COMMISSION IMPLEMENTING DECISION (EU) 2021/1773

of 28 June 2021

pursuant to Directive (EU) 2016/680 of the European Parliament and of the Council on the adequate protection of personal data by the United Kingdom

(notified under document C(2021) 4801)

THE EUROPEAN COMMISSION,

Having regard to the Treaty on the Functioning of the European Union,

Having regard to Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA ([1]), and in particular Article 36(3) thereof,

Whereas:

1. INTRODUCTION

(1) Directive (EU) 2016/680 sets out the rules for the transfer of personal data from competent authorities in the Union to third countries and international organisations to the extent that such transfers fall within its scope of application. The rules on international data transfers by competent authorities are laid down in Chapter V of the Directive (EU) 2016/680, more specifically in Articles 35 to 40. While the flow of personal data to and from countries outside the European Union is essential for efficient law enforcement cooperation, it must be guaranteed that the level of protection afforded to personal data in the European Union is not undermined by such transfers ([2]).

(2) Pursuant to Article 36(3) of Directive (EU) 2016/680, the Commission may decide, by means of an implementing act, that a third country, a territory or one or more specified sectors within a third country or an international organisation ensure(s) an adequate level of protection. Under this condition, transfers of personal data to a third country may take place without the need to obtain any further authorisation (except where another Member State from which the data were obtained has to give its authorisation to the transfer), as provided for in Article 35(1) and recital 66 of the Directive (EU) 2016/680.

(3) As specified in Article 36(2) of Directive (EU) 2016/680, the adoption of an adequacy decision has to be based on a comprehensive analysis of the third country's legal order. In its assessment, the Commission has to determine whether the third country in question guarantees a level of protection 'essentially equivalent' to that ensured within the European Union (recital 67 of Directive (EU) 2016/680). The standard against which the 'essential equivalence' is assessed is that set by EU legislation, notably Directive (EU) 2016/680, as well as the case-law of the Court of Justice of the European Union ([3]). The European Data Protection Board's adequacy referential is also of significance in this regard ([4]).

(4) As clarified by the Court of Justice of the European Union, this does not require finding an identical level of protection ([5]). In particular, the means to which the third country in question has recourse for protecting personal data may differ from the ones employed in the European Union, as long as they prove, in practice, effective for ensuring an adequate level of protection ([6]). The adequacy standard therefore does not require a point-to-point replication of Union rules. Rather, the test lies in whether, through the substance of privacy rights and their effective implementation, supervision and enforcement, the foreign system as a whole delivers the required level of protection ([7]).

([1]) OJ L 119, 4.5.2016, p. 89.
([2]) See recital 64 of Directive (EU) 2016/680.
([3]) See, most recently, Case C-311/18, *Maximilian Schrems v Data Protection Commissioner* ('*Schrems II*') ECLI:EU:C:2020:559.
([4]) See Recommendation 01/2021 on the adequacy referential under the Law Enforcement Directive, adopted on February 2021, available at the following link: https://edpb.europa.eu/our-work-tools/general-guidance/police-justice-guidelines-recommendations-best-practices_en
([5]) Case C-362/14, *Maximilian Schrems v Data Protection Commissioner* ('*Schrems*'), ECLI:EU:C:2015:650, paragraph 73.
([6]) *Schrems*, paragraph 74.
([7]) Communication from the Commission to the European Parliament and the Council, Exchanging and Protecting Personal Data in a Globalised World, COM(2017) 7 of 10.1.2017, Section 3.1, pp. 6-7, available at the following link: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017DC0007&from=EN

(5) The Commission has carefully analysed the relevant law and practice of the United Kingdom (UK). Based on its findings, set out below, the Commission concludes that the United Kingdom ensures an adequate level of protection for personal data transferred from competent authorities in the Union, falling within the scope of Directive (EU) 2016/680, to competent authorities in the United Kingdom falling within the scope of Part 3 of the Data Protection Act 2018 (DPA 2018) ([8]).

(6) This Decision has the effect that such transfers may take place without the need to obtain any further authorisation for a period of four years, subject to possible renewal, and without prejudice to the conditions laid down in Article 35 of the Directive (EU) 2016/680.

2. RULES APPLYING TO THE PROCESSING OF PERSONAL DATA BY COMPETENT AUTHORITIES FOR THE CRIMINAL LAW ENFORCEMENT PURPOSES

2.1. The constitutional framework

(7) The United Kingdom is a parliamentary democracy. It has a sovereign parliament, which is supreme to all other government institutions, an executive drawn from and accountable to parliament and an independent judiciary. The Executive draws its authority from its ability to command the confidence of the elected House of Commons and is accountable to both Houses of Parliament (House of Commons and House of Lords) which are responsible for scrutinising the Government and debating and passing laws. The United Kingdom Parliament has devolved responsibility to the Scottish Parliament, the Welsh Parliament (Senedd Cymru), and the Northern Ireland Assembly for legislating on certain domestic matters in Scotland, Wales and Northern Ireland. While data protection is a matter reserved for the United Kingdom Parliament, i.e. the same legislation applies across the country, other areas of policy relevant to this Decision are devolved. For instance, the criminal justice systems, including policing (the activities carried out by police forces) of Scotland and Northern Ireland are devolved to the Scottish Parliament and Northern Ireland Assembly respectively ([9]).

(8) While the United Kingdom does not have a codified constitution in the sense of an entrenched constitutive document, its constitutional principles have emerged over time, drawn from case-law and convention in particular. The constitutional value of certain statutes, such as Magna Carta, the Bill of Rights 1689 and the Human Rights Act 1998 has been recognised. The fundamental rights of individuals have been developed, as part of the constitution, through common law, the statutes, and international treaties, in particular the European Convention of Human Rights (ECHR), which the United Kingdom ratified in 1951. The United Kingdom also ratified the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108) in 1987 ([10]).

(9) The Human Rights Act 1998 incorporates the rights contained in the ECHR into the law of the United Kingdom. The Act grants any individual the fundamental rights and freedoms provided in Articles 2 to 12 and 14 of the ECHR and Articles 1 to 3 of its First Protocol and Article 1 of its Thirteenth Protocol, as read with Articles 16 to 18 of the ECHR. This includes the right to respect for private and family life, which in turn includes the right to data protection, and the right to a fair trial ([11]). In particular, in accordance with Article 8 of the ECHR, a public authority may only interfere with the right to privacy in accordance with the law, where necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

([8]) Data Protection Act 2018, available at the following link: https://www.legislation.gov.uk/ukpga/2018/12/contents

([9]) UK Explanatory Framework for Adequacy Discussion, section F: Law enforcement, available at the following link: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/872237/F_-_Law_Enforcement_.pdf

([10]) The principles of Convention 108 have originally been implemented into the law of the United Kingdom through the Data Protection Act of 1984, which has been replaced by the DPA 1998, and then in turn by the DPA 2018 (as read with the UK GDPR).The United Kingdom has also signed the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (known as 'Convention 108+') in 2018 and is currently working on the ratification of the Convention.

([11]) Article 6 and 8 of the ECHR (see also Schedule 1 to the Human Rights Act 1998).

(10) In accordance with the Human Rights Act 1998, any action of public authorities must be compatible with a right guaranteed under the ECHR ([12]). In addition, primary and subordinate legislation must be read and given effect in a way, which is compatible with those rights ([13]). As far as an individual considers that his or her rights, including rights to privacy and data protection, have been violated by public authorities, he or she can obtain redress before the United Kingdom courts under the Human Rights Act 1998 and eventually, after exhausting national remedies, he or she can obtain redress before the European Court of Human Rights for violations of the rights guaranteed under the ECHR.

2.2. **The United Kingdom data protection framework**

(11) The United Kingdom withdrew from the Union on 31 January 2020. On the basis of the Agreement on the withdrawal of the United Kingdom of Great Britain and Northern Ireland from the European Union and the European Atomic Energy Community ([14]), Union law continued to apply in the United Kingdom during the transition period until 31 December 2020. Prior to the withdrawal and during the transition period, the legislative framework on the protection of personal data in the United Kingdom governing the processing of personal data by competent authorities 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, consisted of relevant parts of the Data Protection Act 2018, which transposed Directive (EU) 2016/680.

(12) To prepare for the exit from the EU, the Government of the United Kingdom enacted the European Union (Withdrawal) Act 2018 (EUWA) ([15]), which incorporated directly applicable Union legislation into the law of the United Kingdom and provided that so-called 'EU-derived domestic legislation' continues to have effect after the end of the transition period. Part 3 of the DPA 2018 ([16]) transposing Directive (EU) 2016/680 constitutes 'EU-derived domestic legislation' under the EUWA. In accordance with the EUWA, the unmodified 'EU-derived domestic legislation' must be interpreted by the courts of the United Kingdom in accordance with the relevant case-law of the Court of Justice of the European Union (Court of Justice) and general principles of Union law as they had effect immediately before the end of the transition period (referred to as 'retained EU case-law' and 'retained general principles of EU law' respectively) ([17]).

(13) Under the EUWA, the ministers of the United Kingdom have the power to introduce secondary legislation, via statutory instruments, to introduce necessary modifications to retained EU law that result from the United Kingdom's withdrawal from the Union. The Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019 (DPPEC Regulations) ([18]) exercised this power. They amend the United Kingdom data protection legislation, including the DPA 2018, to fit the domestic context ([19]).

([12]) Section 6 of the Human Rights Act 1998.

([13]) Section 3 of the Human Rights Act 1998.

([14]) Agreement on the withdrawal of the United Kingdom of Great Britain and Northern Ireland from the European Union and the European Atomic Energy Community 2019/C 384 I/01, XT/21054/2019/INIT (OJ C 384 I, 12.11.2019, p. 1) ('Withdrawal Agreement' or 'WA'), available at the following link: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:12019W/TXT(02)&from=EN

([15]) European Union Withdrawal Act 2018, available at the following link: https://www.legislation.gov.uk/ukpga/2018/16/contents

([16]) Data Protection Act 2018, available at the following link: https://www.legislation.gov.uk/ukpga/2018/12/contents

([17]) Section 6 of the EUWA 2018.

([18]) The Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019, available at the following link: https://www.legislation.gov.uk/uksi/2019/419/contents/made, as amended by DPPEC 2020, available at the following link: https://www.legislation.gov.uk/ukdsi/2020/9780348213522

([19]) The Exit Regulations make a number of amendments to Part 3 of the DPA 2018. Many of these are technical changes, such as deleting references to 'Member State' or to the 'Law Enforcement Directive' (see for example, Section 48(8) or Section 73(5)(a)) of the DPA 2018 with 'domestic law'), so that Part 3 operates effectively as domestic law after the transition period ends. In some places other types of changes were required, for example, in respect of 'who' adopts 'adequacy decisions' for the purposes of the United Kingdom's data protection legislative framework (see Section 74A of the DPA 2018), i.e. the Secretary of State instead of the European Commission.

(14) Consequently, the legal standards on the processing of personal data by competent authorities 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 in the United Kingdom after the transition period under the Withdrawal Agreement will continue to be set out in relevant parts of the DPA 2018, but as amended by the DPPEC Regulations, in particular in Part 3 of that Act. The United Kingdom General Data Protection Regulation (UK GDPR) does not apply to this type of processing.

(15) Part 3 of the DPA 2018 provides the rules for processing of personal data for criminal law enforcement purposes, including data protection principles, legal grounds of processing (lawfulness), rights of the data subjects, obligations of the competent authorities as controllers and restrictions on onward transfers. At the same time, applicable rules on the oversight, enforcement and redress applicable to the law enforcement sector are provided in Parts 5 and 6 of the DPA 2018.

(16) Moreover, in the light of the relevant role played by the police forces in the law enforcement sector, considerations should be given to the rules governing policing. Policing being a devolved matter, different pieces of legislation that are, however, often similar as to their content are applicable to policing in (a) England and Wales; (b) Scotland; and (c) Northern Ireland ([20]). In addition, various types of guidance documents provides additional clarifications on how the powers of the police should be used. There are three main forms of police guidance: (1) statutory guidance issued under legislation, such as the Code of Ethics ([21]) and the Code of Practice on the Management of Police Information (MoPI Code of Practice) ([22]) issued under the Police Act 1996 ([23]) or PACE codes ([24]) issued under the Police and Criminal Evidence Act ([25]); (2) Authorised Professional Practice on the Management of Police Information (APP Guidance on the Management of Police Information) ([26]), issued by the College of Policing; and (3) operational guidance (published by the police themselves). The National Police Chiefs Council (a coordinating body for all United Kingdom police forces) publishes operational guidance which all police forces have endorsed and which therefore applies nationally ([27]). The aim of this guidance is to ensure consistency between forces in the way information is managed ([28]).

(17) The MoPI Code of Practice was issued by the Secretary of State in 2005, using the powers provided for in Section 39A of the Police Act 1996 ([29]). Any code of practice issued under the Police Act must have the approval of the Secretary of State and is subject to consultation with the National Crime Agency prior to being laid before Parliament. Section 39A (7) of the Police Act requires the police to have due regard to codes issued under the Act

([20]) For a more detailed explanation on the police forces and their powers in the United Kingdom see: UK Explanatory Framework for Adequacy Discussion, section F: Law Enforcement (see footnote 9).

([21]) The Code of Practice for the Principles and Standards of Professional Behaviour for the Policing Profession of England and Wales, available at the following link: https://www.college.police.uk/What-we-do/Ethics/Documents/Code_of_Ethics.pdf; the Police Service Northern Ireland Code of Ethic, available at the following link: https://www.nipolicingboard.org.uk/psni-code-ethics; the Code of Ethic for policing in Scotland, available at the following link: https://www.scotland.police.uk/about-us/code-of-ethics-for-policing-in-scotland/

([22]) Code of Practice on the Management of Police Information, available at the following link: http://library.college.police.uk/docs/APPref/Management-of-Police-Information.pdf

([23]) Police Act 1996, available at the following link: https://www.legislation.gov.uk/ukpga/1996/16/contents

([24]) Police and Criminal Evidence Act 1984 (PACE) codes of practice available at the following link: https://www.gov.uk/guidance/police-and-criminal-evidence-act-1984-pace-codes-of-practice

([25]) Police and Criminal Evidence Act 1984, available at the following link: https://www.legislation.gov.uk/ukpga/1984/60/contents

([26]) Authorised Professional Practice on the Management of Police Information, available at the following link: https://www.app.college.police.uk/app-content/information-management/management-of-police-information/

([27]) Data Protection Manual for Police Data Protection Professionals, available at the following link: https://www.npcc.police.uk/2019%20FOI/IMORCC/225%2019%20NPCC%20DP%20Manual%20Draft%200.11%20Mar%202019.pdf

([28]) For example, the MoPI Code of Practice (see footnote 22) applies to the retention of operational policing information (see recital 47 of this decision).

([29]) According to the information provided by the United Kingdom authorities, during the period of the adequacy talks, the College of Policing was in the process of drafting an Information and Records Management Code of Practice to replace the MoPI. The draft code was published for public consultation on 25 January 2021 and is available at following link: https://www.college.police.uk/article/information-records-management-consultation

hence the police is expected to comply with it ([30]). Moreover, non-statutory guidance (such as the APP Guidance on the Management of Police Information) must always be consistent with the MoPI Code of Practice which sits above it ([31]).In any case, while there might be certain operational situations when police officers need to deviate from this guidance, they are still required to comply with the requirements of Part 3 of the DPA 2018 ([32]).

(18) Further guidance on the data protection legislation of the United Kingdom for processing in the law enforcement sector is provided by the Information Commissioner ('Information Commissioner' or 'ICO') ([33]) (for further details on the ICO see recitals 93 to 109). Although not legally binding, in a court case, the courts would be bound to take into consideration any breach of the guidance, as it carries interpretative weight and demonstrates how the data protection legislation is interpreted and enforced by the Commissioner in practice ([34]).

