; hence public authorities, agencies and other bodies are already captured.

- Employee: this is an individual who holds a position, whether paid or unpaid, which falls under the direction and control of another person.

- Recipient: this is identical to the definition set out under Article 3(10) of the LED, except that the UK has not transposed the latter part of the definition relating to processing by public authorities. This is because all public authorities will, in any case, be bound by the appropriate Part of the DPA 2018.

- Third country: this is a country or territory other than the UK (following the UK's withdrawal from the European Union).

- Personal data: this is identical to the definition set out under Article 3(1) of the LED, except that, for clarity, the UK has separated out the definition of 'identified or identifiable natural person' and have used the term 'identifiable living individual' in lieu of 'natural person'. This latter change is in order to bring Part 3 of the DPA 2018 in line with recital 27 of the GDPR, which clarifies that it does not apply to deceased persons.

- Processing: this is identical to the definition set out under Article 3(2) of the LED, except that the UK has omitted the words "whether or not by automated means" since the definition applies to all processing of personal data.

- Pseudonymisation: this term is not used in the DPA 2018.

- Profiling/ Genetic data/ Biometric data/ and data concerning health: these definitions are identical to those set out in Articles 3(4), 3(12), 3(13), and 3(14) respectively, of the LED except that the UK has used the term 'individual' in lieu of 'natural person'. This is because 'natural person' is not a term which is used in UK law.

- Supervisory authority: Since there is only one data protection supervisory authority in the UK, the ICO, it is not necessary to define this term. Details on the role and functions of the Information Commissioner are set out under Part 5 and Schedules 12 and 13 of the DPA 2018, and explained in Section G of this pack.

- International organisation: This is identical to the definition set out under Article 3(16) of the LED, except that the UK has omitted the word "public" in relation to international law since all law in relation to international organisations will be public.

Principles

The data protection principles within Part 3 of the DPA 2018 set out the key pillars of data protection and mirror those established in the LED. These principles are not new: they have a long and established history in the UK. They provide the foundation upon which the rights of the data subject are constructed, and require that:

- processing be lawful and fair;
- the purposes for processing are specified, explicit, and legitimate;
- personal data be adequate, relevant, and not excessive;
- personal data be accurate and kept up to date;
- personal data be kept for no longer than is necessary; and
- personal data be processed in a secure manner.

Principle that processing be lawful and fair

The first data protection principle in Section 35 of the DPA 2018 sets out that the "first data protection principle is that the processing of personal data for any of the law enforcement purposes must be lawful and fair".[34]

For law enforcement purposes, the processing of personal data is lawful only if and to the extent that it is based on law and either "the data subject has given consent to the processing for that purpose", or "the processing is necessary for the performance of a task carried out for that purpose by a competent authority".[35]

A DPA 2018 compliant lawful basis could be taking and retaining DNA and fingerprints in accordance with Part 5 of the Police and Criminal Evidence Act (which applies to England and Wales). Law enforcement are also permitted to process data using their common law powers where this is conducive to the law enforcement purposes.

In contrast to general processing, the requirement for transparency is not included in regards to law enforcement processing. This is because it is essential that the law enforcement agencies have the powers that they need to investigate crimes and bring

[34] Section 35(1).
[35] This is set out in section 35(2) of the DPA 2018.

offenders to justice,[36] and it mirrors the approach taken in the LED. For instance, were police forces required to act transparently, this may risk undermining any covert operations they might be engaged in.

Conditions and Safeguards for Sensitive Processing

Part 3 of the DPA 2018 defines the following as sensitive data:

- data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs and trade union membership;
- genetic or biometric data; and
- data concerning health, sexuality or sexual orientation.

The first data protection principle states that the processing of sensitive data is only permitted under one of two conditions:

- where the data subject has given consent to the processing, and the controller has an appropriate policy document in place;[37] or
- where the processing is strictly necessary for a law enforcement purpose, it meets at least one of the conditions set out in Schedule 8 to the DPA 2018 and the controller has an appropriate policy document in place.

Schedule 8 sets outs the conditions[38] under which sensitive data may be processed. Competent authorities are routinely required to process significant volumes of sensitive data, but the list at Schedule 8 is exhaustive and reflects the conditions set out in the LED and those that are critical to the effective operation of the criminal justice system.

The Secretary of State may, by regulations, amend Schedule 8 by adding conditions or by omitting any conditions so added[39]. Any regulations made under this section would be subject to the 'affirmative resolution procedure'. This means that the regulations must be actively debated and approved by both Houses of Parliament providing an additional level of scrutiny to the process.

Section 42 of the DPA 2018 details the safeguards which a Competent Authority must apply when undertaking sensitive processing. They **must** have an appropriate policy document in place which explains how the controller complies with the Data Protection Principles when processing sensitive data, as well as the controller's policies for the retention and erasure of personal data. These provide an indication of how long the data are likely to be retained

[36] This is not to say that law enforcement agencies are not transparent in how they operate aspects of the DPA 2018. For example, Section 44 imposes a general duty on controllers under Part 3 of the Bill to make available specified information to data subjects.
[37] It is a requirement to provide this guidance to the ICO upon request according to Section 42.
[38] Conditions include fraud, safeguarding of children, and protecting individuals' vital interests.
[39] Power provided for in Section 35(6).

for. They must retain the policy document, reviewing and updating it as necessary, and must make it freely available to the ICO upon request.

Section 61(1) requires controllers to keep a record of the categories of processing that they are responsible for and Section 61(3) requires processors to keep a record of the categories of processing activities they carry out on a controller's behalf.

Section 61(1) sets out that these records must include, for example, the name and contact details of the controller, the purposes of processing and a description of the categories of data subject and personal data processed by them. Additionally, where the processing is of sensitive data, the controller, or (where the processing is carried out by a processor acting on their behalf) the processor, must state:

- whether the sensitive processing is carried out on the basis of consent or, alternatively, which of the conditions set out in Schedule 8 are relied on;
- how the processing satisfies the requirement that it be lawful and fair; and
- whether personal data is retained and erased in accordance with the policy document and if not, state why.

Principle that purposes of processing be specified, explicit and legitimate

The second data protection principle in Section 36 of the DPA 2018 is one of purpose limitations, stating that firstly, "the law enforcement purpose for which personal data is collected on any occasion must be specified, explicit and legitimate"[40] and secondly, "personal data so collected must not be processed in a manner that is incompatible with the purpose for which it was collected".[41]

The DPA 2018 provides that personal data collected for a law enforcement purpose may be processed for any other law enforcement purpose, whether by the controller that collected the data or by another controller.[42]

However, it can **only** be processed if the controller is authorised by law to process the data for the other purpose, and the processing is necessary and proportionate to that other purpose.[43] For example, the Crown Prosecution Service could process personal data in relation to the prosecution of an offence, and Her Majesty's Prison Service could process the same data to ensure the execution of a criminal penalty. This provision ensures the smooth flow of personal data through the criminal justice system.

[40] Section 36(1)(a).
[41] Section 36(1)(b).
[42] Section 36(3).
[43] Section 36(3).