(19) Finally, as mentioned in recitals 8 to 10, the United Kingdom law enforcement agencies must ensure compliance with the (ECHR) and Convention 108.

(20) In its structure and main components, the legal framework governing the processing of data by United Kingdom criminal law enforcement authorities is thus very similar to the one applying in the EU. This includes the fact that such framework does not only rely on obligations laid down in domestic law, that have been shaped by EU law, but also on obligations enshrined in international law, in particular through the United Kingdom adherence to the ECHR and Convention 108, as well as its submission to the jurisdiction of the European Court of Human Rights. These obligations arising from legally binding international instruments, concerning notably the protection of personal data, are therefore a particular important element of the legal framework assessed in this Decision.

2.3. **Material and territorial scope**

(21) The material scope of Part 3 of the DPA 2018 coincides with the scope of Directive (EU) 2016/680 as specified in Article 2(2) thereof. Part 3 applies to the processing by a competent authority of personal data wholly or partly by automated means and the processing by a competent authority otherwise than by automated means of personal data which forms part of a filing system or is intended to form part of a filing system.

(22) Moreover, in order to fall under the scope of that Part 3, the controller must be a 'competent authority' and the processing must be carried out for a 'law enforcement purpose'. Therefore, the data protection regime that is assessed in this Decision applies to all the law enforcement activities of these competent authorities.

(23) The concept of 'competent authority' is defined in Section 30 of the DPA as a person listed in Schedule 7 to the DPA 2018 as well as any other person to the extent that the person has statutory functions for any of the law enforcement purposes. Competent authorities listed in Schedule 7 include not only police forces, but also all United Kingdom ministerial government departments as well as other authorities with investigatory functions (e.g. the Commissioner for Her Majesty's Revenue and Customs, the Welsh Revenue Authority, the Competition and Markets Authority, Her Majesty's Land Register or the National Crime Agency), prosecutorial agencies, other criminal justice

([30]) In case *R v the Commission of Police of the Metropolis* [2014] EWCA Civ 585, the legal status of the MoPI Code of Practice was confirmed and Lord Justice Laws declared that the Metropolitan Police Commissioner is obliged to have regard to the MoPI Code of Practice and the APP Guidance on Management of Police Information pursuant to Section 39A of the Police Act 1996.

([31]) The police is inspected as to its compliance with the MoPI Code of Practice by Her Majesty's Inspectorate of Constabulary and Fire & Rescue Services (HMICFRS).

([32]) See in this respect, the College of Policing's position on compliance with APP's guidance on all elements of policing, that explains that 'APP is authorised by the professional body for policing (the College of Policing) as the official source of professional practice on policing. Police officers and staff are expected to have regard to APP in discharging their responsibilities. There may be circumstances, however, where there is a legitimate operational reason for a Force to deviate from APP, providing there is a clear rationale for doing so. It would be for the Force to bear the responsibility of any local and national risk of operating outside nationally agreed guidelines, and if an incident or investigation occurs as a consequence (such as through the Independent Office of Police Conduct) the Force is liable for any risk.', available at the following link: https://www.app.college.police.uk/faq-page/

([33]) Guide to Law Enforcement Processing, available at the following link: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/

([34]) See case *Bridges v the Chief Constable of South Wales Police* [2019] EWHC 2341 (Admin) where although noting the non-statutory nature of the Commissioner's guidance, the High Court stated that '[w]hen considering whether or not a data controller has complied with the section 64 obligation [to carry out a Data Protection Impact Assessment in relation to high risk processing], a Court will have regard to the guidance that has been issued by the Information Commissioner in respect of Data Protection Impact Assessments'.

agencies and other holders or organisations who carry out law enforcement activities ([35]). Part 3 of the DPA 2018 also applies to courts and tribunals when they exercise their judicial functions, except for the part related to data subject's rights and ICO oversight ([36]). The list of competent authorities provided by Schedule 7 is not definitive and may be updated by the Secretary of State by Regulations taking into account the changes in the organisation of the public offices ([37]).

(24) The processing in question must also be for a 'law enforcement purpose', defined as 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 ([38]). Processing by a competent authority is not governed by Part 3 of the DPA 2018 where it does not occur for law enforcement purposes. This will be the case, for example, when the Competition and Markets Authority investigates cases that are not criminalised (e.g. mergers between companies). In that case, the UK GDPR, together with Part 2 of the DPA 2018, will apply as the processing of personal data by competent authorities is carried out for purposes other than law enforcement purposes. To determine which data protection regime applies (Part 3 or Part 2 of the DPA 2018) to the processing of personal data in question, the competent authority, i.e. the controller, must consider whether the 'primary purpose' of such processing is one of the law enforcement purposes under the DPA 2018.

(25) As for the territorial scope of Part 3 of the DPA 2018, Section 207(2) provides that the DPA applies to the processing of personal data in the context of the activities of a person who has an establishment in the entire United Kingdom territory. This includes public authorities of territories of England, Wales, Scotland and Northern Ireland which fall under the material scope of Part 3 of the DPA 2018 ([39]).

2.3.1. *Definition of personal data and processing*

(26) The key concepts of personal data and processing are defined in Section 3 of the DPA 2018 and apply throughout the DPA. The definitions closely follow the corresponding definitions set out in Article 3 of Directive (EU) 2016/680. Under the DPA 2018, personal data means any information relating to an identified or identifiable living individual ([40]). Under Section 3(3) of the DPA 2018 an individual is identifiable if he or she can be directly or indirectly identified from the information, including by reference to a name or an identifier or by reference to one or more factors specific to the person's physical, physiological, genetic, mental, economic, cultural or social identity. The notion of 'processing' is defined as an operation or set of operations which is performed on information, or on sets of information, such as (a) collection, recording, organisation, structuring or storage; (b) adaptation or alteration; (c) retrieval, consultation or use; (d) disclosure by transmission, dissemination or otherwise making available; (e) alignment or combination; or (f) restriction, erasure or destruction. Moreover, the Act defines 'sensitive processing' as '(a) the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership; (b) the processing of genetic data, or of biometric data, for the purpose of uniquely identifying an individual; (c) the processing of data concerning health; (d) the processing of data concerning an individual's sex life or sexual orientation' ([41]). In this respect, Section 205 of the DPA 2018 provides the definition of 'biometric data' ([42]), 'data concerning health' ([43]) and 'genetic data' ([44]).

([35]) Among those, Schedule 7 of the DPA 2018 lists the Directors of Public Prosecutors, the Director of Public Prosecutors for Northern Ireland or the Information Commission.

([36]) Section 43(3) of the DPA 2018.

([37]) Section 30(3) of the DPA 2018. The intelligence services (Secret Intelligence Service, Security Service and the Government Communications Headquarters) are not competent authorities (see Section 30(2) of the DPA 2018) and Part 3 of the DPA 2018 does not apply to any of their activities. Their activities fall under the scope of Part 4 of the DPA 2018.

([38]) Section 31 of the DPA 2018.

([39]) This means that the DPA 2018 and therefore this decision do not apply to UK Crown dependencies and the other United Kingdom Overseas Territories, such as for example the Falkland Islands and the territory of Gibraltar.

([40]) Personal data related to deceased persons do not fall into the scope of the DPA 2018.

([41]) Section 35(8) of the DPA 2018.

([42]) 'Biometric data' means personal data resulting from specific technical processing relating to the physical, physiological or behavioral characteristics of an individual, which allows or confirms the unique identification of that individual, such as facial images or dactyloscopic data.

([43]) 'Data concerning health' means personal data relating to the physical or mental health of an individual, including the provision of health care services, which reveals information about his or her health status.

([44]) 'Genetic data' means personal data relating to the inherited or acquired genetic characteristics of an individual which gives unique information about the physiology or the health of that individual and which results, in particular, from an analysis of a biological sample from the individual in question.

(27) Section 32 of the DPA 2018 clarifies the definitions of 'controller' and 'processor' in the context of processing of personal data for law enforcement purposes closely following the equivalent definitions in Directive (EU) 2016/680. The controller means the competent authority, which determines the purposes and means of the processing of personal data. Where the processing is required by law, the controller is the competent authority on which such an obligation is imposed by that law. A processor is defined as any person who processes personal data on behalf of the controller (other than a person who is an employee of the controller).

2.4. **Safeguards, rights and obligations**

2.4.1. *Lawfulness and fairness of processing*

(28) Pursuant to Section 35 of the DPA 2018, the processing of personal data must be lawful and fair, in a manner similar to Article 4(1)(a) of Directive (EU) 2016/680. In accordance with Section 35(2) of the DPA 2018, the processing of personal data for any of the law enforcement purposes is lawful only if 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.

2.4.1.1. Processing on the basis of the law

(29) Similarly to Article 8 of Directive (EU) 2016/680, in order to ensure the lawfulness of a processing falling under Part 3 of the DPA 2018, such processing must be 'based on law'. 'Lawful' processing means authorised by either statute, common law or royal prerogatives ([45]).

(30) The powers of competent authorities are in general governed by statutes, meaning that their functions and powers are set out clearly in legislations adopted by the Parliament ([46]). In certain cases, the police as well as other competent authorities listed under Schedule 7 of the DPA 2018 can rely on common law to process data ([47]). Common law has built up through precedents set by decisions of the courts. The common law is relevant in the context of powers available to the police that derives from this source of law its core duty to protect the public by detecting and preventing crime ([48]). The police forces

([45]) Explanatory Notes to the DPA 2018, paragraph 181, available at the following link: https://www.legislation.gov.uk/ukpga/2018/12/pdfs/ukpgaen_20180012_en.pdf.

([46]) The National Crime Agency, for example, derives its powers from the Crime and Courts Act 2013, available at the following link: https://www.legislation.gov.uk/ukpga/2013/22/contents. Similarly, the Food Standards Agency's powers are provided for by the Food Standards Act 1999, available at the following link: https://www.legislation.gov.uk/ukpga/1999/28/contents. Other examples include the Prosecution of Offenders Act 1985, which created the Crown Prosecution Service (see https://www.legislation.gov.uk/ukpga/1985/23/contents); the Commissioners for Revenue and Customs Act 2005 which established Her Majesty's Revenue and Customs (see https://www.legislation.gov.uk/ukpga/2005/11/contents); the Criminal Procedure (Scotland) Act 1995, which created the Scottish Criminal Cases Review Commission (see https://www.legislation.gov.uk/ukpga/1995/46/contents); the Justice (Northern Ireland) Act 2002, which established the Public Prosecution Service in Northern Ireland (see https://www.legislation.gov.uk/ukpga/2002/26/contents) and the Serious Fraud Office was created and given its powers under the Criminal Justice Act 1987 (see https://www.legislation.gov.uk/ukpga/1987/38/contents).

([47]) For example, according to the information provided by the United Kingdom authorities, within the Crown Office and Procurator Fiscal Service, responsible for prosecuting cases in Scotland, the Lord Advocate, who is the head of the system of prosecution in Scotland, derives his powers to investigate deaths and prosecute offences from common law, whilst some of his function are established in statute. Moreover, the Crown and, by extension various government, departments and Ministers, also derive their powers from a combination of legislation, common law and the royal prerogative (these are common law powers vested in the Crown but which are exercised by Ministers).

([48]) UK Explanatory Framework for adequacy Discussion, section F: Law Enforcement, page 8 (see footnote 9).

have, however, both common law and legislative powers ([49]) to execute such a duty. Where the police have a statutory power, this supersedes any common law power ([50]).

(31) The breadth of the police officer's common law powers and obligations has been recognised by the courts to include 'all steps which appear to him necessary for keeping the peace, for preventing crime or for protecting property from criminal injury' ([51]). Common law powers are not unqualified powers. They are subject to a range of limitations, including limits established by the courts ([52]) and by legislation, in particular, the Human Rights Act 1998 and the Equality Act 2010 ([53]). Moreover, for competent authorities processing data under Part 3 of the DPA 2018, this includes exercising common law powers consistently with the requirements set out in the DPA 2018 ([54]). Furthermore, a decision to perform any sort of data processing must consider the requirements of applicable guidance, such as the MoPI Code of Practice as well as guidance specific to one of the United Kingdom countries ([55]). A number of guidance documents are issued by the government and operational policing to ensure police officers exercise processing their powers within the limits set by common law or the relevant statute ([56]).

(32) Royal prerogatives represent another component of the 'law' and refer to certain powers vested in the Crown and exercisable by the executive that are not based on statute, but derive from the sovereignty of the monarch ([57]). There are very few examples of prerogative powers being relevant in the law enforcement context. They include, for example, the mutual legal assistance framework enabling the sharing of data by a Secretary of State with third

([49]) The key pieces of legislation providing the regime on the main police powers (arrest, searches, authorisation of continued detention, finger printing, taking of intimate samples, warrant interception, access to communication data) are: (i), for England and Wales, the Police and Criminal Evidence Act 1984 (PACE), available at the following link: https://www.legislation.gov.uk/ukpga/1984/60/contents (as amended by the Protection of Freedoms Act 2012 (PoFA), available at the following link: https://www.legislation.gov.uk/ukpga/2012/9/contents) and the Investigatory Powers Act 2016 (IPA), available at the following link: https://www.legislation.gov.uk/ukpga/2016/25/contents); (ii) for Scotland, the Criminal Justice (Scotland) Act 2016, available at the following link: https://www.legislation.gov.uk/asp/2016/1/contents and the Criminal Procedure (Scotland) Act 1995, available at the following link: https://www.legislation.gov.uk/ukpga/1995/46/contents); (iii) for Northern Ireland, the Police and Criminal Evidence (Northern Ireland) Order 1989, available at the following link: https://www.legislation.gov.uk/nisi/1989/1341/contents.

([50]) The United Kingdom authorities have explained that the supremacy of statutory law is a long established in the United Kingdom, as far back as the judgment in *Entick v Carrington* [1765] EWHC KB J98, which recognised that there were limits on the exercise of powers by the executive and established the principle that common law powers and prerogative powers of the monarch and government are subordinate to the law of the land.

([51]) See case *Rice v Connolly* [1966] 2 QB 414.

([52]) See case *R(Catt) v Association of Chief police Officers* [2015] AC 1065, where in relation to the police power's to obtain and hold the information of an individual (who had committed a crime), Lord Sumption held that 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. The judge considered that, in this case, common law powers were amply sufficient to authorise the obtaining and storage of the kind of public information in question on these appeals.

([53]) Equality Act 2010, available at the following link: https://www.legislation.gov.uk/ukpga/2010/15/contents

([54]) For an example of a case where police common law powers are assessed under the framework of the DPA 1998, see the decision of the High Court in *Bridges v the Chief Constable of South Wales Police* (see footnote 33). See also cases *Vidal-Hall v Google Inc* [2015] EWCA Civ 311 and *Richard v BBC* [2018] EWHC 1837 (Ch).

([55]) See for example the guidance of the Police Service of Northern Ireland on records management service instruction, available at the following link: https://www.psni.police.uk/globalassets/advice–information/our-publications/policies-and-service-procedures/records-management-080819.pdf

([56]) The House of Commons has published a briefing document which sets out the key common law and statutory powers of the police in England and Wales (see https://researchbriefings.files.uk/documents/CBP-8637/CBP-8637.pdf). According to this document, for example, while the powers of maintaining 'the Crown's peace' is common law derived power as well as 'the use of force', 'the stop and search powers' are always derived from Statute. Moreover, the Scottish Government provides information on its website on the police powers of arrest and stop search (see https://www.gov.scot/policies/police/police-powers/).