Additionally, personal data collected for any of the law enforcement purposes may not be processed for a purpose that is not a law enforcement purpose unless the processing is authorised by law.[44]

Principle that personal data be adequate, relevant and not excessive

The Third Data Protection Principle set out under Section 37 of the DPA 2018 requires that personal data processed for any of the law enforcement purposes must be adequate, relevant, and not excessive in relation to the purpose for which it is processed. This is focussed on data minimisation and ensuring competent authorities store and access personal data for a legitimate reason.

Principle that personal data be accurate and kept up to date

The fourth data protection principle in Section 38 of the DPA 2018 adds that personal data must be accurate and, where necessary, kept up to date. Should it be the case that personal data is inaccurate, every reasonable step must be taken to ensure that it is erased or rectified without delay.[45]

When rectifying or erasing inaccurate data, regard needs to be paid to the law enforcement purpose for which it is processed.[46] This ensures that both the rights of data subjects and the operational needs of law enforcement agencies are recognised.

The above point was carefully considered during the drafting stages of the Data Protection Bill, as there may be specific and limited operational reasons why data cannot be rectified. Most likely this will be if the inaccurate personal data in question needs to be preserved in its original form for evidential purposes.

Additionally, it would not be appropriate to require controllers to correct data in all cases, for example if the inaccuracy is contained within a witness statement, which is necessarily one person's belief as to the facts concerning a particular allegation. This position is also in line with recital 30 of the LED concerning accuracy, as it relates to personal data based on subjective perceptions such as witness statements.

In practice, it is logical for the competent authorities to ensure their personal data is up to date. It is critical for criminal investigations, for example, that intelligence relied on is accurate. High-quality data allows policing to establish where, when, and how often crime is happening. This ensures:

- victims of crime are provided with access to appropriate support services;
- the public are given accurate information about crime in their area;

[44] Section 36(4).
[45] Section 38(1)(b).
[46] Section 38(1)(b).

- the police can plan their work in support of victims and meet the demands of investigations based on accurate information and intelligence.

Section 38(2) provides that personal data processing must distinguish between data based on facts and that based on assessment, such as a witness statement. Section 38(3) requires personal data be categorised so there is a clear distinction between the personal data relating to victims, witnesses, suspects, and those convicted. In this section, the UK has transposed the requirements of Article 6 and clarified the language used to ensure the requirements are widely understood by Competent Authorities. The UK is in the process of developing a set of standardised principles that will support LEAs in taking a standard approach to these requirements.

Principle that personal data be kept for no longer than is necessary

The fifth data protection principle in Section 39 of the DPA 2018 sets out that "personal data processed for any of the law enforcement purposes must be kept for no longer than is necessary for the purpose for which it is processed".[47]

It further requires that "appropriate time limits must be established for the periodic review of the need for the continued storage of personal data for any of the law enforcement purposes".[48] This requirement is in line with Article 5 of the LED which requires Member States either to set appropriate time limits for erasure or, as the UK has done, require them to carry out periodic reviews.

Personal data held by the police, for example, are subject to strict retention and destruction schedules. Much operational data held by the police, with some exceptions, is governed by MoPI which explicitly stipulates that data associated with all but the most serious public protection matters must be subject to periodic review and destroyed where retention cannot be justified by the review.

Operationally, the fifth data protection principle also applies to archiving activities. Law enforcement are permitted to archive personal data if it is conducive to the public interest, for example for historical or scientific purposes or to enable the compilation of statistics. However, Section 41 provides a **robust safeguard** to this provision by expressly prohibiting archiving that is specifically related to an individual or is likely to cause significant distress to the data subject.

Principle that personal data be processed in a secure manner

The sixth data protection principle in Section 40 of the DPA 2018 covers security and confidentiality. It stipulates that "personal data processed for any of the law enforcement

[47] Section 39(1).
[48] Section 39(2).

purposes must be processed in a manner that ensures appropriate security of the personal data, using appropriate technical or organisational measures".

Here, "appropriate security" includes protection against unauthorised or unlawful processing and against accidental loss, destruction or damage. Section 66(1) further specifies that each controller and each processor must implement appropriate technical and organisational measures to ensure a level of security appropriate to the risks arising from the processing of personal data. The ICO's website provides a range of advice on security measures safeguarding cloud computing and privacy impact assessments.[49]

Rights of the Data Subject

Overview and Scope

In addition to setting out the key data protection principles, Part 3 of the DPA 2018 also provides certain rights to data subjects. This:

- enables data subjects to exercise greater control and autonomy over their data; and
- enables data subject to have a greater awareness of the personal data that is held on them, for how long, and for what purposes.

Rights include:

- free access[50] (to obtain a copy of the personal data held along with certain key information about it such as the purposes for processing, the categories of data held and the reasons for holding it);[51]
- rectification of inaccurate data (unless required as evidence);
- right to erasure (unless it is required as evidence) or restriction of processing;
- right not to be subject to automated decision making (an additional right to those specified in the LED); and
- right to exercise their rights through the ICO.

Form of Provision of Information

Section 52 of the DPA 2018 requires that any information to be provided to the data subject is in a concise, intelligible and easily accessible form, using clear and plain language. This is

[49] The range of advice provided by the ICO can be found at: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/resources/

[50] Except that a controller may charge a reasonable fee where a request is manifestly unfounded or excessive as outlined below.

[51] The default maximum period for responding to a subject access request is one month. Meeting this time limit may, in some cases, prove to be challenging, particularly where the controller holds a significant volume of data in relation to the data subject. Section 54 provides the Secretary of State with a power to extend the applicable time-period to up to three months, affording them the flexibility to take into account the operational experience of police forces, the CPS, prisons and others in responding to requests from data subjects under the new regime.

fundamental to transparency and contributes to maintaining public confidence in Competent Authority processing.

In order to prevent unlawful disclosure, where the controller has reasonable doubts about the identity of an individual making a request for information, they may request the provision of additional information in order to confirm their identity, and may delay dealing with the request until their identity is confirmed.

Any information that is required to be provided to the data subject must be provided free of charge. Prior to the DPA 2018, Competent Authorities could routinely charge a small fee for this service, but the removal of this fee is consistent with the ethos of the legislation.

Manifestly Unfounded or Excessive Requests by the Data Subject

There are certain circumstances where Competent Authorities are either unable to comply with the request, or unable to do so without incurring a significant cost. Section 53 of the DPA 2018 specifies that, where a request from a data subject is manifestly unfounded or excessive[52], the controller may charge a reasonable fee[53] for dealing with the request or they may refuse it. A reasonable fee should be based on the administrative costs of complying with the request, according to the ICO[54].

This is not an unqualified exemption. The onus is on the controller to demonstrate that the request is manifestly unfounded or excessive. This acts as a safeguard to ensure that the ability to charge a fee is not misused by controllers as a way to restrict data subject rights.

Right to be informed

The right to be informed is a key requirement of both the LED and Part 3. It is about enabling data subjects to understand what Competent Authorities do with their personal data, in a clear and concise way. This can help foster trust with public and promotes transparency.

Section 44 of the DPA 2018 requires Competent Authorities to make available to the data subject the following information (some of which is for the specific purpose of enabling that subject's rights under Part 3):

- the identity and the contact details of the controller;
- where applicable, the contact details of the data protection officer;
- the purposes for which the controller processes personal data;

[52] An example of a request that may be excessive is one that merely repeats the substance of previous requests.

[53] The Secretary of State may by regulations specify limits on the fees that a controller may charge.

[54] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-of-access/

- the existence of the rights of data subjects to request from the controller access to, and rectification of, their personal data (subject to exemptions - see 'restrictions and safeguards' below); and
- the existence of the right to lodge a complaint with the Commissioner and the contact details of the Commissioner.

They must also, in specific cases, provide the data subject with the following information:

- information about the legal basis for the processing;
- information about the period for which the personal data will be stored or, about the criteria used to determine that period;
- where applicable, information about the categories of recipients of the personal data (including recipients in third countries or international organisations); and
- such further information as is necessary to enable the exercise of the data subject's rights[55] under Part 3.

Right of access by the data subject

The right of access enables data subjects to obtain a copy of their personal data as well as other supplementary information. It helps data subjects to understand how and why Competent Authorities use their personal data and to verify the lawfulness of any processing.

Section 45 of the DPA 2018 entitles a data subject to obtain confirmation from a Competent Authority as to whether or not their personal data is being processed, and, where that is the case, requires them to grant access to the personal data along with pertinent information that enables data subjects to exercise their rights. This includes the purposes of, and legal basis, for the processing; the categories of personal data concerned; and the recipients or categories of recipients to whom the personal data has been disclosed.

The information to which the data subject is entitled must be provided in writing, without undue delay, and within one month.

Right to rectification, erasure and restriction of processing

Under Section 46, a Competent Authority must, if requested by the data subject, rectify any inaccurate personal data belonging to them. Although in practice, Competent Authorities may have already taken steps to ensure that the personal data was accurate when it was first obtained, this right imposes a specific obligation to reconsider the accuracy upon request.

Where personal data is inaccurate because it is incomplete, the controller must, if requested by a data subject, complete it. If they are unable to correct it, they may if it is appropriate to

[55] For example, where the personal data was collected without the knowledge of the data subject.

do so provide a supplementary statement to rectify personal data. For example, competent authorities are allowed to keep accurate records of allegations made, even if the allegations are unfounded.

Where a Competent Authority would be required to rectify personal data under this section but it is required as evidence, such as a witness statement, which is necessarily one person's belief as to the facts concerning a particular allegation, they must – instead of rectifying the personal data – restrict its processing. This approach affords protection to the data subject, while maintaining the integrity of the criminal justice process.

Where a Competent Authority rectifies personal data, it must notify the organisation (if any) from which the inaccurate personal data originated. If the data has been disclosed, the controller must also notify the recipients of the rectification. This helps all controllers domestic and international to comply with the fourth Data Protection Principle.

As well as rectifying data, the DPA 2018 places an obligation on Competent Authorities to erase personal data where the processing of the personal data would infringe one of the Data Protection Principles[56], or where the controller has a legal obligation to erase the data. Though this is not an absolute right, in practice, the controller should conduct periodic reviews of their retention policies to ensure compliance.

Where the controller **would** ordinarily be required by the Data Protection Principles to erase personal data, but it is required, for example as evidence, they must, instead, restrict its processing.

Where a data subject contests the accuracy of personal data, but the claim cannot be verified, the controller must restrict its processing.

In summary, if requested to erase data by the data subject, the controller must look at the requirements under Section 47 of the DPA 2018. They must erase the data or restrict access where there is a legal obligation to do so, or where the processing infringes on the principles in Part 3.

Right not to be subject to automated decision-making

Section 49 of the DPA 2018 prohibits a controller from making a significant decision or a decision that adversely impacts the data subject based solely on automated processing unless that decision is required or authorised by law[57]. A 'significant decision' is one which

[56] Particularly relevant is the Fifth Data Protection Principle, which requires that personal data be kept for no longer than is necessary. What constitutes "no longer than is necessary" will depend on the class of data (for example DNA and fingerprints, which have a retention period governed by the Protection of Freedoms Act 2012).

[57] It is unlikely that an automated decision will be made in the law enforcement context, given the considerable element of human intervention in this space (e.g. police officers).

has an adverse legal effect on the data subject, or which otherwise significantly affects them.

Purely 'automated **decision making**' applies to decisions, often based on algorithms, made wholly without human input. By contrast, decisions involving automated **processing**[58] require the final decision to be made by a human. For example, in the UK speeding cameras are used to enforce speed limits and capture vehicles travelling over the legal limit; when the limit is triggered the camera takes a picture of a vehicle registration for further processing.

This is automated processing and enables police forces to produce a 'speeding ticket' enforcement notice. Before any such ticket is issued a member of police staff – either warranted or civilian – will intervene to ensure the enforcement is legitimate (though a route of appeal is still available).

The UK Government is not currently aware of any wholly automated decision making processes which would fall within Part 3 of the Act. However, to ensure that the rights of data subjects are maintained, sections 49 and 50 of the DPA 2018 enable data subjects to request not to be subject to automated decisions if it might have a significant legal effect on them.

If a significant decision is required by law[59], Section 50 requires the Controller to inform the data subject a decision has been taken based solely on automated processing and provide them with 21 days to ask the controller to reconsider the decision or retake the decision with human intervention.

Whilst it is not current practice in law enforcement processing, it is possible automated decision-making could evolve in a law enforcement context as technology in this space continues to become prevalent. It is therefore possible that new, additional safeguards will be needed as a result of future developments in this area.

Consequently, Section 50 of the DPA 2018 creates a power to make regulations to allow the Secretary of State to impose additional safeguards or amend the existing safeguards. This adds a degree of future proofing to the UK framework and is an important safeguard to protect citizen's rights. This power would be subject to the affirmative process. This means that explicit approval would be required by both Houses of Parliament which adds an additional layer of scrutiny to the power.

---

[58] Automated processing is when an operation is carried out on personal data using pre-determined fixed parameters which allow for no discretion by the system and does not involve further human intervention in its operation to produce a result or output. It is regularly used in law enforcement to filter down large data sets to manageable amounts for a human operator to then use.

[59] This is referred to in the DPA 2018 as a 'qualifying significant decision'.

Restrictions and Safeguards

For important operational reasons, sometimes it is necessary to restrict the rights afforded to data subjects to protect and preserve the administration of justice. The UK has utilised the flexibility afforded by the LED[60] to adapt the framework and restrict some of the rights to enable UK Competent Authorities to continue their important work.

For example, the rights of, provision of information; free access; rectification; erasure and restriction of processing, do not apply to the processing of relevant personal data[61] during a criminal investigation or criminal proceedings, including proceedings for the purpose of executing a criminal penalty. This is because the exercise of such rights could undermine the proceedings e.g. if a person, by requesting access to their personal data, became aware that they were a suspect in a criminal investigation and impeding the legal process.

Moreover, a Competent Authority may restrict (wholly or partly) the provision of information, access, rectification, erasure, and restriction where it is "necessary and proportionate" to:

- avoid obstructing an official or legal inquiry, investigation or procedure;
- avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties;
- protect public security;
- protect national security; or
- protect the rights and freedoms of others

This provision gives the practical effect of allowing Competent Authorities to neither confirm nor deny the existence of personal data and is critically important to protect the effective functioning of the criminal justice system. It is also consistent with the exceptions provided in the LED. For example, there may be occasions when complying with the duty to allow access to data would in itself disclose sensitive or potentially damaging information, thus undermining the point of the restriction and potentially damaging an operation.