([57]) According to the information provided by the United Kingdom authorities, prerogative powers exercised by the government include, for example, the making and ratification of treaties, the conduct of diplomacy, the use of the armed forces within the United Kingdom to maintain the peace in support of the police.

countries for law enforcement purposes and the power to share data in this way is not always set out in statute ([58]). Royal prerogatives are bound by common law principles ([59]) and are subordinate to statute, therefore subject to the limits provided by the Human Rights Act 1998 and the DPA 2018 ([60]).

(33) Similarly to Article 8 of Directive (EU) 2016/680, the United Kingdom regime requires that in order to comply with the principle of lawfulness, competent authorities should ensure that, when the processing is based on the law, it must also be 'necessary' to perform the task carried out for the law enforcement purpose. The ICO gives guidance in this respect clarifying that 'it must be a targeted and proportionate way of achieving the purpose. The lawful basis will not apply if you can reasonably achieve the purpose by some other less intrusive means. It is not enough to argue that processing is necessary because you have chosen to operate your business in a particular way. The question is whether the processing is necessary for the stated purpose' ([61]).

2.4.1.2. Processing on the basis of the 'consent' of the data subject

(34) As mentioned in recital 28, Section 35(2) of the DPA 2018 provides for the possibility to process personal data on the basis of the 'consent' of the individual.

(35) However, consent does not appear to be a legal basis relevant for the processing operations falling within the scope of the present decision. In fact, the processing operations covered by the present decision will always concern data that has been transferred under Directive (EU) 2016/680 by a competent authority of a Member State to a United Kingdom competent authority. Therefore, they will typically not involve the type of direct interaction (collection) between a public authority and data subjects that can be based on consent under Section 35(2)(a) of the DPA 2018.

(36) While reliance on consent is thus not considered relevant for the assessment carried out under this Decision, it is worth noting, for sake of completeness, that in a law enforcement context processing is never based solely on consent as a competent authority must always have an underlying power that enables it to process the data ([62]). More specifically, and similarly to what is allowed under Directive (EU) 2016/680 ([63]), this means that consent serves as an additional condition to enable certain limited and specific processing operations that could otherwise not be carried out, for example the collection and processing of a DNA sample of an individual who is not a suspect. In this case, the processing would not be carried out if the consent is not given or is withdrawn ([64]).

([58]) In this respect, see the assessment of the United Kingdom onward transfer regime in recitals 74–87.

([59]) See case *Bancoult v Secretary of State for Foreign and Commonwealth Affairs* [2008] UKHL 61 whereby the courts held that the prerogative power to make Orders in Council was also subject to the ordinary grounds of judicial review.

([60]) See case *Attorney-General v De Keyser's Royal Hotel Ltd* [1920] AC 508 where the court held that prerogative powers cannot be used when statutory powers replace them; case *Laker Airways Ltd v Department of Trade* [1977] QB 643, where the court found that prerogative powers cannot be used in order to frustrate statutory law; case *R v Secretary of State for the Home Department, ex p. Fire Brigades Union* [1995] UKHL 3 where court held that prerogative powers cannot be used where they conflict with enacted legislation, even when that enacted legislation is not yet in force; case *R (Miller) v Secretary of State for Exiting the European Union* [2017] UKSC 5 where the court confirmed the ability for statute law to adjust and abolish prerogative powers. For a general overview of the relationship between the Royal prerogatives and the statute or the Common law powers, see the briefing paper of the House of Commons, available at the following link: https://researchbriefings.files.parliament.uk/documents/SN03861/SN03861.pdf

([61]) Guide to Law Enforcement Processing, 'What is the first principle about?' available at the following link: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/principles/#ib2

([62]) This follows from the language of the relevant provision of the DPA 2018, according which the processing of personal data for any of the law enforcement purposes is lawful only if and to the extent that 'it is based on law' and either (a) the data subject has given consent to the processing for that purpose; or (b) the processing is necessary for the performance of a task carried out for that purpose by a competent authority'.

([63]) See recitals 35 and 37 of Directive (EU) 2016/680.

([64]) The United Kingdom authorities have explained that one example of when consent may be an appropriate basis for processing would be where the police obtains a DNA sample in relation to a missing person to match against a body if one is found. Under such circumstances, it would be inappropriate for the police to compel the data subject to provide a sample; instead, the police would ask for the individual's consent, which is freely given and can be withdrawn at any point. If consent is withdrawn, the data could no longer be processed, unless a new legal basis was established to continue to process the sample (e.g. the data subject became a suspect). A further example could arise when a police force investigates a crime in which a victim (it could be a victim of a robbery, sexual offence, domestic violence, relatives of a homicide or other victim of a crime) could benefit from a referral to Victim Support (an independent charity dedicated to supporting people affected by crime and traumatic incidents). In such circumstances, the police will only share the personal information such as the name and contact details with Victim Support if they have the consent of the victim.

(37) In cases requiring the consent of the individual, such consent must be unambiguous and involve a clear affirmative action ([65]). Police forces are required to have a privacy notice including, among others, the necessary information related to the valid use of consent. In addition, some of them publish additional material on how they comply with data protection legislation, including how and when they would use consent as a legal basis ([66]).

2.4.1.3. Sensitive processing

(38) Specific safeguards should exist where 'special categories' of data are being processed. In this respect, similarly to what is provided by Article 10 of Directive (EU) 2016/680, Part 3 of the DPA 2018 provides stronger safeguards for so-called 'sensitive processing' ([67]).

(39) According to Section 35(3) of the DPA 1998, sensitive data can be processed by competent authorities for law enforcement purposes only in two cases: (1) the data subject has given consent to the processing for the law enforcement purpose and at the time when the processing is carried out, the controller has an appropriate policy document in place ([68]); or (2) the processing is strictly necessary for the law enforcement purpose, the processing meets at least one of the conditions in Schedule 8 to the DPA 2018, and at the time when the processing is carried out, the controller has an appropriate policy document in place ([69]).

(40) As regards the first case and as explained in recital 38, reliance on consent is not considered relevant in the type of transfer situation subject to the present this Decision ([70]).

(41) When the processing of sensitive data does not rely on consent, it can be carried out using one of the conditions listed in Schedule 8 to the DPA 2018. These conditions relate to processing necessary for statutory purposes; the administration of justice; the protection of the vital interests of the data subject or of another individual; the safeguarding of children and of individuals at risk; legal claims; judicial acts; preventing fraud; archiving; where personal data is manifestly made public by the data subject. Apart from the case when the data is manifestly made public, all of the conditions provided by Schedule 8 are subject to a 'strict necessity' test. As clarified by the ICO, 'strictly necessary in this context means that the processing has to relate to a pressing social need, and you cannot

([65]) There is no separate definition of 'consent' for the purposes of processing personal data under Part 3 of the DPA 2018. The ICO provided guidance on the notion of 'consent' under Part 3 of DPA 2018, clarifying that it has the same meaning and should be aligned with the definition provided by the GDPR, notably that 'consent must be freely given, specific and informed and there must be a genuine choice about agreeing to the data being processed' (Guide to Law Enforcement Processing, 'What is the first principle about?' (see footnote 64) and Guide to Data Protection on consent, available at the following link: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/consent/).

([66]) See, for example, the information at the webpage of the Lincolnshire police (see https://www.lincs.police.uk/resource-library/data-protection/law-enforcement-processing/) or at the webpage of the West Yorkshire Police (see https://www.westyorkshire.police.uk/sites/default/files/2018-06/data_protection.pdf).

([67]) Section 35(8) of the DPA 2018.

([68]) Section 35(4) of the DPA 2018.

([69]) Section 35(5) of the DPA 2018.

([70]) For sake of completeness, it is worth noting that, when processing is based on consent, it must be freely given, specific and informed and there must be a specific choice about agreeing to the data being processed. In addition, the controller, when processing on the basis of the consent of the data subject, is required to have in place an 'appropriate policy document' (APD). Section 42 of the DPA 2018 outlines the requirements that the APD must fulfil. It makes clear that the document must, as a minimum, explain the controller's procedures for securing compliance with the data protection principles and explain the controller's policies as regards the retention and erasure of personal data. According to Section 42 of the DPA 2018, this means that the controller must produce a document which (a) explains the controller's procedures for securing compliance with the data protection principles; and (b) explains the controller's policies as regards the retention and erasure of personal data processed in reliance on the consent of the data subject or giving an indication of how long such personal data is likely to be retained. In particular, the Policy Document requires that the controller, in respecting his duty of recording the processing activities, should always include the elements mentioned in points (a) and (b). The ICO has published a template document (Guide to Law Enforcement Processing. 'Conditions for sensitive processing', available at the following link: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/conditions-for-sensitive-processing) and can take enforcement action if the controllers fail to meet these requirements. The APD is also examined by courts when considering potential breaches of the DPA 2018. For example, in the recent case of *R (Bridges) v Chief Constable of South Wales Police*, the courts reviewed the controller's APD and found that it was adequate but would have benefitted from further detail. As a result, the South Wales Police reviewed the APD and updated it in line with the new ICO guidance (see footnote 33). Furthermore, pursuant to Section 42(3) of the DPA 2018, the APD should be kept under a regular review by the controller. Finally, as an additional safeguard, pursuant to Section 42(4) of the DPA 2018, the controller is required to keep an augmented record of processing activities, including additional elements when compared to the general obligation that falls on the controller to keep records over the processing activities set out in Section 61 DPA 2018.

reasonably achieve it through less intrusive means' ([71]). Moreover, some of the conditions are subject to additional restrictions. For example, to rely on the 'statutory purposes' condition and the 'safeguarding condition' (Schedule 8, paragraph 1 and paragraph 4) there is an additional substantial public interest test to be fulfilled. Moreover, in relation to the conditions regarding the safeguard of the child (Schedule 8, paragraph 4) the data subject must also be of a specific age and considered at risk. Moreover, the controller can only apply the condition provided in paragraph 4 of Schedule 8 in case of specific circumstances ([72]). Similarly, there are restrictions for the 'judicial acts' and 'preventing fraud' conditions (Schedule 8, paragraphs 7 and 8 respectively). Both are only applicable to specific controllers. In the case of judicial acts, only a court or another judicial authority may use such a condition and, in the case of fraud prevention, only controllers who are anti-fraud organisations are able to rely on this condition.

(42) Finally, when the processing relies on one of the conditions listed in Schedule 8 and pursuant respectively to Section 42 DPA 2018, an 'appropriate policy document' must be in place – explaining the controller's procedures for securing compliance with the data protection principles and the controller's policies as regards the retention and erasure of personal data – and augmented record obligations apply.

2.4.2. *Purpose limitation*

(43) Personal data should be processed for a specific purpose and subsequently used only insofar as this is not incompatible with the purpose of processing. This data protection principle is guaranteed by Section 36 of the DPA 2018. This provision, similarly to Article 4(1)(b) of Directive (EU) 2016/680, requires that (a) the law enforcement purpose for which personal data is collected on any occasion must be specified, explicit and legitimate; and (b) personal data so collected must not be processed in a manner that is incompatible with the purpose for which it was collected.

(44) Where competent authorities process data for a law enforcement purpose, this may include archiving, scientific or historical research and statistical purposes ([73]). In these cases, the DPA 2018 also clarifies that archiving (or processing for scientific or historical research and statistical purposes) is not permitted where it is carried out with respect to decisions made in relation to a particular data subject or if it is likely to cause him or her substantial damage or distress ([74]).

2.4.3. *Accuracy and data minimisation*

(45) Data must be accurate and, where necessary, kept up to date. It must also be adequate, relevant and not excessive in relation to the purposes for which it is processed. Similarly to Article 4(1)(c), (d) and (e)) of Directive (EU) 2016/680, these principles are ensured in Sections 37 and 38 of the DPA 2018. Every reasonable step must be taken to ensure that personal data that is inaccurate ([75]) is erased or rectified without

([71]) Guide to Law Enforcement Processing, 'Conditions for sensitive processing' (see footnote 70).

([72]) The processing is carried out without the consent of the data subject when: (a) consent to the processing cannot be given by the data subject; (b) the controller cannot reasonably be expected to obtain the consent of the data subject to the processing; (c) the processing must be carried out without the consent of the data subject because obtaining the consent of the data subject would prejudice the provision of the protection mentioned in subparagraph (1)(a).

([73]) See Section 41(1) of DPA 2018.

([74]) See Section 41(2) of DPA 2018.

([75]) Section 205 of the DPA 2018 defines the term 'inaccurate' as 'incorrect or misleading' personal data. The United Kingdom authorities have explained it being typical that data related to criminal investigations will often be incomplete, but regardless of that, can be accurate.

delay ([76]), having regard to the law enforcement purpose for which it is processed ([77]), and to ensure that personal data which is inaccurate, incomplete or no longer up to date is not transmitted or made available for any of the law enforcement purposes ([78]).

(46) Furthermore, similarly to Article 7 of Directive (EU) 2016/680, the United Kingdom data protection regime specifies that personal data based on facts must, so far as possible, be distinguished from personal data based on personal assessments ([79]). Where relevant and as far as possible, a clear distinction must be made between personal data relating to different categories of data subjects, such as suspects, persons convicted of a criminal offence, victims of a criminal offence and witnesses ([80]).

2.4.4. *Storage limitation*

(47) Pursuant to Article 5 of Directive (EU) 2016/680, data should, in principle, be kept for no longer than is necessary for the purposes for which the personal data is processed. According to Section 39 of the DPA 2018 and similarly to Article 5 of that Directive, it is prohibited to keep personal data processed for any of the law enforcement purposes for longer than is necessary in relation to the purpose for which it is processed. The United Kingdom legal regime 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. Further rules on practices related to retention of personal data and the applicable time limits have been set out in the relevant legislation and guidance governing the powers and functioning of the police. For example, in England and Wales the College of Policing's MoPI Code of Practice, together with the APP Guidance on the Management of Police Information, provides a framework to ensure a consistent risk based retention, review and disposal process for the management of operational policing information ([81]). This framework sets clear expectations across the service as to how information should be created, shared, used and managed within and between individual police forces and other agencies ([82]). The police are expected to comply with the Code of Practice and compliance is verified by Her Majesty's Inspectorate of Constabulary and Fire & Rescue Services ([83]).

(48) The Police Service of Northern Ireland (PSNI) is not required by law to follow the MoPI Code of Practice. However, the MoPI framework adopted in 2011 is supplemented by a PSNI Handbook ([84]), which sets out policies and procedures on the way in which the MoPI Code of Practice is applied in Northern Ireland.

([76]) Section 38(1)(b) of the DPA 2018.

([77]) According to UK Explanatory Framework for Adequacy Discussion, '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' (see UK Explanatory Framework for Adequacy Discussions, section F: Law Enforcement, page 21, see footnote 9).

([78]) Section 38(4) of the DPA 2018. Moreover, under Section 38(5) of the DPA 2018 the quality of personal data must be verified before it is transmitted or made available, in all transmissions of personal data, the necessary information enabling the recipient to assess the degree of accuracy, completeness and reliability of the data and the extent to which it is up to date must be included, and if, after personal data has been transmitted, it emerges that the data was incorrect or that the transmission was unlawful, the recipient must be notified without delay.

([79]) Section 38(2) of the DPA 2018.

([80]) Section 38(3) of the DPA 2018.

([81]) This framework ensures consistency in the application of the storage of the personal data acquired. The review period depends on the offences which are divided in 4 groups: (1) certain public protection matters; (2) other sexual violent and serious offences; (3) all other offences; (4) miscellaneous. More details are available at the APP Guidance on the Management of Police Information (see footnote 26).