However, as a safeguard, where such a restriction is applied, the data subject must be informed that their rights have been restricted and the reasons for the restriction – unless this would undermine the reason for applying it.

Section 42 also requires, as a safeguard against the misuse of the controller's ability to restrict a data subject's rights, that Competent Authorities record the reason for restricting information and to make this record available to the ICO if requested. In addition, data

[60] In Article 18

[61] This is data contained in a judicial decision or in other documents relating to the investigation or proceedings which are created by or on behalf of a court or other judicial authority such as a judge's notes on proceedings.

subjects are empowered through this legislation to approach the ICO or the Courts directly if they believe that their rights have not been respected. This helps to ensure that Competent Authorities apply the exemptions appropriately and proportionately and supports data subjects to exercise their rights.

Exercise of Rights through the Commissioner

As discussed above, where a Competent Authority restricts the rights of the data subject, Section 51 empowers the data subject to request the ICO to check that the restriction imposed by the controller (or, in the case of rectification, that the refusal of the data subject's request to rectify the personal data) was lawful.

The ICO must then take appropriate steps to respond to the request, which may include the exercise of any powers conferred upon the body by the DPA 2018[62]. The ICO has a full suite of regulatory powers and procedural steps at its disposal to ensure Competent Authorities comply with the legal requirements in the Act.

The ICO must inform the data subject whether they deem the restriction to be lawful, as well as the right of the data subject to take the matter to court. The ICO must also inform the data subject of any further steps that they themselves are considering taking under Part 6 of the DPA 2018. The ICO have a proven track record of effective and robust action against Competent Authorities.

The ICO's regulatory powers and track record are set out in detail in Section G of this pack. Section G also includes information on judicial redress for data subjects.

National Security certificates

Section 79 of the DPA 2018 provides that a Minister of the Crown (as defined in subsection (12)) may issue a certificate certifying that a restriction, wholly or partly, is a necessary and proportionate measure to protect national security.

Subsection (3) provides that such a certificate is to be taken as conclusive evidence that the restriction (both specific and general) is required. A certificate issued by a Minister of the Crown is a means of giving a controller legal certainty as to the application of a restriction.

This replicates analogous provisions in Section 28 of the DPA 1998 and is consistent with the provisions elsewhere in the DPA 2018 (national security certificates are available in the UK GDPR and Part 4). Section 130 of the DPA 2018 requires the ICO to publish a record of all

[62] See Sections 142 to 146 of the DPA 2018, which refer to a suite of enforcement powers including information and assessment notices.

national security certificates which have been issued, ensuring greater transparency on the use of such certificates than under the previous data protection legislation

The ICO will publish details of all national security certificates which have been issued, including the full text of the certificate where possible. There may be some cases where the text of the certificate is sensitive and cannot be published. In those cases, the fact of the certificate, the date it was signed, and which minister signed it, will still be published.

Any person directly affected by the issuing of any certificate may appeal to the tribunal to challenge the decision to issue the certificate. Such an appeal would be heard by the Upper Tribunal which would apply judicial review principles when determining the appeal.

In applying such principles, the Upper Tribunal would be able to consider a wide range of issues, including necessity, proportionality, and lawfulness. This would enable, for example, the Upper Tribunal to consider whether the decision to issue the certificate was reasonable, having regard to the impact on the rights of data subjects and balancing the need to safeguard national security.

PART III: ACCOUNTABILITY AND COMPLIANCE

The LED requires Competent Authorities to adopt a proactive, systematic, and accountable attitude towards data protection compliance on a wholesale basis.

Sections 55 to 71 of the DPA 2018 place both general obligations – such as the duty to cooperate with the ICO – and specific obligations on Competent Authorities – for example, the requirement that they have in place a Data Protection Officer ("DPO"). This ensures accountability and compliance and is important in a law enforcement context as it helps to maintain public trust.

These sections do not apply a "one size fits all" approach to accountability and compliance. Rather, they ask Competent Authorities to implement technical and organisation measures that are appropriate to the risks[63] to individuals' rights and freedoms that arise from processing, while the oversight of the ICO and DPO in contrast remain constant. Any measures that are implemented must also be reviewed and updated where necessary.

It is also worth noting that Article 21 of the LED provided Member States with the power to designate 'Joint Controllers' and, within this provision, which controller should be the lead controller. The UK has chosen not to implement this, as it may not account for the nuances of the relationship between controllers in common.

[63] Section 66 further emphasises that security of personal data held must be at a level appropriate to the risks of processing.

Instead, Section 58 requires joint controllers to ensure there is an unambiguous apportionment of responsibilities to ensure accountability, and to decide which controller will provide which function. This section also contains a derogation allowing Member States to allow data subjects to bring proceedings against each of the controllers involved. The UK has not restricted the rights of the data subject in this respect thereby giving effect to the derogation.

Furthermore, Part 3 of the DPA 2018 sets out various measures to ensure the accountability of controllers and processors. These include:

- Data Protection by Design and Default: Section 57 of the DPA 2018 places a requirement on controllers to implement appropriate technical and organisational measures to ensure that only personal data which is necessary for each specific purpose of the processing is processed. It also aims to restrict access to data.

  For example, the Police National Database allows the police service to share local information and intelligence on a national basis. It is available to all forces and some of the National agencies, but access is restricted to those officers who are appropriately trained to handle intelligence and also those with a legitimate need to access the data.

  This section also enables Competent Authorities to become more cost effective by "designing-in" data protection and privacy at the start of system or project development, thereby avoiding often costly attempts to retrofit these after implementation. Significantly, this places data protection at the heart of system design and processing operations.

  It is **identical** to Article 20 of the LED except for:
  - Removal of the reference to Member State or Union law and EU mechanisms, bodies or institutions; and
  - Removal of examples such as pseudonymisation or data minimisation.

- Security of Measures: Section 66 of the DPA 2018 emphasises that each controller and each processor must implement appropriate technical and organisational measures to ensure a level of security appropriate to the risks arising from the processing of personal data. It is **identical** to its LED counterpart (Article 29) except for summarising various concepts set out under Article 29, such as data media control, storage control, and user control under "unauthorised interference" in Section 66.

- Processing carried out on behalf of a controller: Sections 59 and 60 provide a suite of measures to ensure that, where a controller delegates the processing to another organisation, that organisation meets the requirements of the DPA 2018. These are

identical to their LED counterparts (Articles 22–23). The DPA 2018 provides for the processor to be liable for their activities in essentially the same way as a controller.

If a situation arises whereby a processor begins to determine the purpose and means of processing, in breach of Part 3 of the DPA 2018, they then, by default, become a controller in respect of that data. Importantly, this means that the processor then takes on the liabilities of a controller in their own right and would be required to demonstrate compliance as such.

In a Part 3 context, this means that if the processor is not a "Competent Authority" as defined in Part 3, they move to the UK GDPR regime and would be subject to the additional requirements of that regime. Even so, given that the data being processed may well be of a sensitive nature, it is entirely appropriate that the person or organisation who determines the means and purpose of that processing is held legally responsible.