([82]) According to the information provided by the United Kingdom authorities, other organisations are free to follow the MoPI Code of Practice principles if they wish, for example, Her Majesty's Revenue and Customs and the National Crime Agency voluntarily adopt many of the MoPI Code of Practice principles to ensure consistency across law enforcement. In general, most organisations will provide their staff with specific policies and guidance for all staff on how to handle personal data as part of their role and tailored to the specific organisation. This would usually include mandatory training as well.

([83]) The MoPI Code of Practice was issued using powers provided under the Police Act 1996, which enables the College of Policing to issue codes of practice, relating to the effective functioning of policing. Any code of practice made under the Act must have approval of the Secretary of State and is subject to consultation with the National Crime Agency prior to being laid in Parliament. Section 39A(7) of the Police Act 1996 requires the police to have due regard to Codes issued under the Police Act 1996.

([84]) PSNI MoPI Handbook Chapter 1-6.

(49) In Scotland, the Police forces rely on the Record Retention Standard Operating Procedure (SOP) ([85]) which supports the Police Service of Scotland Records Management Policy ([86]). The SOP sets specific retention rules for the records held by Police Scotland.

(50) In addition to the overarching requirement to review records which applies across the whole of the United Kingdom, further detail is provided in localised rules. To give a few examples, with respect to England and Wales, the Police and Criminal Evidence Act, as amended by the Protection of Freedom Act 2012 (PoFA), makes provision for the retention of fingerprints and DNA profiles as well as a specific regime for individuals not convicted ([87]). The PoFA also created the position of Commissioner for the Retention and Use of Biometric Material ('the Biometrics Commissioner') ([88]). Specific rules on custody images are set out in the 2017 Custody Image Review ([89]). Concerning Scotland, the Criminal Procedure (Scotland) Act 1995 provides the rules for the obtaining and retention of fingerprint and biological samples ([90]). As in the case of England and Wales, the legislation regulates the retention of biometric data in different cases ([91]).

2.4.5. *Data security*

(51) Personal data must be processed in a manner that ensures their security, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage. To that end, public authorities are to take appropriate technical or organisational measures to protect personal data from possible threats. These measures must be assessed taking into consideration the state of the art and related costs.

(52) These principles are reflected in Section 40 of the DPA 2018 according to which, similarly to Article 4(1)(f) of Directive (EU) 2016/680, personal data processed for any of the law enforcement purposes must be processed in a manner that ensures appropriate security of the personal data, using appropriate technical or organisational measures. This includes protecting the data against unauthorised or unlawful processing and against accidental loss,

([85]) Record Retention Standard Operating Procedure (SOP), available at the following link: https://www.scotland.police.uk/spa-media/nhobty5i/record-retention-sop.pdf

([86]) For more details on record management, see information related to the National Records of Scotland, available at the following link: https://www.nrscotland.gov.uk/record-keeping/records-management.

([87]) The retention periods varies depending on whether or not an individual has been convicted (Sections 63I–63KI of the PACE 1984). For example in the case of an adult convicted of a recordable offence his or her fingerprints and DNA profile may be retained indefinitely (Section 63I(2) of the PACE 1984), while the retention is limited in time if the convicted person is under 18, the offence is a 'minor' recordable offence and the person has not been convicted before (Section 63K of the PACE 1984). Retention in the case of a person arrested or charged but not convicted is limited in time to three years (Section 63F of the PACE 1984). Extension of this retention period has to be approved by judicial authority (Section 63F(7) of the PACE 1984). In case of people arrested or charged but not convicted for minor offence, it is not possible to retain (Section 63D and Section 63H of the PACE 1984).

([88]) Section 20 of the PoFA 2012 creates the position of the Biometrics Commissioner. Among others functions, the Biometrics Commissioner decides whether or not the police may retain DNA profile records and fingerprints obtained from individuals arrested but not charged with a qualifying offence (Section 63G of the PACE 1984). Moreover, the Biometrics Commissioner has a general responsibility to keep the retention and use of DNA and fingerprints, and retention on national security grounds, under review (Section 20(2) of the POFA 2012). The Biometric Commissioner is appointed under the Code for Public Appointments (the Code is available at the following link: Governance Code for Public Appointments - GOV.UK (www.gov.uk)) and his terms of appointment make it clear that he may only be removed from office by the Home Secretary under a narrowly defined set of circumstances; these include a failure to carry out his duties for a period of three months, conviction for a criminal offence or a failure to comply with the terms of his appointment.

([89]) Review of the Use and Retention of Custody Images, available at the following link: https://www.gov.uk/government/publications/custody-images-review-of-their-use-and-retention

([90]) Sections 18 and following of Criminal Procedure (Scotland) Act 1995.

([91]) The retention periods vary according to whether the person has been convicted (Section 18(3) of the Criminal Procedure (Scotland) Act 1995) or whether he or she is underage. In this latter case, the retention period is 3 years from the conviction in the children's hearing (Section 18E(8) of the Criminal Procedure (Scotland) Act 1995). Data of people arrested but not convicted cannot be retained (Section 18(3) of the Criminal Procedure (Scotland) Act 1995) except in specific cases and depending on the gravity of the crime (Sections 18A of the Criminal Procedure (Scotland) Act 1995). The Scottish Biometrics Commissioner Act 2020 (see https://www.legislation.gov.uk/asp/2020/8/contents) creates the position of the Scottish Biometrics Commissioner who must prepare and revise codes of practice (approved by the Scottish Parliament) concerning the acquisition, retention, use and destruction of biometric data for criminal justice and police purposes (Section 7 of the Scottish Biometrics Commissioner Act 2020).

destruction or damage ([92]). Section 66 of the DPA 2018 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. According to the explanatory notes, the controller must evaluate the risks and implement appropriate security measures based on this evaluation, for example, encryption or specific levels of security clearance for staff processing the data ([93]). The evaluation must also take into account, for example, the nature of the data processed and any other relevant factors or circumstances that might affect the security of the processing.

(53) The regime governing compliance with the data security principles is very similar to one established by Articles 29 to 31 of Directive (EU) 2016/680. In particular, in case of a personal data breach in relation to personal data for which the controller is responsible, according to Section 67(1) of the DPA 2018, the controller must, without undue delay, and where feasible, within 72 hours after becoming aware of the breach, notify the personal data breach to the Information Commissioner ([94]). The obligation to notify does not apply when the personal data breach is unlikely to result in a risk to the rights and freedoms of individuals ([95]). The controller must document the facts relating to any personal data breach, its effects and remedial action taken in a way that enables the Information Commissioner to verify compliance with the DPA ([96]). If a processor becomes aware of a security breach, it must notify the controller without undue delay ([97]).

(54) Under Section 68(1) of the DPA 2018, if a personal data breach is likely to pose a high risk to the rights and freedoms of individuals, the controller must inform the data subject of the breach without undue delay ([98]). The notice must include the same information as the notification to the Information Commissioner described in recital 53. This obligation does not apply if the controller has implemented appropriate technical and organisational protection measures, which were applied to the personal data affected by the breach. It also does not apply if the controller has taken subsequent measures, which ensure that the high risk to the rights and freedoms of data subjects is no longer likely to materialise. Finally, the controller is not required to notify the data subject if doing so would involve a disproportionate effort ([99]). In that case, the information must be made available to the data subject in another equally effective way, for example, by means of a public communication ([100]). If the controller has not informed the data subject of the breach, the Information Commissioner, having been notified pursuant to Section 67 of the DPA and after considering the likelihood of the breach resulting in a high risk, can require the controller to notify the data subject of the breach ([101]).

([92]) In accordance with the Explanatory Notes to the DPA 2018 (see footnote 45), the controller must, in particular: design and organise their security to fit the nature of the personal data they hold and the harm that may result from a security breach; be clear about who in their organisation is responsible for ensuring information security; make sure they have the right physical and technical security, backed up by robust policies and procedures and reliable, well-trained staff; and be ready to respond to any breach of security swiftly and effectively.

([93]) Paragraph 221 of the Explanatory Notes to the DPA 2018 (see footnote 45).

([94]) Section 67(4) of the DPA 2018 provides that the notification must include a description of the nature of the personal data breach (including, where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned), the name and contact details of a contact point, a description of the likely consequences of the personal data breach, and a description of the measures taken or proposed to be taken by the controller to address the personal data breach (including, where appropriate, measures to mitigate its possible adverse effects).

([95]) Section 67(2) of the DPA 2018.

([96]) Section 67(6) of the DPA 2018.

([97]) Section 67(9) of the DPA 2018.

([98]) Under Section 68(7) of the DPA 2018 the controller may restrict, wholly or partly, the provision of information to the data subject to the extent that and for so long as the restriction is, having regard to the fundamental rights and legitimate interests of the data subject, a necessary and proportionate measure to (a) avoid obstructing an official or legal inquiry, investigation or procedure; (b) avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties; (c) protect public security; (d) protect national security; (e) protect the rights and freedoms of others.

([99]) Section 68(3) of the DPA 2018.

([100]) Section 68(5) of the DPA 2018.

([101]) Section 68(6) of the DPA 2018, subject to the limitation provided for in Section 68(8) of the DPA 2018.

2.4.6. *Transparency*

(55) Data subjects must be informed of the main features of the processing of their personal data. This data protection principle is reflected in Section 44 of the DPA 2018 which, similarly to Article 13 of Directive (EU) 2016/680, provides that the controller has a general duty to make available to data subjects information on the processing of their personal data (whether by making the information generally available to the public or in any other way) ([102]). The information required to be made available includes (a) the identity and the contact details of the controller; (b) where applicable, the contact details of the data protection officer; (c) the purposes for which the controller processes personal data; (d) the existence of the rights of data subjects to request from the controller access to personal data, rectification of personal data, and erasure of personal data or the restriction of its processing; and (e) the existence of the right to lodge a complaint with the Information Commissioner and the contact details of the Commissioner ([103]).

(56) The controller must also, in specific cases for the purpose of enabling the exercise of a data subject's rights under the DPA 2018 (for example when the personal data being processed was collected without the knowledge of the data subject), give the data subject information about (a) the legal basis for the processing; (b) information about the period for which the personal data will be stored or, where that is not possible, about the criteria used to determine that period; (c) where applicable, information about the categories of recipients of the personal data (including recipients in third countries or international organisations); (d) such further information as is necessary to enable the exercise of the data subject's rights under Part 3 of the DPA 2018 ([104]).

2.4.7. *Individual rights*

(57) Data subjects must be granted a number of enforceable rights. Chapter 3 of Part 3 of the DPA 2018 provides individuals with rights of access, rectification and erasure and restriction ([105]), which are comparable to those provided under Chapter 3 of Directive (EU) 2016/680.

(58) The right of access is set out in Section 45 of the DPA 2018. First, an individual is entitled to obtain a confirmation from the controller whether his/her personal data is being processed or not ([106]). Second, where the personal data is processed, the data subject has a right to access that data and receive the following information about the processing: (a) the purposes and legal bases of the processing; (b) the categories of data concerned; (c) the recipient to whom the data has been disclosed; (d) the period for which the personal data is to be stored; (e) the existence of the data subject's right to rectification and erasure of personal data; (f) the right to lodge a complaint; and (g) any information about the origin of the personal data concerned ([107]).

(59) Pursuant to Section 46 of the DPA 2018, the data subject has a right to require the controller to rectify inaccurate personal data relating to him or her. The controller must rectify (or where the data is inaccurate because it is incomplete, complete) the data without undue delay. If the personal data must be maintained for the purposes of evidence, the controller must (instead of rectifying the personal data) restrict its processing ([108]).

([102]) The Guide to Law Enforcement Processing gives the following example: 'You have a generic privacy notice on your website which covers basic information about the organisation, the purpose you process personal data for, a data subject's rights and their right to complain to the Information Commissioner. You have received intelligence that an individual was present when a crime took place. On first interviewing this individual, you need to provide the generic information, as well as the further supporting information, to enable their rights to be exercised. You can only restrict the fair processing information you are providing if it will adversely affect the investigation you are undertaking' (Guide to Law Enforcement Processing, 'What information should we supply to an individual?', available at the following link: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/individual-rights/the-right-to-be-informed/#ib3).

([103]) The Guide to Law Enforcement Processing states that the information supplied about the processing of personal data must be concise, intelligible and easily accessible; written in clear and plain language, adapting this to the needs of vulnerable persons, such as children; and free of charge (Guide to Law Enforcement Processing, 'How should we provide this information?', available at the following link: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/individual-rights/the-right-to-be-informed/#ib1).

([104]) Section 44(2) of the DPA 2018.

([105]) For a detailed analysis of the subjects' rights see: Guide to Law Enforcement Processing on individual rights, available at the following link: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/individual-rights/

([106]) Section 45(1) of the DPA 2018.

([107]) Section 45(2) of the DPA 2018.

([108]) Section 46(4) of the DPA 2018.

(60) Section 47 of the DPA 2018 provides individuals with a right to erasure and restriction of processing. The controller must ([109]) erase personal data without undue delay where the processing of the personal data would infringe any of the data protection principles, the legal grounds of the processing, or the safeguards related to archiving and sensitive processing. The controller must also erase the data if they have a legal obligation to do so. If the personal data must be maintained for the purposes of evidence, the controller must (instead of erasing the personal data) restrict its processing ([110]). The controller must restrict the processing of personal data if a data subject contests the accuracy of personal data, but it is not possible to ascertain whether it is accurate or not ([111]).

(61) Where a data subject requests the rectification or erasure of personal data or the restriction of its processing, the controller must inform the data subject in writing whether the request has been granted, and if it has been refused, inform the data subject of the reasons for the refusal and the available redress avenues (data subject's right to make a request to the Information Commissioner to investigate whether the restriction has been applied lawfully, right to lodge a complaint with the Information Commissioner, and right to apply for a compliance order to a court) ([112]).

(62) Where the controller rectifies personal data received from another competent authority, it must notify the other authority ([113]). Where the controller rectifies, erases or restricts the processing of personal data which has been disclosed by the controller, the controller must notify the recipients, and the recipients must similarly rectify, erase or restrict the processing of the personal data (insofar as they retain responsibility for it) ([114]).

(63) Moreover, the data subject has the right to be informed without undue delay by the controller about a personal data breach when this is likely to result in a high risk to the rights and freedoms of individuals ([115]).

(64) In relation to all those rights of the data subject and similarly to what is provided under Article 12 of Directive (EU) 2016/680, the controller has an obligation to ensure that any information to the data subject is provided in a concise, intelligible and easily accessible form ([116]) and, where possible, it should be provided in the same form as the request ([117]). The controller must comply with a request of the data subject without undue delay or in any case before, in principle, the end of a period of one month from the request ([118]). Where the controller has reasonable doubts about the identity of an individual, they may request additional information and delay dealing with the request until the identity is ascertained. The controller can require a reasonable fee or refuse to act when it deems the request to be manifestly unfounded. ([119]). The ICO has provided guidance on when a request is considered to be manifestly unfounded or excessive and when a fee can be requested ([120]).

(65) Moreover, under Section 53(4) of the DPA 2018, the Secretary of State can by regulations specify the maximum amount of a fee.

([109]) A data subject may request the controller to erase personal data or to restrict its processing (but the duties of the controller to erase the data or restrict its processing apply whether or not such a request is made).

([110]) Sections 46(4) and 47(2) of the DPA 2018.

([111]) Section 47(3) of the DPA 2018.

([112]) Section 48(1) of the DPA 2018.

([113]) Section 48(7) of the DPA 2018.

([114]) Section 48(9) of the DPA 2018.

([115]) Section 68 of the DPA 2018.

([116]) Section 52(1) of the DPA 2018.

([117]) Section 52(3) of the DPA 2018.

([118]) Section 54 of the DPA 2018 defines the meaning of 'applicable time period' which means the period of 1 month, or such longer period as may be specified in regulations, beginning with the relevant time (when the controller receives the request in question; when the controller receives the information (if any) requested in connection with a request under Section 52(4) of the DPA; or when the fee (if any) charged in connection with the request under Section 53 of the DPA is paid.

([119]) Section 53(1) of the DPA 2018.

([120]) According to the ICO guidance, a controller may decide to charge a data subject if his/her request is manifestly unfounded or excessive, but still it chooses to respond to it. The fee must be reasonable and able to justify the cost. Guide to Law Enforcement Processing 'Manifestly unfounded and excessive requests', available at the following link: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/individual-rights/manifestly-unfounded-and-excessive-requests/

2.4.7.1 Restrictions of the rights of the data subject and transparency obligations

(66) A competent authority can, under certain circumstances, restrict certain rights of the data subject: the right to access ([121]), to be informed ([122]), to know about a personal data breach ([123]), and to be informed about the reason of the refusal of a request of rectification or erasure ([124]). Similarly to the regime contained in Chapter III of Directive (EU) 2016/680, the competent authority can only apply the restriction where it is, having regard to the fundamental rights and legitimate interests of the data subject, necessary and proportionate to: (a) avoid obstructing an official or legal inquiry, investigation or procedure; (b) avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties; (c) protect public security; (d) protect national security; (e) protect the rights and freedoms of others.

(67) The ICO has provided guidance on the application of those restrictions. According to this guidance, controllers must carry out a case-by-case analysis to balance the rights of the individual against the harm disclosure would cause. In particular, they need to justify any restriction applied as necessary and proportionate and may only limit what is provided if it would prejudice the aforementioned purposes ([125]).

(68) There are also a number of other pieces of guidance issued by competent authorities that provide detailed information on all aspects of the data protection legislation, including on the application of the restrictions of data subjects' rights ([126]). For example, in relation to Section 45(4), the Data Protection Manual of the National Police Chief's Counsel states: 'It is important to note that the restrictions can only be applied as far as is necessary and can only be applied as long as is necessary. Consequently a blanket application of the restriction to all of an applicant's personal data or permanent application of the restriction are not permitted. On the latter point, it is often the case that personal data collected without the knowledge of the data subject who is a suspect in an investigation needs to be initially protected from disclosure to them, to avoid prejudicing the investigation while the investigation is proceeding, but at a later date there would be no harm in disclosure if the personal data had been disclosed to the individual during interview. Police forces must adopt processes that ensure the application of these restrictions is only to the extent required and is only for the necessary duration' ([127]). This guidance also provide examples of when each of the restrictions is likely to be engaged ([128]).

(69) Moreover, in relation to the possibility to restrict any of the above-mentioned rights for the protection of 'national security', a controller may apply for a certificate signed by a cabinet Minister or the Attorney General (or the Advocate General for Scotland) certifying that a restriction of such rights is a necessary and proportionate measure for the protection of national security ([129]). The United Kingdom government has issued guidance on national security certificates under the DPA 2018 that notably highlight that any limitation to data subjects' rights for safeguarding national security must be proportionate and necessary ([130]) (for more details on the national security certificates see recitals 131 to 134).

([121]) Section 45(4) of the DPA 2018.
([122]) Section 44(4) of the DPA 2018.
([123]) Section 68(7) of the DPA2018.
([124]) Section 48(3) of the DPA 2018.
([125]) See, for example, the Guide to Law Enforcement Processing on the right of access, available at the following link: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/individual-rights/the-right-of-access/#ib8
([126]) See, for example, the Data Protection Manual for Police Data Protection Professional issued by the National Police Chief Counsel (see footnote 27) or the guidance provided by the Serious Fraud Office, available at the following link: https://www.sfo.gov.uk/publications/guidance-policy-and-protocols/sfo-operational-handbook/data-protection/
([127]) Data protection Manual of the National Police Chief Counsel, page 140 (see footnote 27).
([128]) The Data Protection Manual of the National Police Chief Counsel provides that, 'avoid obstructing an official or legal inquiry, investigation or procedure' is likely to be relevant to personal data processed for inquests, family court proceedings, non-criminal internal discipline enquiries, and inquiries such as the Independent Inquiry into Child Sexual Abuse; while 'protect the rights and freedoms of others' is relevant to personal data that would also relate to other individuals as well as the applicant' (Data Protection Manual of the National Police Chief Counsel, page 140, see footnote 27).
([129]) Section 79 of the DPA 2018.
([130]) UK Government Guidance on National Security Certificates, available at the following link: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/910279/Data_Protection_Act_2018_-_National_Security_Certificates_Guidance.pdf

(70) Moreover, where a restriction to a data subject's right applies, the competent authority must inform the data subject without undue delay that their rights have been restricted, of the reasons for the restriction, and of the available redress avenues, unless providing that information would undermine the reason for applying the restriction ([131]). As a further safeguard against the misuse of restrictions, the controller must record the reasons for restricting information and make the record available to the Information Commissioner if requested ([132]).

(71) If the controller refuses to provide additional transparency information, or access, or refuses a request for rectification, erasure or restriction of processing, the individual can request the Information Commissioner to investigate whether the controller has used the restriction lawfully ([133]). The concerned individual can also make a complaint to the Information Commissioner or apply to a court to order the controller to comply with the request ([134]).

2.4.7.2. Automated decision making

(72) Sections 49 and 50 of the DPA 2018 cover respectively the rights related to automated decision-making and the safeguards to be applied ([135]). Similarly to Article 11 of Directive (EU) 2016/680, the controller can only take a significant decision based solely on automated processing of personal data if it is required or authorised by law ([136]). A decision is significant, if it would produce an adverse legal effect concerning the data subject or significantly affect the data subject ([137]).

(73) Where the controller is required or authorised by law to make a significant decision, Section 50 of the DPA 2018 sets out the safeguards that will apply to such a decision (which is defined as a 'qualifying significant decision'). The controller must, as soon as reasonably practicable, notify the data subject that such a decision has been made. The data subject can then, within a month, request the controller to reconsider the decision or take a new decision that is not based solely on automated processing. The controller must consider the request and inform the data subject of the outcome of that consideration. The DPA 2018 gives the Secretary of State the power to adopt regulations for additional safeguards ([138]). No such regulations have been adopted yet.

2.4.8. *Onward transfers*

(74) The level of protection afforded to personal data transferred from a law enforcement authority of a Member State to a United Kingdom law enforcement authority must not be undermined by the further transfer of such data to recipients in a third country. Such 'onward transfers', which from the perspective of a United Kingdom law enforcement authority constitute international transfers from the United Kingdom, should be permitted only where the further recipient outside the United Kingdom is itself subject to rules ensuring a similar level of protection to that guaranteed within the United Kingdom legal order.

([131]) Section 44(5) and (6): Section 45(5) and (6); Section 48(4) of the DPA 2018.
([132]) Section 44 (7); Section 45(7); Section 48(6) of the DPA 2018.
([133]) Section 51 of the DPA 2018.
([134]) Section 167 of the DPA 2018.
([135]) Regarding the scope of the automated processing, the Explanatory Notes to the DPA 2018 states that: 'these provisions are in relation to fully automated decision-making and not to automated processing. Automated processing (including profiling) is when an operation is carried out on data without the need for human intervention. It is regularly used in law enforcement to filter down large data sets to manageable amounts for a human operator to then use. Automated decision-making is a form of automated processing and requires the final decision to be made without human interference'. (Explanatory Notes to the DPA, paragraph 204, see footnote 45).
([136]) In addition to the protections provided for in the DPA, there are other legislative restrictions in the United Kingdom legal framework, which apply to law enforcement agencies and would prevent automated processing (including profiling) that results in unlawful discrimination. The Human Rights Act 1998 incorporates the rights from the ECHR into the law of the United Kingdom, including the right in Article 14 of the Convention, the prohibition on discrimination. Similarly, the Equality Act 2010 prohibits discrimination against people with protected characteristics (which includes sex, race, disability, etc.).
([137]) Section 49(2) of the DPA 2018.
([138]) Section 50(4) of the DPA 2018.

(75) The United Kingdom regime on international transfers is regulated by Chapter 5 of Part 3 of the DPA 2018 ([139]) and reflects the approach taken in Chapter V of Directive (EU) 2016/680. In particular, in order to transfer a personal data to a third country, a competent authority must meet three conditions: (a) the transfer must be necessary for a law enforcement purpose; (b) the transfer must be based on: (i) an adequacy regulation in respect of the third country; (ii) if not based on an adequacy regulation, the existence of appropriate safeguards; or (iii) if not based on an adequacy decision or appropriate safeguards, it must be based on special circumstances; and (c) the recipient of the transfer must be: (i) a relevant authority (i.e. the equivalent of a competent authority) in the third country; (ii) a 'relevant international organisation' e.g. an international body that carries out functions corresponding to any of the law enforcement purposes; or (iii) a person other than a relevant authority, but only where the transfer 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; a 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 ([140]).

(76) Adequacy regulations with respect to a third country, a territory or a sector within a third country, an international organisation, or a description ([141]) of such a country, territory, sector or organisation are adopted by the Secretary of State. As regards the standard to be met, the Secretary of State has to assess whether such a territory/sector/organisation ensures an adequate level of protection of personal data. Section 74A(4) of the DPA 2018 specifies that, to this end, the Secretary of State must consider a number of elements that reflects those listed in under Article 36 of Directive (EU) 2016/680 ([142]). In this respect, since the end of the transition period, Part 3 of the DPA 2018 constitutes 'EU-derived domestic legislation' which, as explained, will be interpreted by the United Kingdom courts in accordance with relevant case-law of the Court of Justice dating from before the United Kingdom's departure from the Union and general principles of Union law, as they had effect immediately before the end of the transition period. This includes the 'essential equivalence' standard that will thus apply to the adequacy assessments carried out by the United Kingdom authorities.

(77) As for the procedure, the regulations are subject to the 'general' procedural requirements provided for in Section 182 of the DPA 2018. Under this procedure, the Secretary of State must consult the Information Commissioner when

([139]) This new framework became at the end of the transition period, including the power for the Secretary of State to make adequacy regulations. However, the DPPEC Regulations (in particular, paragraphs 10–12 of the Schedule 21 that these Regulations insert into the DPA 2018) provide that certain transfers of personal data on and after the end of the transition period are treated as if they are based on adequacy regulations. These transfers include transfers to third countries which are the subject of an EU adequacy decision at the end of transition period and to EU Member States, the EFTA States and the territory of Gibraltar by virtue of their application of the Law Enforcement Directive to law enforcement data processing (the EFTA States apply the Directive (EU) 2016/680 as a result of their obligations under the Schengen *acquis*). This means that at the end of the transition period the transfers to these countries can continue as before the EU exit. After the end of the transition period, the Secretary of the State must conduct a review of the adequacy findings within 4 years.

([140]) Sections 73 and 77 of the DPA 2018.

([141]) The United Kingdom authorities have explained that the description of a country or international organisation refers to a situation where it would be necessary to do a specific and partial determination of adequacy with focused restrictions (for example an adequacy regulation in relation to only certain type of data transfers).

([142]) See Section 74A(4) of the DPA 2018 which provides that when assessing the adequacy of the level of protection 'the Secretary of State must, in particular, take account of (a) the rule of law, respect for human rights and fundamental freedoms, relevant legislation, both general and sectoral, including concerning public security, defence, national security and criminal law and the access of public authorities to personal data, as well as the implementation of such legislation, data protection rules, professional rules and security measures, including rules for the onward transfer of personal data to another third country or international organisation, which are complied with in that country or international organisation, case-law, as well as effective and enforceable data subject rights and effective administrative and judicial redress for the data subjects whose personal data is transferred; (b) the existence and effective functioning of one or more independent supervisory authorities in the third country or to which an international organisation is subject, with responsibility for ensuring and enforcing compliance with data protection rules, including adequate enforcement powers, for assisting and advising data subjects in exercising their rights and for cooperation with the Commissioner; and (c) the international commitments the third country or international organisation concerned has entered into, or other obligations arising from legally binding conventions or instruments as well as from its participation in multilateral or regional systems, in particular in relation to the protection of personal data'.

proposing to make future United Kingdom adequacy regulations ([143]). Once adopted by the Secretary of State, those regulations are laid before Parliament and subject to thenegative resolution' procedure under which both Houses of Parliament can scrutinise the regulation and have the ability to pass a motion annulling the regulation within a 40-day period ([144]).

(78) According to Section 74B(1) of the DPA 2018, the adequacy regulations must be reviewed at intervals of not more than four years and the Secretary of State must, on an ongoing basis, monitor developments in third countries and international organisations that could affect decisions to make adequacy regulations, or to amend or revoke such regulations. Where the Secretary of State becomes aware that a given country or an organisation no longer ensures an adequate level of protection of personal data, he must, to the extent necessary, amend or revoke the regulations and enter into consultations with the third country or international organisation concerned to remedy the lack of an adequate level of protection.

(79) Similarly to what is provided in the Article 37 of Directive (EU) 2016/680, in the absence of an adequacy regulation, a transfer of personal data in the context of the law enforcement sector would be possible when appropriate safeguards are in place. Such safeguards are ensured by means of either (a) a legal binding instrument containing appropriate safeguards for the protection of personal data; or (b) an assessment performed by the controller which, having assessed all the circumstances surrounding the transfer, concludes that appropriate safeguards exist to protect the data ([145]). Furthermore, when transfers are based on appropriate safeguards, the DPA 2018 provides that, in addition to the ICO's normal oversight role, competent authorities must provide specific information about the transfers to the ICO ([146]).

(80) If a transfer is not based on an adequacy decision or appropriate safeguards, it can take place only in certain, specified circumstances, referred to as 'special circumstances' ([147]). This is the case when the transfer is necessary: (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 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) ([148]). It may be noted that points (d) and (e) do not apply if the rights and freedoms of the data subject override the public interest in the transfer ([149]). This set of circumstances corresponds to the specific situations and conditions qualifying as 'derogations' under Article 38 of Directive (EU) 2016/680.

(81) In those circumstances, 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 Information Commissioner upon request ([150]).

(82) Section 78 of the DPA 2018 regulates the scenario of 'subsequent transfers', namely when personal data that has been transferred from the United Kingdom to a third country, is subsequently transferred to another third country or an international organisation. Pursuant to Section 78(1), the United Kingdom transferring controller must make it a condition of the transfer that the data is not to be further transferred to a third country without the authorisation of the transferring controller. In addition, according to Section 78(3) and similarly to what is provided under Article 35(1)(e) of Directive (EU) 2016/680, a number of substantive requirements apply in case such an authorisation is required. More specifically, when deciding whether to authorise or not the transfer, a competent

([143]) See the Memorandum of Understanding between the Secretary of State for the Department for Digital, Culture, Media and Sport and the Information's Commissioner's Office on the role of the ICO in relation to new United Kingdom adequacy assessment, available at following link: https://www.gov.uk/government/publications/memorandum-of-understanding-mou-on-the-role-of-the-ico-in-relation-to-new-uk-adequacy-assessments.

([144]) During this 40-day period, both Houses of Parliament can have an opportunity, should they wish, to vote against the regulations; if such a vote is passed the regulations will ultimately cease to have any further legal effect.

([145]) Section 75 of the DPA 2018.

([146]) According to Section 75(3) of the DPA 2018, where a transfer of data takes place in reliance on appropriate safeguards: (a) the transfer must be documented; (b) the documentation must be provided to the Commissioner on request; and (c) the documentation must include, in particular: (i) the date and time of the transfer; (ii) the name of and any other pertinent information about the recipient; (iii) the justification for the transfer; and (iv) a description of the personal data transferred.