- The Designation of Data Protection Officers (DPO): Sections 69–71 of the DPA 2018 set out the requirement to regarding the designation, position, and tasks of the DPO. This requirement did not exist in the previous legislation (Data Protection Act 1998) but it is not a new concept amongst the Law Enforcement community, where a similar role for data protection implementation and advice is long established. This part is **identical** to its LED counterpart (Article 32), except for:
    - the replacement of the reference to Member State or Union law to domestic law;
    - exempting courts and other independent judicial authorities when acting in their judicial capacity from that obligation. This is legislated for in the LED;[64]
    - an additional subparagraph (Section 70(3)) making clear that the DPO should not be asked to perform any duties that could give rise to a conflict of interest.

- Data Protection Impact Assessments: Sections 64 and 65 of the DPA 2018 outline the circumstances in which controllers are required to carry out a data protection impact assessment, as well as cases in which prior consultation with the ICO is necessary. These are **identical** to their LED counterparts (Articles 64–65) except for:
    - Removal of the reference to Member State or Union law and EU mechanisms, bodies or institutions; and
    - Replacement of the term *"supervisory authority"* with the ICO.

[64] Article 32(1).

Prior to the DPA 2018 coming into force, controllers were already encouraged to complete a DPIA and many Competent Authorities did so as a matter of good practice. However, Section 64 renders DPIAs a legal requirement for processing that is likely to be "high risk".

This could refer to any processing activity that is likely to have significant impact on an individual. In a law enforcement context, whilst not exhaustive, this may include any use of new innovative technology, or any new use of existing technology (such as AI) or processing of biometric data for the purpose of uniquely identifying an individual (such as facial recognition). Moreover, this requirement ensures routine completion of DPIAs is mainstreamed in internal data protection practice whilst keeping data protection concerns at the forefront of any new processing activity.

- Breach notification: Sections 67–68 of the DPA 2018 place a requirement on controllers and processors to notify the ICO in the case of a personal data breach. The articles are **identical** to their LED counterparts (Articles 30–31), except for alteration of EU terminology. Data breaches can cause numerous and significant issues. In a law enforcement context, this could be particularly serious, as it could result in reputational damage and a loss of confidentiality.

  Section 68 requires Competent Authorities to notify the data subject, when there is likely to be a **high** risk to the rights and freedoms of an individual as a result of a data breach (for example financial loss or reputational damage). This is important, as it enables data subjects to take the necessary precautions to protect themselves and also enables the Competent Authority to acknowledge their mistake and apologise if that is appropriate.

  In practice, the threshold for notifying individuals is higher than the requirement to notify the ICO. The duty to notify data subjects bites when none of the provisions in Section 68(3) or 68(7) apply – if; the data involved in the breach is either encrypted or unintelligible, or if the Competent Authority has taken the right mitigating action to prevent the high risk from actually materialising, then the duty to notify the data subject falls away. As a safeguard against misuse of this provision, Section 68(6) enables the ICO to require Competent Authorities to notify the data subject, if they disagree with the Competent Authorities' assessment of the risk involved.

- Records of Processing Activities: Section 61 sets out the requirement to maintain a record of processing activities. The article is **identical** to its LED counterpart (Article 24), except for
  - The replacement of the reference to supervisory authority, with the ICO.
  - The ability to provide, as appropriate, a general description of the technical and organisational security measures referred to in Section 66 of the DPA

2018 rather than the technical and organisational security measures referred to in Article 29(1).

- Logging: Section 62 of the DPA 2018 sets out the requirement for law enforcement agencies (acting as controller) and/or processors (acting under the conditions set out in Section 59) to keep logs of their automated processing operations.[65]

  The logs are to be used for assisting controllers and processors to verify the lawfulness of the processing, for self-monitoring purposes (including internal disciplinary proceedings), for ensuring the security and integrity of the data being processed, and to support criminal proceedings. This means at any time the controller or the ICO can check their compliance with Part 3 requirements.

  These are **identical** to their LED counterparts (Articles 25–26). Article 63(2) of the LED provides a derogation allowing a transitionary period until May 2023 to bring older systems into compliance. This is reflected in Schedule 20(14) in respect of legacy systems.

[65] At least for collection, alteration, consultation, disclosure (including transfers), combination and erasure.

PART IV: INTERNATIONAL TRANSFERS

The UK applies high standards of data protection and enshrines the rights of data subjects within its legal framework for international transfers of law enforcement data to countries outside of the EU. This part explains the provisions set out in:

- the DPA 2018
- the Data Protection, Privacy and Electronic Communications Regulations 2019

DPA 2018

The DPA 2018 provides the legal framework for competent authorities to transfer personal data to third countries.[66] Before transferring data, competent authorities must (in line with the LED) meet three conditions:

- the transfer must be necessary for any of the law enforcement purposes;
- the transfer must be based on:
    - an adequacy decision in respect of the third country;[67] or
    - if not based on an adequacy decision, the existence of appropriate safeguards; or
    - if not based on an adequacy decision or on there being appropriate safeguards, is based on special circumstances; and
- The transfer must be to:
    - a relevant authority (i.e. the equivalent of a competent authority) in the third country;
    - a 'relevant international organisation' e.g. an international body that carries out functions for any of the law enforcement purposes; or
    - a person other than a relevant authority, provided it is strictly necessary for performing one of the law enforcement purposes; there are no fundamental rights and freedoms of the data subject concerned that override the public interest necessitating the transfer; the transfer of the personal data to a relevant authority in the third country would be ineffective or inappropriate; and the recipient is informed of the purposes for which the data may be processed.

As highlighted above, transfers to third countries without an adequacy decision may be made with assurance that appropriate safeguards are in place. These safeguards may be provided through:

- a legal instrument providing appropriate safeguards for the protection of personal data binds the intended recipient; or

[66] Chapter 5 of Part 3 of the DPA 2018.
[67] Currently no adequacy decisions have been made with respect to law enforcement specifically.

- an assessment performed by the controller which, having assessed all the circumstances[68] surrounding transfers of that type of personal data to a third country, concludes that appropriate safeguards exist.

Where the transfer is based on the latter point, the transfer's date, time, and justification, the name of and any other pertinent information about the recipient, and a description of the personal data transferred must be documented, and provided to the ICO upon request.

If a transfer is not based on an adequacy decision or appropriate safeguards, it may be based on special circumstances, which are:

a. to protect the vital interests of the data subject or another person;
b. to safeguard the legitimate interests of the data subject;
c. for the prevention of an immediate and serious threat to the public security of a member state or third country;
d. in individual cases for any of the law enforcement purposes; or
e. in individual cases for a legal purpose (such as in relation to legal proceedings or to obtain legal advice).

When a transfer is made, the transfer's date, time and justification, the name of and any other pertinent information about the recipient, and a description of the personal data transferred must be documented, and provided to the ICO upon request.

If the competent authority determines that the fundamental rights and freedoms of the data subject override the public interest in the transfer then transfers under points d and e above are prohibited.

Onward transfers

Where personal data is transferred from the UK to third countries or international organisations, any subsequent transfer must only, in principle,[69] take place after the competent authority from which the data was obtained has given its authorisation (the original transfer should provide the recipient with any specific handling conditions).