([147]) Guide to Law Enforcement Processing, 'Are there any special circumstances?', available at the following link: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/international-transfers/#ib3

([148]) Section 76 of the DPA 2018.

([149]) Section 76 of the DPA 2018.

([150]) Section 76(3) of the DPA 2018.

authority has to make sure that the further transfer is necessary for a law enforcement purpose and should consider, among other factors, (a) the seriousness of the circumstances leading to the request for authorisation; (b) the purpose for which the personal data was originally transferred; and (c) the standards for the protection of personal data that apply in the third country or international organisation to which the personal data would be transferred.

(83) Furthermore, when the data subject to a further transfer from the United Kingdom was originally transferred from the European Union, additional safeguards apply.

(84) First, Section 73(1)(b) of the DPA 2018 – similarly to Article 35(1)(c) of Directive (EU) 2016/680 – provides that in a case where the personal data was originally transmitted or otherwise made available to the controller or another competent authority by a Member State, that Member State, or any person based in that Member State which is a competent authority for the purposes of Directive (EU) 2016/680, must have authorised the transfer in accordance with the law of the Member State.

(85) However, similarly to Article 35(2) of Directive (EU) 2016/680, such an authorisation is not required when (a) 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 (b) the authorisation cannot be obtained in good time. In this case, the authority in the Member State which would have been responsible for deciding whether to authorise the transfer must be informed without delay ([151]).

(86) Second, the same approach applies in case of data originally transferred from the European Union to the United Kingdom, then further transferred by the United Kingdom to a third country which would subsequently onward transfer it to a third country. In that case, pursuant to Section 78(4), the United Kingdom competent authority cannot give its authorisation to the latter transfer, under Section 78(1), unless the 'member State [that has originally transferred the data in question], or any person based in that member State which is a competent authority for the purposes of the Law Enforcement Directive, has authorised the transfer in accordance with the law of the member State'. These safeguards are important as they enable Member States' authorities to ensure continuity of protection, in compliance with EU data protection law, throughout the 'transfer chain'.

(87) This new framework for international transfers became applicable at the end of the transition period ([152]). However, paragraphs 10-12 of Schedule 21 (introduced by the DPPC Regulations) provide that as of the end of the transition period, certain transfers of personal data are treated as if they are based on adequacy regulations. These transfers include transfers to a Member State, an EFTA State, a third country which is the subject of an EU adequacy decision at the end of transition period and the territory of Gibraltar. Consequently, the transfers to these countries can continue as before the United Kingdom's withdrawal from the Union. After the end of the transition period, the Secretary of State must conduct a review of these adequacy findings during a period of four years, i.e. by the end of December 2024. According to the explanation provided by the United Kingdom authorities, although the Secretary of State needs to undertake such a review by the end of December 2024, the transitional provisions do not include a 'sunset' provision and the relevant transitional provisions will not automatically cease to have effect if a review is not completed by the end of December 2024.

2.4.9. *Accountability*

(88) Under the accountability principle, public authorities processing data are required to put in place appropriate technical and organisational measures to effectively comply with their data protection obligations and be able to demonstrate such compliance, in particular to the competent supervisory authority.

(89) This principle is reflected in Section 56 of the DPA 2018, which introduces a general accountability obligation for the controller, i.e. an obligation to implement appropriate technical and organisational measures to ensure, and to be able to demonstrate, that the processing of personal data complies with the requirements of Part 3 of the DPA 2018. The measures implemented must be reviewed and updated where necessary, and where proportionate in relation to the processing, include appropriate data protection policies.

([151]) Section 73(5) of the DPA 2018.

([152]) The applicability of this new framework must be read in the light of Article 782 of the Trade and Cooperation Agreement between the European Union and the European Atomic Energy Community, of the one part, and the United Kingdom of Great Britain and Northern Ireland, of the other part (OJ L 444, 31.12.2020, p. 14) ('the EU-UK TCA'), available at the following link: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:22020A1231(01)&from=EN

(90) In line with Chapter IV of Directive (EU) 2016/680, Sections 55–71 of the DPA 2018 provide for different mechanisms to ensure accountability and allow controllers and processors to demonstrate compliance. In particular, controllers are required to implement data protection measures by design and by default, i.e. to ensure that data protection principles are implemented in an effective manner and are required to maintain records of all categories of processing activities for which the controller is responsible (including information on the identity of the controller, contact details of the data protection officer, the purposes of the processing, the categories of recipients of disclosures, and a description of the categories of data subject, and personal data) and keep these records available for the Information Commissioner on request. The controller and processor must also keep logs for certain processing operations and make them available to the Information Commissioner ([153]). The controllers are also specifically required to cooperate with the Information Commissioner in the performance of the Commissioner's tasks.

(91) The DPA 2018 also sets out additional requirements for processing that is likely to result in a high risk to the rights and freedoms of individuals. These include an obligation to carry out data protection impact assessments and to consult the Information Commissioner before processing if such an assessment indicates that the processing would result in a high risk to the rights and freedoms of individuals (in the absence of measures to mitigate the risk).

(92) The controllers must furthermore appoint a data protection officer, unless the controller is a court, or other judicial authority, acting in its judicial capacity ([154]). The controller must ensure that the data protection officer is involved in all issues relating to the protection of personal data, have necessary resources and access to personal data and processing operations and can independently perform its tasks. The tasks of the data protection officer are set out in Section 71 of the DPA 2018, including providing information and advice, monitoring compliance as well as cooperating with and acting as a contact point for the Information Commissioner. In performing its tasks, the data protection officer must have regard to the risks associated with processing operations, taking into account the nature, scope, context and purposes of processing.

2.5. **Oversight and enforcement**

2.5.1. *Independent oversight*

(93) In order to ensure that an adequate level of data protection is guaranteed also in practice, an independent supervisory authority tasked with powers to monitor and enforce compliance with the data protection rules must be in place. This authority is to act with complete independence and impartiality in performing its duties and exercising its powers.

(94) In the United Kingdom, the oversight and enforcement of compliance with the UK GDPR and the DPA 2018 is carried out by the Information Commissioner ([155]). The Information Commissioner oversees also the processing of personal data by competent authorities falling under the scope of Part 3 of the DPA 2018 ([156]). The Information Commissioner is a 'Corporation Sole': a separate legal entity constituted in a single person. The Information Commissioner is supported in her work by an office. On 31 March 2020 the Information Commissioner's Office had 768 permanent staff ([157]). The sponsor-department of the Information Commissioner is the Department for Digital, Culture, Media and Sport ([158]).

([153]) Section 62 of the DPA 2018.
([154]) Section 69 of the DPA 2018.
([155]) Article 36(2)(b) of the Directive (EU) 2016/680.
([156]) Section 116 of the DPA 2018.
([157]) Information Commissioner's Annual Report and Financial Statements 2019-2020, available at the following link: https://ico.org.uk/media/about-the-ico/documents/2618021/annual-report-2019-20-v83-certified.pdf
([158]) A Management Agreement regulates the relation between the two. In particular, the key responsibilities of DCMS, as sponsoring department, include: ensuring that the ICO is adequately funded and resourced; representing the interests of the ICO to Parliament and other Government departments; ensuring that there is a robust national data protection framework in place; and providing guidance and support to the ICO on corporate issues such as estate issues, leases and procurement (the Management Agreement 2018-2021 available at the following link: https://ico.org.uk/media/about-the-ico/documents/2259800/management-agreement-2018-2021.pdf).

(95) The independence of the Commissioner is explicitly established in Article 52 of the UK GDPR which reflects the requirements laid down in Article 52(1) to (3) of Regulation (EU) 2016/679 of the European Parliament and of the Council ([159]). The Commissioner must act with complete independence in performing her tasks and exercising her powers in accordance with the UK GDPR, remain free from external influence, whether direct or indirect, in relation to those tasks and powers, and neither seek nor take instructions from anyone. The Commissioner must also refrain from any action incompatible with her duties and shall not, while holding office, engage in any incompatible occupation, whether gainful or not.

(96) The conditions for the appointment and removal of the Information Commissioner are set out in Schedule 12 to the DPA 2018. The Information Commissioner is appointed by the Queen on a recommendation from Government pursuant to a fair and open competition. The candidate must have the appropriate qualifications, skills and competence. In accordance with the Governance Code on Public Appointments ([160]), a list of appointable candidates is made by an advisory assessment panel. Before the Secretary of State at the Department for Digital, Culture, Media and Sport finalises his or her decision, the relevant Select Committee of Parliament must carry out a pre-appointment scrutiny. The position of the Committee is made public ([161]).

(97) The Information Commissioner holds office for a term of up to seven years. The Information Commissioner can be removed from office by Her Majesty following an Address by both Houses of Parliament ([162]). No request for dismissal of the Information Commissioner can be presented to either House of Parliament unless a Minister has presented a report to that House stating that he or she is satisfied that the Information Commissioner is guilty of serious misconduct and/or the Commissioner no longer fulfils the conditions required for the performance of the Commissioner's functions ([163]).

(98) The funding of the Information Commissioner comes from three sources: (i) data protection charges paid by controllers which are set by a Secretary of State's regulations ([164]) and amount to 85–90 % of the Office's annual budget ([165]); (ii) grant in aid which may be paid by the Government to the Information Commissioner and is mainly used to finance the operating costs of the Information Commissioner as regards non-data protection related tasks ([166]); (iii) fees charged for services ([167]). At present, no such fees are charged.

(99) The general functions of the Information Commissioner in relation to the processing of personal data falling under the scope of Part 3 of the DPA 2018, are laid down in Schedule 13 to the DPA 2018. The tasks include monitoring and enforcement of Part 3 of the DPA 2018, promoting public awareness, advising Parliament, the government and other institutions on legislative and administrative measures, promoting the awareness of controllers and processors of their obligations, providing information to a data subject concerning the exercise of the data subject's rights, and

([159]) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1).

([160]) Governance Code on Public Appointments, available at the following link: https://www.gov.uk/government/publications/governance-code-for-public-appointments

([161]) Second Report of Session 2015–2016 of the Culture, Media and Sports Committee at the House of Commons, available at the following link: https://publications.parliament.uk/pa/cm201516/cmselect/cmcumeds/990/990.pdf

([162]) An 'Address' is a motion laid before Parliament which seeks to make the Monarch aware of Parliament's opinions on a particular issue.

([163]) Schedule 12, paragraph 3 to the DPA 2018.

([164]) Section 137 of the DPA 2018.

([165]) Section 137 and 138 of the DPA 2018 contain a number of safeguards to ensure the charges are set at an appropriate level. In particular, Section 137(4) of the DPA 2018 lists the matters which the Secretary of State must have regard to when making regulations which specify the amount different organisations must pay. Section 138(1) and Section 182 of the DPA 2018 also contain a legal requirement for the Secretary of State to consult with the Information Commissioner and other representatives of persons likely to be affected by the regulations, before they are made so that their views can be taken into account. In addition, under Section 138(2) of the DPA 2018, the Information Commissioner is required to keep the working of the Charges Regulations under review and may submit proposals to the Secretary of State for amendments to be made to the Regulations. Finally, except where regulations are made simply to take into account an increase in the retail price index (in which case they will be subject to the negative resolution procedure), the regulations are subject to the affirmative resolution procedure and may not be made until they have been approved by resolution of each House of Parliament.

([166]) The Management Agreement clarified that 'The Secretary of State may make payments to the IC out of money provided by Parliament under paragraph 9 of Schedule 12 to the DPA 2018. After consultation with the IC, DCMS will pay to the IC appropriate sums (the grant in aid) for ICO administrative costs and the exercise of the IC's functions in relation to a number of specific functions, including freedom of information' (Management Agreement 2018–2021, paragraph 1.12, see footnote 158).

([167]) Section 134 of the DPA 2018.

conducting investigations. To maintain the independence of the judiciary, the Information Commissioner is not authorised to exercise her functions in relation to processing of personal data by an individual acting in a judicial capacity, or a court or tribunal acting in its judicial capacity. However, oversight on the judiciary is ensured by specialised bodies, discussed below.

2.5.1.1. Enforcement, including sanctions

(100) The Commissioner has general investigative, corrective, authorisation and advisory powers in relation to processing of personal data to which Part 3 of the DPA 2018 applies. The Commissioner has the powers to notify the controller or the processor of an alleged infringement of Part 3, to issue warnings to a controller or processor that intended processing operations are likely to infringe provisions of Part 3, and to issue reprimands to a controller or processor where processing operations have infringed provisions of Part 3. Moreover, on its own initiative or on request, the Commissioner may issue opinions to the United Kingdom Parliament, the government or other institutions and bodies as well as to the public on any issue related to the protection of personal data ([168]).

(101) Furthermore, the Commissioner has powers to:

— order the controller and the processor (and in certain circumstances any other person) to provide necessary information by giving an information notice ('information notice') ([169]),

— carry out investigations and audits by giving an assessment notice, which may require the controller or processor to permit the Commissioner to enter specified premises, inspect or examine documents or equipment, interview people processing personal data on behalf of the controller ('assessment notice') ([170]),

— obtain otherwise access to documents of controllers and processors and access to their premises in accordance with Section 154 of the DPA 2018 ('powers of entry and inspection'),

— exercise corrective powers including by means of warnings and reprimands or give orders by a mean of an enforcement notice, which requires controllers/processors to take or refrain from taking specified steps ('enforcement notice') ([171]), and

— issue administrative fines in the form of a penalty notice ('penalty notice') ([172]).

(102) The ICO's Regulatory Action Policy sets out the circumstances under which the Commissioner will issue respectively an information, assessment, enforcement and penalty notice ([173]). An enforcement notice may imposes requirements which the Commissioner considers appropriate for the purpose of remedying the failure. A penalty notice requires the person to pay to the Information Commissioner an amount specified in the notice. A penalty notice may be given when there has been a failure to comply with certain provisions of the DPA 2018 ([174]) or may be given to a controller or processor that has not complied with an information notice, an assessment notice or an enforcement notice.

(103) More specifically, in determining whether to give a penalty notice to a controller or processor and determining the amount of the penalty, the Information Commissioner must have regard to the matters listed Section 155(3) of the DPA 2018, including the nature and gravity of the failure, the intentional or negligent character of the failure, any action taken by the controller or processor to mitigate the damage suffered by data subjects, the degree of responsibility of the controller or processor (taking into account technical and organisational measures

([168]) Paragraph 2 of the Schedule 13 to the DPA 2018.
([169]) Section 142 of the DPA 2018 (subject to the restrictions in Section 143 DPA 2018).
([170]) Section 146 of the DPA 2018 (subject to the restrictions in Section 147 DPA 2018).
([171]) Section 149 to 151 of the DPA 2018 (subject to the restrictions in Section 152 DPA 2018).
([172]) Section 155 of the DPA 2018 (subject to the restrictions in Section 156 DPA 2018).
([173]) Regulatory Action Policy, available at the following link: https://ico.org.uk/media/about-the-ico/documents/2259467/regulatory-action-policy.pdf
([174]) In particular the ICO may issue a penalty notice for compliance failure set out in Section 149(2), (3), (4), or (5) of the DPA 2018.

implemented by the controller or processor), any relevant previous failures by the controller or processor; the categories of personal data affected by the failure and whether the penalty would be effective, proportionate and dissuasive.

(104) The maximum amount of the penalty that may be imposed by a penalty notice is (a) GBP 17 500 000 in relation to a failure to comply with data protection principles (Sections 35, 36, 37, 38(1), 39(1) and 40 of the DPA 2018) transparency obligations and individual rights (Sections 44, 45, 46, 47, 48, 49, 52 and 53 of the DPA 2018), and principles for international transfers of personal data (Sections 73, 75, 76, 77 or 78 of the DPA 2018); and (b) GBP 8 700 000 otherwise ([175]). In relation to a failure to comply with an information notice, an assessment notice or an enforcement notice, the maximum amount of the penalty that may be imposed by a penalty notice is GBP 17 500 000.

(105) According to its latest annual reports (2018–2019 ([176]), 2019–2020 ([177])), the Information Commissioner has conducted a number of investigations in relation to processing of personal data by criminal law enforcement. For example, the Commissioner conducted an investigation and published an Opinion in October 2019 concerning the law enforcement use of facial recognition technology in public places. The investigation particularly focused on the use of live facial recognition capabilities in South Wales Police and the Metropolitan Police Service (MPS). Moreover, the Commissioner investigated the MPS 'Gangs matrix' ([178]) and found a range of serious infringements of data protection law that were likely to undermine public confidence in the matrix and the use of the data.

(106) In November 2018, the Information Commissioner issued an enforcement notice and the MPS subsequently took the steps required to increase security and accountability and to ensure that the data was used proportionately.

(107) Another example of a recent enforcement action is the GBP 325 000 fine issued by the Commissioner in May 2018 against the Crown Prosecution Service, for losing unencrypted DVDs containing recordings of police interviews. Moreover, the Information Commissioner conducted investigations into broader topics, for example in the first half of 2020 on the use of Mobile Phone Extraction for Policing Purposes and the processing of victims' data by the police.

(108) In addition to those enforcement powers of the Information Commissioner, certain violations of the data protection legislation constitute offences and may therefore be subject to criminal sanctions (Section 196 of the DPA 2018). This, for example, applies to obtaining or disclosing personal data without the consent of the controller and procuring the disclosure of personal data to another person without the consent of the controller ([179]); re-identifying information that is de-identified personal data without the consent of the controller responsible for de-identifying the personal data ([180]); intentionally obstructing the Commissioner to exercise its powers in relation to inspection of personal data in accordance with international obligations ([181]), making false statements on response to an information notice, or destroying information in connection to information and assessment notices ([182]).

(109) The Information Commissioner also has a duty under Section 139 of the DPA 2018 to lay before each House of Parliament a general report on the exercise of their functions under the Act ([183]).

([175]) Section 157 of the DPA 2018.
([176]) Information Commissioner's Annual Report and Financial Statements 2018–2019, available at the following link: https://ico.org.uk/media/about-the-ico/documents/2615262/annual-report-201819.pdf
([177]) Information Commissioner's Annual Report 2019–2020 (see footnote 157).
([178]) A database which recorded intelligence related to alleged gang members and victims of gang-related crimes.
([179]) Section 170 of the DPA 2018.
([180]) Section 171 of the DPA 2018.
([181]) Section 119 of the DPA 2018.
([182]) Sections 144 and 148 of the DPA 2018.
([183]) As set out in the Management Agreement, the annual report must: (i) cover any corporate, subsidiary or joint ventures under the ICO's control; (ii) comply with the Treasury's Financial Reporting Manual (FReM); (iii) contain a governance statement, setting out the ways in which the Accounting Officer has managed and controlled the resources used in the organisation during the course of the year, demonstrating how well the organisation is managing risks to the achievement of its aims and objectives; and (iv) outline main activities and performance during the previous financial year and set out in summary form forward plans (Management Agreement 2018–2021, paragraph 3.26, see footnote 158).

2.5.2. *Oversight over the judiciary*

(110) Oversight of the processing of personal data by the courts and judiciary is twofold. Where a judicial office holder or a court is not acting in a judicial capacity, oversight is provided by the Information Commissioner. Where the controller is operating in a judicial capacity, the ICO cannot exercise its oversight functions ([184]) and the oversight is carried out by special bodies. This reflects the approach taken in Article 32 of Directive (EU) 2016/680.

(111) In particular, in the second scenario, for the courts of England and Wales and the First-tier and Upper Tribunals of England and Wales, such oversight is provided by the Judicial Data Protection Panel ([185]). Additionally, the Lord Chief Justice and Senior President of Tribunals have issued a Privacy Notice ([186]) which sets out how the courts in England and Wales process personal data for a judicial function. A similar notice has been issued by the Northern Irish ([187]) and Scottish judiciaries ([188]).

(112) Moreover, in Northern Ireland, the Lord Chief Justice of Northern Ireland has appointed a High Court judge as Data Supervisory Judge (DSJ) ([189]). They have also issued guidance to the Northern Irish Judiciary on what to do in the event of a loss or potential loss of data and the process for dealing with any issues arising from this ([190]).

(113) In Scotland, the Lord President has appointed a Data Supervisory Judge to investigate any complaints on grounds of data protection. This is set out under the judicial complaints rules which mirror those established for England and Wales ([191]).

(114) Finally, in the Supreme Court, one of the Supreme Court Justices is nominated to oversee data protection.

([184]) Section 117 of the DPA 2018.

([185]) The Panel is responsible for providing guidance and training to the judiciary. It also deals with complaints from data subjects in respect of the processing of personal data by courts, tribunals and individuals acting in a judicial capacity. The Panel aims to provide the means through which any complaint could be resolved. If a complainant was unhappy with a decision of the Panel, and they provided additional evidence, the Panel could reconsider its decision. While the Panel itself does not impose financial sanctions, if the Panel considers that there is a sufficiently serious breach of the DPA 2018, it may refer it to the Judicial Conduct Investigation Office (JCIO), which will investigate the complaint. If the complaint is upheld, it is a matter for the Lord Chancellor and Lord Chief Justice (or a senior judge delegated to act on his behalf) to decide what action should be taken against the office holder. This could include, in order of severity: formal advice, formal warning, and reprimand and, ultimately, removal from office. If an individual is dissatisfied with the way the complaint has been investigated by the JCIO, they can further complain to the Judicial Appointments and Conduct Ombudsman (see https://www.gov.uk/government/organisations/judicial-appointments-and-conduct-ombudsman). The Ombudsman has the power to ask the JCIO to reinvestigate a complaint and can propose that the complainant be paid compensation where it believes that they have suffered damage as a result of maladministration.

([186]) The privacy notice from the Lord Chief Justice and Senior President of Tribunals is available at the following link: https://www.judiciary.uk/about-the-judiciary/judiciary-and-data-protection-privacy-notice

([187]) The privacy notice issued by the Lord Chief Justice of Northern Ireland is available at the following link: https://judiciaryni.uk/data-privacy

([188]) The Privacy Notice for Scottish Courts and Tribunals is available at the following link: https://www.judiciary.uk/about-the-judiciary/judiciary-and-data-protection-privacy-notice

([189]) The DSJ provides guidance to the judiciary and investigates breaches and/or complaints in respect of the processing of personal data by courts or individuals acting in a judicial capacity.

([190]) Where the complaint or breach is deemed to be serious it is referred to the Judicial Complaints Officer for further investigation in accordance with the Lord Chief Justice in Northern Ireland's Code of practice on Complaints. The outcome of such a complaint could include: no further action, advice, training or mentoring, informal warning, formal warning, final warning, restriction of practice or referral to a statutory tribunal. The code of practice on complaints issued by the Lord Chief Justice in Northern Ireland is available at the following link: https://judiciaryni.uk/sites/judiciary/files/media-files/14G.%20CODE%20OF%20PRACTICE%20Judicial%20~%2028%20Feb%2013%20%28Final%29%20updated%20with%20new%20comp..__1.pdf

([191]) Any complaint which is founded is investigated by the Data Supervisory Judge and referred to the Lord President who has the power to issue advice, a formal warning or a reprimand should he deem to be necessary (Equivalent rules exist for tribunal members and are available at the following link: https://www.judiciary.scot/docs/librariesprovider3/judiciarydocuments/complaints/complaintsaboutthejudiciaryscotlandrules2017_1d392ab6e14f6425aa0c7f48d062f5cc5.pdf?sfvrsn=5d3eb9a1_2).

2.5.3. *Redress*

(115) In order to ensure adequate protection and in particular the enforcement of individual rights, the data subject should be provided with effective administrative and judicial redress, including compensation for damages.

(116) First, a data subject has the right to lodge a complaint with the Information Commissioner, if the data subject considers that, in connection with personal data relating to him or her, there is an infringement of Part 3 of the DPA 2018 ([192]). As described in recitals 100 and 109, the Information Commissioner has the power to assess the compliance of the controller and processor with the DPA 2018, require them to take or refrain from taking necessary steps in case of non-compliance and impose fines.

(117) Second, the DPA 2018 provides a right to a remedy against the Information Commissioner. If the Commissioner fails to 'progress' ([193]) a complaint made by the data subject, the complainant has access to judicial remedy, as they can apply a First Tier Tribunal ([194]) to order the Commissioner to take appropriate steps to respond to the complaint, or to inform the complainant of progress on the complaint ([195]). In addition, any person who is given any of the notices above (information, assessment, enforcement or penalty notice) from the Commissioner may appeal to a First Tier Tribunal. If the Tribunal considers, that the decision of the Commissioner is not in accordance with the law or the Information Commissioner should have exercised its discretion differently, the Tribunal must allow the appeal, or substitute another notice or decision which the Information Commissioner could have given or made ([196]).

(118) Third, individuals can obtain judicial redress against controllers and processors directly before the courts under Section 167 of the DPA 2018. If, on an application by a data subject, a court is satisfied that there has been an infringement of the data subject's rights under the data protection legislation, the court may order the controller in respect of the processing, or a processor acting on behalf of that controller, to take steps specified in the order or to refrain from taking steps specified in the order. Moreover, under Section 169 of the DPA 2018, any person who suffers damage by reason of a violation of a requirement of the data protection legislation (including Part 3 of the DPA 2018), other than the UK GDPR, is entitled to compensation for that damage from the controller or the processor, except if the controller or processor proves that the controller or processor is not in any way responsible for the event giving rise to the damage. Damage includes both financial loss and damage not involving financial loss, such as distress.

(119) Fourth, as far as any person considers that his or her rights, including rights to privacy and data protection, have been violated by public authorities, he or she can obtain redress before the United Kingdom courts under the Human Rights Act 1998. The controllers under Part 3 of the DPA 2018, i.e. the competent authorities, are always public authorities within the meaning of the Human Rights Act 1998. An individual who claims that a public authority has acted (or proposes to act) in a way which is incompatible with a Convention right, and consequently unlawful under Section 6(1) of the Human Rights Act 1998 can bring proceedings against the authority in the appropriate court or tribunal, or rely on the rights concerned in any legal proceedings, when he or she is (or would be) a victim of the unlawful act ([197]).

([192]) Section 165 of the DPA 2018.

([193]) Section 166 of the DPA 2018 refers specifically to the following situations: (a) the Commissioner fails to take appropriate steps to respond to the complaint; (b) the Commissioner fails to provide the complainant with information about progress on the complaint, or of the outcome of the complaint, before the end of the period of 3 months beginning when the Commissioner received the complaint; or (c) if the Commissioner's consideration of the complaint is not concluded during that period, fails to provide the complainant with such information during a subsequent period of 3 months.

([194]) The First Tier Tribunal is the court competent for handling appeals against decisions made by government regulatory bodies. In the case of the Information Commissioner's decision, the competent chamber is the 'General Regulatory Chamber' which has jurisdiction over the whole United Kingdom.

([195]) Section 166 of the DPA 2018.

([196]) Sections 161 and 162 of the DPA 2018.

([197]) See case *Brown v Commissioner* of the Met 2016 where the court provided redress for the claimant in the data protection context in an action brought against the police. The court found in the claimant's favor, upholding her claims of breach of the DPA 1998 obligations, breach of the HRA 1998 (and the related right in Article 8 of the ECHR) and the tort of misuse of private information (the defendant ultimately conceded they were in breach of the DPA and ECHR, so the judgment was focused on what remedy was appropriate). As a result of these breaches, the court awarded monetary damages to the claimant.

(120) If the court finds any act of a public authority to be unlawful, it can grant such relief or remedy, or make such order, within its powers as it considers just and appropriate ([198]). The court can also declare a provision of primary legislation to be incompatible with a right guaranteed under the ECHR.

(121) Finally, after exhausting national remedies, an individual can obtain redress before the European Court of Human Rights for violations of the rights guaranteed under the ECHR.

2.6. **Onward sharing**

(122) United Kingdom law authorises the sharing of data by a law enforcement authority with other UK authorities for purposes other than the ones for which it was originally collected (so-called 'onward sharing') subject to certain conditions.

(123) Similarly to what is provided under Article 4(2) of Directive (EU) 2016/680, Section 36(3) of the DPA 2018 allows that personal data collected by a competent authority for a law enforcement purpose may be further processed (whether by the original controller or by another controller) for any other law enforcement purpose, provided that the controller is authorised by law to process data for the other purpose and the processing is necessary and proportionate ([199]). In this case, all the safeguards provided by Part 3 of the DPA 2018 and analysed above apply to the processing carried out by the receiving authority.

(124) In the United Kingdom legal order, different laws explicitly allow onward sharing. In particular, (i) the Digital Economy Act 2017 allows the sharing between public authorities for several purposes, for example in case of any fraud against the public sector which would involve loss or a risk to loss for a public authority ([200]) or in case of a debt owed to a public authority or to the Crown ([201]); (ii) the Crime and Courts Act 2013 permits the sharing of information with the National Crime Agency (NCA) ([202]) for combating, investigating and prosecuting serious and organised crime; (iii) the Serious Crime Act 2007 allows public authorities to disclose information to anti-fraud organisations for the purposes of preventing fraud ([203]).

(125) These laws explicitly provide that the sharing of information should be in compliance with the rules set in the DPA 2018. Moreover, the College of Policing has issued an Authorised Professional Practice on Information Sharing ([204]) to assist the police in complying with their data protection obligations under the UK GDPR, DPA and Human Rights Act 1998. The compliance of the sharing with the applicable data protection legal framework can, of course, be subject to judicial review ([205]).

(126) Moreover, similarly to what is set out in Article 9 of Directive (EU) 2016/680, the DPA 2018 provides that personal data collected for any law enforcement purpose may be processed for a purpose that is not a law enforcement one when the processing is authorised by law ([206]). This type of sharing covers two scenarios: (1) when a criminal law enforcement authority shares data with a non-criminal law enforcement authority other than an intelligence agency (such as e.g. a financial or tax authority, a competition authority, a youth welfare office); (2) when a criminal law

([198]) Section 8(1) of Human Rights Act 1998.
([199]) Section 36(3) of the DPA 2018.
([200]) Section 56 of the Digital Economy Act 2017, available at the following link: https://www.legislation.gov.uk/ukpga/2017/30/contents
([201]) Section 48 of the Digital Economy Act 2017.
([202]) Section 7 of the Crime and Courts Act 2013, available at the following link: https://www.legislation.gov.uk/ukpga/2013/22/contents
([203]) Section 68 of the Serious Crime Act 2007, available at the following link: https://www.legislation.gov.uk/ukpga/2007/27/contents
([204]) The Authorised Professional Practice on Information Sharing is available at the following link: https://www.app.college.police.uk/app-content/information-management/sharing-police-information
([205]) See for example case *M v the Chief Constable of Sussex Police* [2019] EWHC 975 (Admin) where the High Court was asked to consider data sharing between the police and a Business Crime Reduction Partnership (BCRP), an organisation empowered to manage exclusion notice scheme, prohibiting persons from entering its members' commercial premises. The court reviewed the data sharing, which was taking place on the basis of an agreement having the purpose of protecting the public and preventing crime and ultimately concluded that most aspects of data sharing were lawful, except in relation with some sensitive information shared between the police and BCRP. Another example is case *Cooper v NCA* [2019] EWCA Civ 16 where the Court of Appeal upheld the data sharing between the police and the Serious Organised Crime Agency (SOCA), a law enforcement agency currently part of the NCA.
([206]) Section 36(4) of the DPA 2018.

enforcement authority shares data with an intelligence agency. In the first scenario, the processing of personal data will fall within the scope of the UK GDPR as well as under Part 2 of the DPA 2018. As specified in the Decision adopted under Regulation (EU) 2016/679, the safeguards provided by the UK GDPR and Part 2 of the DPA 2018 provide a level of protection that is essentially equivalent to the one provided within the Union ([207]).