When deciding on a request for the authorisation of an onward transfer, the competent authority that carried out the original transfer should take due account of all relevant factors, including:

a. the seriousness of the circumstances leading to the request for authorisation of the subsequent transfer;

[68] This could include whether the body has any co-operation agreements with Europol or Eurojust, the level of confidentiality applied to the data, ensuring the data will not be processed for other purposes than for the purposes of the transfer. In addition, it is likely to include a consideration of human rights such as ensuring that the data would not be used to impose the death penalty on an individual or any other form of cruel and inhuman treatment.

[69] See last paragraph of this section.

b. the purpose for which the personal data was originally transferred; and
c. the standards of data protection which apply in the country or international organisation to which the data will be transferred.

The competent authority that carried out the original transfer should also be able to subject the onward transfer to specific conditions. Such specific conditions can be described, for example, in handling codes.

If the personal data was originally received from a competent authority in another EU Member State, that authority must first authorise any onward transfer unless the controller determines that the transfer is necessary for the prevention of an immediate and serious threat either to the public security of a Member State or a third country or to the essential interests of a Member State, and it cannot be obtained in good time (in which case the relevant authority must be informed without delay).

Data Protection, Privacy and Electronic Communications Regulations 2019

In the process of transferring data with third countries, the UK has no plans to lower its data protection standards below those enshrined in the DPA 2018. The legislation the Parliament has recently passed (the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 (the DPPEC Regulations)) further illustrates this.[70]

Paragraph 42 of Schedule 2 to the DPPEC Regulations effectively replicates the provisions of Article 36 of the LED, and inserts these into Section 74 of the DPA 2018.[71] It differs from the previous drafting of Section 74 (which was operable prior to the UK's exiting of the EU), in the single sense that it repatriates the power to make an adequacy decision regarding a third country from the European Commission to the Secretary of State.

Reviews of an adequacy decision will take place at an interval of no more than four years.

Transitional Adequacy Provisions for EU Member States

The UK has already taken steps to maintain existing outgoing flows of data as an interim measure in a no deal scenario from the UK to the EU Member States and Gibraltar through the DPPEC Regulations.

[70] These were debated and approved by Parliament and made by the Minister on the 28th February 2019. They are available at: http://www.legislation.gov.uk/uksi/2019/419/contents/made

[71] Paragraph 42 of Schedule 2 to the DPPEC Regulations is available at: http://www.legislation.gov.uk/uksi/2019/419/schedule/2/paragraph/42/made

These Regulations seek to minimise the impact for data flows from the UK to the EU[72] by deeming adequate[73] the EU and Gibraltar, in the event of a no deal, allowing the free flow of data from the UK to these jurisdictions with no need to rely on alternative mechanisms for transfers.

PART V: OVERSIGHT, ENFORCEMENT, AND REDRESS

A key feature of modern policing and law enforcement in the United Kingdom is the presence of external agencies that offer oversight of the law enforcement partners privy to Part 3 of the DPA 2018.[74]

This part will highlight additional oversight requirements in other pieces of domestic legislation on law enforcement data processing.

ICO

Article 41 of the LED permitted Member States to designate that the Supervisory Authority required to be established by the EU GDPR (in the case of the UK, the ICO) be the same authority for the purposes of the Directive. Having a single authority deal with all data protection issues ensures that there is a common standard for all personal data processing, whether general or law enforcement related.

This section has detailed the role of the ICO in relation to ensuring compliance with the Part 3 requirements. The ICO has a number of enforcement powers which they can utilise to ensure the requirements are met and to uphold data subjects' rights, including information notices through to large fines in particularly serious breaches. Further details on this are in Section G of this pack.

Additionally, the ICO pay close attention to the development of new technologies which use personal data. For example, they were an intervener in the recent court case *R (Bridges) v Chief Constable of South Wales Police*. This was a case concerning the legality of the use of Live Facial Recognition (LFR) by the police in which the High Court found that South Wales Police were operating their LFR system lawfully.

As an illustration of the importance the UK places on effective enforcement, it is worth noting that Article 57 of the LED required Member States to ensure effective penalties are in place to actively dissuade Competent Authorities from breaching the requirements of Part

[72] And to the EEA for general processing.
[73] To see these changes please see paragraph 102 of Schedule 2 to the DPPEC Regulations, which will insert a new Schedule 21 into the DPA 2018. This new Schedule 21 to the DPA 2018 makes transitional provision with part 3 of this new Schedule relating to international transfers.
[74] For more information on the ICO, please refer to Section G of this pack.

3, but it is silent on the range of the penalty available.

To ensure consistency between application of the UK GDPR and the transposition of the LED, the UK implemented **the same penalties** specified in the UK GDPR to Part 3 processing. Depending on the breach, this could be up to £8,700,000 or up to £17,500,000. Failure to comply with sections 35, 36, 37, 38(1), 39(1), 40, 44, 45, 46, 47, 48, 49, 52, 53, 73, 74, 75, 76, 77 or 78 would attract the higher rate. This sends a strong message to Competent Authorities that even though they are public sector bodies, they are not immune from effective enforcement action.

Recent examples of enforcement action, the ICO have taken against law enforcement agencies include:[75]

- In 2018, an investigation by the ICO found that the Metropolitan Police Service's (MPS) use of the Gangs Matrix, a database that records intelligence related to alleged gang members, led to multiple and serious breaches of data protection laws. An **enforcement notice was issued**, compelling the MPS to ensure it complies with data protection laws in the future. They were given six months to implement recommended changes.
- In 2018, the ICO **fined Gloucestershire Police £80,000** after sending a bulk email that identified victims of non-recent child abuse.
- In 2018, the ICO **fined the Crown Prosecution Service (CPS) £325,000** after they lost unencrypted DVDs containing recordings of police interviews.

Other Oversight Mechanisms

In addition to the ICO, there are a number of external agencies that offer oversight of law enforcement partners processing data under Part 3 of the DPA 2018.

For ease of reference, the scope of these agencies has been narrowed to those who interact most frequently with the Government's principle law enforcement partners. They include regulators, advisory groups, and independent oversight bodies. This section details their approach to, and guidance issued on, privacy and data protection more broadly, and demonstrates how they comply with the DPA 2018.

Investigatory Powers Commissioner's Office (IPCO)

The Investigatory Powers Commissioner's Office provides independent oversight of the use of investigatory powers by intelligence agencies, police forces, and other public authorities.

[75] For further information on the ICO's enforcement powers, please see Section G of the adequacy pack.

To ensure greater compliance, the IPCO has a significantly expanded staff compared to its predecessor organisations, including a team of inspectors, in-house legal and technical expertise, and a Technical Advisory Panel (TAP) to provide expert advice.

The IPCO is also responsible for keeping the interception of communications and the acquisition and disclosure of communications data by intelligence agencies, police forces and other public authorities under review.

To reflect their functions, the police and law enforcement bodies have more limited powers under the investigatory powers legislation compared to the intelligence community (UKIC).[76] Even though these powers are less frequently used, IPCO's inspections ensure that the law enforcement community are aware of their obligations.

The IPCO report to the Prime Minister on a half-yearly basis with respect to the carrying out of the Interception of Communications Commissioner's functions.

The IPCO's aim is to provide effective oversight to ensure that the conduct of public authorities is compliant in relation to the following statutory functions:

- Interception of Communications under Chapter 1 of Part 1 Regulation of Investigatory Powers Act 2000 (RIPA);
- Acquisition and Disclosure of Communications Data under Chapter 2 Part 1 of RIPA;
- Encryption notices issued by the Secretary of State under Part 3 of RIPA in relation to the information obtained under Chapter 1 Part 1 RIPA; and
- Complaints of unintentional unlawful electronic interception (which attract a civil monetary penalty) under section 1(1.A) of RIPA.

Her Majesty's Inspectorate of the Constabulary and Fire and Rescue Services (HMICFRS) and Her Majesty's Inspectorate of Constabulary in Scotland (HMICS)

The HMICFRS has statutory responsibility for the inspection of the police forces, and since July 2017 the fire and rescue services, of England and Wales. The HMICS provides independent scrutiny of both Police Scotland and the Scottish Police Authority (SPA).

They function as inspectorates, rather than as a regulator, and therefore while they may submit recommendations to police forces to improve their performance, they do not directly hold these forces to account. These recommendations are made public and forces consider HMICFRS' ratings as a serious matter.[77]

Case Study: Police National Computer Audits

[76] For further information on UKIC and the IPA, please see Section H of the pack.

[77] For example, Kent Police received an 'Inadequate' in the CDI inspections of 2017. They followed the Inspectorate's recommendations and made a series of extensive improvements to their management of data. The force was subsequently rated 'Outstanding' in the same inspections of 2018.

The Inspectorate have consistently engaged in data handling and information management by police forces over the past decade. In 1998, a Police Research Group Report was produced which highlighted concerns and issues relating to the quality of data being inputted onto the Police National Computer (PNC).

In 2000 the HMIC (prior to their taking on of fire and rescue inspections) report 'On the Record' investigated data quality and the management of PNC data. The report recommended that HMIC should monitor force performance against a set of targets embedded in the Association of Chief Police Officers (ACPO) PNC Compliance Strategy. A further two reports were produced by HMIC in 2001 and 2002.

The Metropolitan Police Service's (MPS) PNC Steering Group were one of the forces across the United Kingdom that responded to the Inspections (as is their statutory responsibility), with updates on their commitment to implementing the inspectorate's recommendations. This included developing risk assessed Force Data Protection Officer audit programmes. Following the first run of this programme, the MPS identified resources required and allocated them under the management of the Data Protection Officer.

In 2003, the HMIC PNC Compliance Audit Team was formed to carry out focused PNC inspections of all forces in England and Wales and on invitation from HMIC (Scotland) to inspect the Scottish police forces. Further reports on the PNC were published between 2004 to 2010. This audit function was recently extended to cover non police use of PNC.

Biometrics Commissioner

The Biometrics Commissioner is independent of government. The Commissioner's role is to keep the retention and use by the police of DNA samples, DNA profiles, and fingerprints under review. The statute introduced a new regime to govern the retention and use by the police of DNA samples, profiles, and fingerprints. The Commissioner does not have jurisdiction in Scotland, except in respect of his power to review national security determinations which are made or renewed by the police in connection with the retention of DNA profiles and fingerprints.

The role further includes:

- deciding applications by the police to retain DNA profiles and fingerprints (under section 63G of the Police and Criminal Evidence Act 1984);
- reviewing national security determinations which are made or renewed by the police in connection with the retention of DNA profiles and fingerprints; and
- providing reports to the Home Secretary about the carrying out of their functions.

Where an individual is arrested for, but not charged with, specific offences, their DNA profile and fingerprint record will normally be deleted. However, the police can apply to the Biometrics Commissioner for permission to retain their DNA profile and fingerprint record for a period of up to 3 years. The application must be made within 28 days of the police decision not to proceed with a prosecution.

If the police make such an application, the Biometrics Commissioner would first give both them and the arrested individual an opportunity to make written representations and then, taking into account factors including the age and vulnerability of the victim(s) of the alleged offences, and their relationship to the suspect, make a decision on whether or not retention is appropriate.

If the Biometrics Commissioner agrees to allow retention, the police will be able to retain that individual's DNA profile and fingerprint record for a period of up to 3 years from the date the samples were taken. At the end of that period, the police will be able to apply to a District Judge (Magistrates' Courts) for a single 2 year extension to the retention period. If the application is rejected, the force must then destroy the DNA profile and fingerprint record.

Where the Biometrics Commissioner considers that the making, or renewal, of an application to allow retention is unnecessary, he has the power to order the destruction of the DNA profile or fingerprint record in question

Surveillance Camera Commissioner

The Office of the Commissioner was created under the Protection of Freedoms Act 2012 to further regulate CCTV in England and Wales. The Act required a code of practice about surveillance camera systems to be produced and it sets out new guidelines for CCTV and automatic number plate recognition. The role of the Surveillance Camera Commissioner is to:

- encourage compliance with the surveillance camera code of practice;
- review how the code is working; and
- to provide advice to ministers on whether the code needs amending.

The Commissioner has no enforcement or inspection powers. They work with relevant authorities to make them aware of their duty to have regard to the code.[78] The Commissioner further:

- provides advice on the effective, appropriate, proportionate, and transparent use of surveillance camera systems;

[78] The Commissioner is not responsible for enforcing the code, inspecting CCTV operators to check they are complying with the code, providing advice regarding covert surveillance, and providing advice regarding domestic CCTV systems.

- reviews how the code is working and, if necessary, add others to the list of authorities who must have due regard to the code; and
- provides advice on operational and technical standards.

The code sets out twelve guiding principles which strike a balance between protecting the public and upholding civil liberties. They affirm the principles of necessity and proportionality that underpin Part 3 of the DPA 2018.[79] More recently, in March 2019 the Surveillance Camera Commissioner published guidance to assist policing authorities using LFR to comply with their statutory obligations arising from Section 31(1) of PoFA and the Surveillance Camera Code of Practice.[80]

Both the Biometrics and Surveillance Camera Commissioners submit annual reports to the Home Secretary, which are then laid before Parliament.

College of Policing

The College of Policing was established in 2012 as the professional body for everyone who works for the police service in England and Wales. The purpose of the College is to provide those working in policing with the skills and knowledge necessary to prevent crime, protect the public, and secure public trust.

The College's Authorised Professional Practice provide an online and public guide to data protection for police officers, including measures in place prior to any data security incident, and reactive measures to handle a data breach incident if one occurs. It also influences the development of retention and disposal schedules in some forces.

The College recommends that the national policing lead for data protection should be contacted if a data breach affects more than one force. The College also provides further advice to mitigate risks around data breaches by external organisations.

Select Committees

[79] For example, Principle 1 states: "Use of a surveillance camera system must always be for a specified purpose which is in pursuit of a legitimate aim and necessary to meet an identified pressing need", and Principle 6 states : "No more images and information should be stored than that which is strictly required for the stated purpose ...".

[80] The guidance is available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/786392/AFR_police_guidance_of_PoFA_V1_March_2019.pdf.

The Home Affairs Select Committee (HASC)[81] is one[82] of the Departmental Select Committees, the powers of which are set out in the House of Commons Standing Orders.[83] The Committee consists of 11 Members of Parliament, drawn from the three largest political parties. The House of Commons appoints the Committee with the task of examining the expenditure, administration, and policy of the Home Office and its associated public bodies. In Scotland, the Justice Subcommittee on Policing, performs the same function. [84]

Select Committees choose their own subjects of inquiry and seek written and oral evidence from a wide range of relevant groups and individuals. At the end of an inquiry, the Committee will often produce a report setting out its findings and making recommendations to the Government. The Government is expected to respond to each of the report's recommendations.

In 2018, HASC launched an inquiry into the challenges facing the police and their readiness to respond to them. The report welcomed efforts to integrate the police with other public services and other multi-agency teams. The report also emphasised the role of police in protecting vulnerable people from harm, and recommended a less risk-averse approach to data-sharing towards these ends.

Additional Statutory Requirements

Police and Criminal Evidence Act 1984 (PACE) Criminal Justice (Scotland) Act 2016 and the Criminal Procedure (Scotland) Act 1995

Combined, these Acts govern the major part of police powers of investigation, including arrest, detention, interrogation, entry and search of premises, personal search, and the taking of samples in the UK. As part of this legislation, there are statutory PACE Codes of Practice, which police officers are required to consider and refer to when carrying out various procedures associated with their work. The Act attempts to strike a fair balance between the exercise of power by those in authority and the rights of members of the public.

PACE Codes of Practice

---

[81] https://www.parliament.uk/business/committees/committees-a-z/commons-select/home-affairs-committee/

[82] The Science and Technology Committee is another example of a Select Committee which scrutinises, amongst other things, policing use of technology. https://www.parliament.uk/business/committees/committees-a-z/commons-select/science-and-technology-committee/

[83] Standing Orders can be found at: https://www.parliament.uk/business/publications/commons/standing-orders-public11/

[84] https://www.parliament.scot/parliamentarybusiness/CurrentCommittees/policing-sub-committee.aspx

The PACE Codes of Practice[85] regulate police powers in England and Wales and protect public rights. These strike a balance between the powers of the police and the rights and freedoms of the public.

Code D is particularly relevant to the processing of data by the police. It concerns the principal methods used by police to identify people in connection with the investigation of offences and the keeping of accurate and reliable criminal records. The provisions of the PACE coupled with Code D (and read alongside MoPI) are designed to make sure fingerprints, samples, impressions, and photographs are taken, used, and retained, with identification procedures carried out only when justified and necessary for preventing, detecting, or investigating crime.

Failure to observe the requirement detailed in PACE can have very serious consequences affecting the viability of trials. Section 57 of the Criminal Justice (Scotland) Act 2016 requires the Lord Advocate to issue a Code of practice about investigative functions. This included the questioning, and recording of questioning, of persons suspected of committing offences, and the conduct of identification procedures involving such persons.

To a lesser extent, Code E and Code F which cover the audio and visual recording of interviews with suspects in a police station or other suitable location, are also broadly relevant to information management, particularly as they engage the sixth Data Principle on the secure processing of personal data. Both Codes issue security requirements on all recordings, from sealed master recordings to those taken on secure digital networks or away from a police station.

Section 200 of the DPA 2018 requires that the ICO produce and publish guidance about how they propose to perform their legislative duty to have regard to the PACE Codes of Practice when investigating offences and charging offenders. The issue of such guidance is aimed to assist the police in its obligations to ensure that personal data be adequate, relevant, and not excessive for the purpose(s) they are being processed, in line with the Data Protection Principles. This also ensures that PACE and the DPA 2018 offer a consistent message on privacy.

Protection of Freedoms Act 2012

The Protection of Freedoms Act 2012[86] ("PoFA") brings in a number of changes across the criminal justice landscape in England and Wales and has been seen as part of a rebalancing exercise of rights in favour of the individual.

Of particular relevance, Part 1 Chapter 1 of the Act covers the retention of DNA and fingerprints by the police. The equivalent provisions in Northern Ireland are contained

[85] https://www.gov.uk/guidance/police-and-criminal-evidence-act-1984-pace-codes-of-practice
[86] http://www.legislation.gov.uk/ukpga/2012/9/contents/enacted

within the Criminal Justice (Northern Ireland) Act 2013. The Act has yet to be commenced; however, PSNI have taken an operational decision to start complying with the provisions of the Act, likely from September, on a non-statutory basis. In Scotland, the equivalent provisions are contained in the Criminal Procedure (Scotland) Act 1995, although the provisions in relation to the Biometrics Commissioner will be implemented via the Scottish Biometrics Commissioner Bill[87].

The legislation strikes a balance between protecting the freedoms of those who are innocent of any offence, whilst ensuring that the police continue to have the capability to protect the public and bring criminals to justice.

PoFA was enacted in response to the 2008 judgment of the European Court of Human Rights (ECHR) in the case of *S and Marper v UK*.[88] In this case, the court ruled that the blanket retention of DNA profiles posed a disproportionate interference with the right to respect private life, in violation of Article 8 of the European Convention on Human Rights.

In regard to biometric data, PoFA amended Part V of PACE to only allow for the indefinite retention of fingerprints and DNA profiles on convicted adults, or adults who have been charged but hold a previous conviction. The Act excludes under-18s, and non-convicted adults from indefinite biometric data retention, and reduces the length of time for which data on these persons can be retained.

PoFA also goes beyond the 2008 ECHR judgment in its protection of the right to respect privacy. The Act requires all DNA samples to be destroyed within 6 months of being taken[89], regardless of whether the subject has faced or is facing a conviction. This allows sufficient time for the sample to be analysed and a DNA profile to be produced for use on the database.

Any data retained is limited in its use by the police for the purposes of national security, conducting a terrorist investigation, the prevention or detection of crime, the investigation of an offence or the conduct of a prosecution, and the identification of a deceased person.

Section 20 of PoFA establishes the independent office of Commissioner for the Retention and Use of Biometric Material (the 'Biometrics Commissioner': see above).

PoFA also makes a contribution towards safeguarding the vulnerable and criminal records. Criminal records disclosure is required for anyone working or involved in activities with vulnerable groups. Chapter 2 takes some activities completely outside the scope of the

[87] https://www.parliament.scot/parliamentarybusiness/Bills/111859.aspx
[88] https://hudoc.echr.coe.int/eng#{"fulltext":["S & Marper"],"documentcollectionid2":["GRANDCHAMBER","CHAMBER"],"itemid":["001-90051"]}
[89] The only exception to this is if the sample is required for use as evidence in court.

regime, and changes the rules relating to disclosure, giving applicants, rather than the Disclosure and Barring Service, greater control over who is provided with their information.

On data protection more broadly, PoFA gives the right to have certain data provided in an electronic form suitable for reuse, and amends provisions relating to the appointment, role, and tenure of the Information Commissioner.

PoFA also created the role of Surveillance Camera Commissioner, which as detailed above, encourages compliance with the Surveillance Camera Code of Practice[90]. The code sets out twelve guiding principles which strike a balance between protecting the public and upholding civil liberties; they affirm the principles of necessity and proportionality that underpin Part 3 of the DPA 2018.

Redress

Outside of ICO enforcement action, there are clear judicial routes for redress available to data subjects such as through the First Tier Tribunal (General Regulatory Chamber) and the Upper Tribunal. More detail is available on these routes in Section G.

90 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/282774/SurveillanceCameraCodePractice.pdf