(127) In the second scenario, with respect to the sharing of data collected by a criminal law enforcement authority with an intelligence agency for purposes of national security, the legal basis authorising such sharing is the Counter Terrorism Act 2008 (CTA 2008) ([208]). Under the CTA 2008, any person may give information to any of the intelligence services for the purpose of discharging any of the functions of that service, including 'national security'.

(128) As regards the conditions under which data can be shared for national security purposes, the Intelligence Services Act and the Security Services Act limit the ability of the intelligence services to obtain data to what is necessary to discharge their statutory functions. Competent authorities, falling under the scope of Part 3 of the DPA 2018, seeking to share data with the intelligence services will need to consider a number of factors/limitations, in addition to the statutory functions of the agencies which are set out in the Intelligence Services Act and the Security Services Act ([209]). Section 20 of the CTA 2008 makes clear that any data sharing pursuant to Section 19 of the CTA 2008 must still comply with the data protection legislation; which means that all of the limitations and requirements of the DPA 2018 apply. Furthermore, law enforcement authorities and intelligence services are public authorities for the purpose of the Human Rights Act 1998, and must thus ensure that they act in compliance with rights guaranteed under the ECHR, including its Article 8. In order words, these requirements mean that all data sharing between law enforcement agencies and intelligence services shall comply with data protection legislation and the ECHR.

(129) The processing by intelligence services of personal data received or obtained from law enforcement authorities purposes of national security is subject to a number of conditions and safeguards ([210]). Part 4 of the DPA 2018 applies to all processing by or on behalf of the intelligence services. It sets out the main data protection principles

([207]) Commission Implementing Decision pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by the United Kingdom C(2021) 4800.

([208]) Section 19 of the Counter Terrorism Act 2008, available at the following link: https://www.legislation.gov.uk/ukpga/2008/28/section/19

([209]) Section 2(2) of the Intelligence Service Act 1994 (see https://www.legislation.gov.uk/ukpga/1994/13/contents) provides that 'The Chief of the Intelligence Service shall be responsible for the efficiency of that Service and it shall be his duty to ensure— (a) that there are arrangements for securing that no information is obtained by the Intelligence Service except so far as necessary for the proper discharge of its functions and that no information is disclosed by it except so far as necessary— (i) for that purpose; (ii) in the interests of national security; (iii) for the purpose of the prevention or detection of serious crime; or (iv) for the purpose of any criminal proceedings; and (b) that the Intelligence Service does not take any action to further the interests of any United Kingdom political party' while Section 2(2) of the Security Service Act 1989 (see https://www.legislation.gov.uk/ukpga/1989/5/contents) provides that 'The Director-General shall be responsible for the efficiency of the Service and it shall be his duty to ensure— (a) that there are arrangements for securing that no information is obtained by the Service except so far as necessary for the proper discharge of its functions or disclosed by it except so far as necessary for that purpose or for the purpose of the prevention or detection of] serious crime or for the purpose of any criminal proceedings]; and (b) that the Service does not take any action to further the interests of any political party; and (c) that there are arrangements, agreed with Director-General of the National Crime Agency, for coordinating the activities of the Service in pursuance of Section 1(4) of this Act with the activities of police forces, the National Crime Agency and other law enforcement agencies'.

([210]) Safeguards and limitations on the powers of the intelligence services are also regulated by the Investigatory Powers Act 2016, which, together with the Regulation of Investigatory Powers Act 2000 for England, Wales and Northern Ireland and the Regulation of Investigatory Powers (Scotland) Act 2000 for Scotland, provide for the legal basis for the use of such powers. However, these powers are not relevant in the context 'onward sharing', since they cover direct collection of personal data by intelligence agencies. For an assessment of the powers granted to the intelligence agencies under the Investigatory Powers Act, see the Commission's Implementing Decision pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by the United Kingdom C(2021) 4800.

(lawfulness, fairness and transparency ([211]); purpose limitation ([212]); data minimisation ([213]); accuracy ([214]); storage limitation ([215]) and security ([216]), imposes conditions on the processing of special categories of data ([217]), provides for data subject rights ([218]), requires data protection by design ([219]) and regulates international transfers of personal data ([220]).

(130) At the same time, Section 110 of the DPA 2018 provides for an exemption from specified provisions in Part 4 of the DPA 2018, when such exemption is required to safeguard national security. Section 110(2) of the DPA 2018 lists the provisions from which an exemption is allowed. It includes the data protection principles (except the principle of lawfulness), the data subject rights, the obligation to inform the Information Commissioner about a data breach, the Information Commissioner's powers of inspection in accordance with international obligations, certain of the Information Commissioner's enforcement powers, the provisions that make certain data protection violations a criminal offence, and the provisions relating to special purposes of processing, such as journalistic, academic or artistic purposes. This exemption can be relied upon on the basis of a case-by-case analysis ([221]). As explained by the United Kingdom authorities and confirmed by the case-law of United Kingdom courts, '(a) controller must consider the actual consequences to national security or defence if they had to comply with the particular data protection provision, and if they could reasonably comply with the usual rule without affecting national security or defence' ([222]). Whether or not the exemption has been used appropriately is subject to the oversight of the ICO ([223]).

([211]) Under Section 86(6) of the DPA 2018, to determine fairness and transparency of the processing, regard is to be had to the method by which data is obtained. In this sense, the fairness and transparency requirement is accomplished if data is obtained from a person who is lawfully authorised or required to supply it.

([212]) Under Section 87 of the DPA 2018, the purposes of the processing must be specified, explicit and legitimate. The data must not be processed in a manner that is incompatible with the purposes for which it is collected. Under the Section 87(3) further compatible processing of personal data can be only allowed if the controller is authorised by law to process the data for that purpose and the processing is necessary and proportionate to that other purpose. The processing should be regarded as compatible, if the processing consists of processing for archiving purposes in the public interest, for purposes of scientific or historical research or for statistical purposes, and is subject to appropriate safeguards (Section 87(4) of the DPA 2018).

([213]) Personal data must be adequate, relevant and not excessive (Section 88 of the DPA 2018).

([214]) Personal data must be accurate and up to date (Section 89 of the DPA 2018).

([215]) Personal data must not be kept longer than is necessary (Section 90 of the DPA 2018).

([216]) The sixth data protection principle is that personal data must be processed in a manner that includes taking appropriate security measures as regards risks that arise from processing personal data. The risks include (but are not limited to) accidental or unauthorised access to, or destruction, loss, use, modification or disclosure of, personal data (Section 91 of the DPA 2018). Section 107 also requires that (1) each controller must implement appropriate security measures appropriate to the risks arising from the processing of personal data; and (2) in the case of automated processing, each controller and each processor implement preventative or mitigative measures based on an evaluation of risk.

([217]) Section 86(2)(b) and Schedule 10 of the DPA 2018.

([218]) Chapter 3 of Part 4 of the DPA 2018, notably the rights: of access, of rectification and deletion, to object to the processing and not to be subject to automated decision making, to intervene in automated decision-making and to be informed about the decision-making. Moreover, the controller must give the data subject information about the processing of their personal data.

([219]) Section 103 of the DPA 2018.

([220]) Section 109 of the DPA 2018. Transfers of personal data to international organisations or countries outside of the United Kingdom are possible if the transfer is a necessary and proportionate measure carried out for the purposes of the controller's statutory functions, or for other purposes provided for in specific Sections of the Security Service Act 1989 and the Intelligence Services Act 1994.

([221]) See case *Baker v Secretary of State for the Home Department* [2001] UKIT NSA2 (*'Baker v Secretary of State'*).

([222]) UK Explanatory Framework for Adequacy Discussions, section H: National Security Data Protection and Investigatory Powers Framework, page 15-16, available at the following link: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/872239/H_-_National_Security.pdf See also *Baker v Secretary of State* (see above footnote 221), in which the Tribunal quashed a national security certificate issued by the Home Secretary and confirming the application of the national security exception, considering that there was no reason to provide for a blanket exception on the obligation to answer access requests and that allowing such exception in all circumstances without a case-by-case analysis exceeded what was necessary and proportionate for the protection of national security.

([223]) See MoU between ICO and UKIC according to which 'Upon the ICO receiving a complaint from a data subject, the ICO will want to satisfy themselves that the issue has been handled correctly, and, where applicable, that the application of any exemption has been used appropriately' (Memorandum of Understanding between Information Commission's Office and the United Kingdom Intelligence Community, paragraph 16, available at the following link: https://ico.org.uk/media/about-the-ico/mou/2617438/uk-intelligence-community-ico-mou.pdf).

(131) Moreover, in relation to the possibility to restrict any of the above-mentioned rights for the protection of 'national security', section 79 of the DPA 2018 provides for the possibility of a controller to apply for a certificate signed by a Cabinet Minister or the Attorney General certifying that a restriction of such rights is, or at any time was, a necessary and proportionate measure to protect national security ([224]). The United Kingdom government has issued guidance on national security certificates under the DPA 2018 that notably highlight that any limitation to data subjects' rights for safeguarding national security must be proportionate and necessary ([225]). All national security certificates must be published on the ICO's website ([226]).

(132) The certificate should be for a fixed duration of no more than five years, so to be regularly reviewed by the executive ([227]). A certificate shall identify the personal data or categories of personal data subject to the exemption as well the provisions of the DPA 2018 to which the exemption applies ([228]).

(133) It is important to note that national security certificates do not provide for an additional ground for restricting data protection rights for national security reasons. In other words, the controller or processor can only rely on a certificate when they have concluded it is necessary to rely on the national security exemption, which must be applied on a case-by-case basis. Even if a national security certificate applies to the matter in question, the ICO can investigate whether or not reliance on the national security exemption was justified in a specific case ([229]).

(134) Any person directly affected by the issuing of the certificate can appeal to the Upper Tribunal ([230]) against the certificate ([231]) or, where the certificate identifies data by means of a general description, challenge the application of the certificate to specific data ([232]).

(135) The tribunal will review the decision to issue a certificate and decide whether there were reasonable grounds for issuing the certificate ([233]). It can consider a wide range of issues, including necessity, proportionality and lawfulness, having regard to the impact on the rights of data subjects and balancing the need to safeguard national security. As a result, the tribunal may determine that the certificate does not apply to specific personal data which is the subject of the appeal ([234]).

([224]) The DPA 2018 has repealed the possibility to issue certificate under Section 28(2) of the Data Protection Act 1998. However, the possibility to issue 'old certificates' still exists to the extent that there is an historic challenge under the 1998 Act (see para. 17 of Part 5 of Schedule 20 of the DPA 2018). However, this possibility seems very rare and will apply only in limited cases, such as, for example, where a data subject brings a challenge on the use of the national security exemption in relation to a processing by a public authority that has carried out its processing under the 1998 Act. It is to be noted that in these cases, Section 28 of the DPA 1998 will apply in its entirety, including therefore the possibility for the data subject to challenge the certificate. At the moment there are no national security certificate issued under the DPA 1998.

([225]) United Kingdom Government Guidance on National Security Certificates under the Data Protection Act 2018, available at the following link: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/910279/Data_Protection_Act_2018_-_National_Security_Certificates_Guidance.pdf

([226]) According to Section 130 of the DPA 2018, the ICO may decide not to publish the text or part of the text of the certificate, if it would be against the interest of national security or would be contrary to the public interest or might jeopardise the safety of any person. In this cases the ICO will however publish the fact that the certificate has been issued.

([227]) United Kingdom Government Guidance on National Security Certificates, paragraph 15, see footnote 225.

([228]) United Kingdom Government Guidance on National Security Certificates, paragraph 5, footnote 225.

([229]) Section 102 of the DPA 2018 requires the controller to be in a position to demonstrate that it has complied with the DPA 2018. This implies that an intelligence service would need to demonstrate to the ICO that when relying on the exemption, it has considered the specific circumstances of the case. The ICO also publishes a record of the national security certificates, which is available at the following link: is available at the following link: https://ico.org.uk/about-the-ico/our-information/national-security-certificates/.

([230]) The Upper Tribunal is the court competent to hear appeals against decisions made by lower administrative tribunals and has specific competence for direct appeals against decisions of certain government bodies.

([231]) Section 111(3) of the DPA 2018.

([232]) Section 111(5) of the DPA 2018.

([233]) In the case *Baker v Secretary of State* (see footnote 221), the information Tribunal quashed a national security certificate issued by the Home Secretary, considering that there was no reason to provide for a blanket exception on the obligation to answer access requests and that allowing such exception in every circumstances without a case-by-case analysis exceeded what was necessary and proportionate for the protection of national security.

([234]) United Kingdom Government Guidance on National Security Certificates, paragraph 25, footnote 225.

(136) A different set of possible restrictions concern those applying, under Schedule 11 of the DPA 2018, to certain provisions of Part 4 of the DPA 2018 ([235]) to safeguard other important objectives of general public interest or protected interests such as, for example, parliamentary privilege, legal professional privilege, the conduct of judicial proceedings or the combat effectiveness of the armed forces. The application of these provisions is either exempted for certain categories of information ('class based'), or exempted to the extent that the application of these provisions would be likely to prejudice the protected interest ('prejudice based') ([236]). Prejudice-based exemptions can only be invoked as far as the application of the listed data protection provision would be likely to prejudice the specific interest in question. The use of an exemption must therefore always be justified by referring to the relevant prejudice that would be likely to occur in the individual case. Class-based exemptions can be invoked only with respect to the specific, narrowly defined category of information for which the exemption is granted. These are similar in purpose and effect to several of the exceptions to the UK GDPR (under Schedule 2 of the DPA 2018) which, in turn, reflect those provided in Article 23 GDPR.

(137) It follows from the above that limitation and conditions are in place under the applicable United Kingdom legal provisions, as also interpreted by the courts and the Information Commission, to ensure that these exemption and restrictions remain within the boundaries of what is necessary and proportionate to protect national security.

(138) The processing of personal data carried out by the intelligence services under Part 4 of the DPA 2018 is overseen by the Information Commissioner ([237]).

(139) The general functions of the Information Commissioner in relation to the processing of personal data by intelligence services under Part 4 of the DPA 2018 are laid down in Schedule 13 to the DPA 2018. The tasks include, but are not limited to, in particular, monitoring and enforcement of Part 4 of the DPA 2018, promoting public awareness, advising Parliament, the government and other institutions on legislative and administrative measures, promoting the awareness of controllers and processors of their obligations, providing information to a data subject concerning the exercise of the data subject's rights, and conducting investigations

(140) The Commissioner, as for Part 3 of the DPA 2018, has the power to notify controllers of an alleged infringement and to issue warnings that a processing is likely to infringe the rules, and issues reprimands when the infringement is confirmed. It can also issue enforcement and penalty notices for violations of certain provision of the act ([238]). However, differently than for other parts of the DPA 2018, the Commissioner cannot give an assessment notice to a national security ([239]).

(141) Moreover, Section 110 of the DPA 2018 provides an exception to the use of certain powers of the Commissioner when this is required for the purposes of safeguarding national security. This includes the power of the Commissioner to issue (any type of) notices under the DPA (information, assessment, enforcement and penalty notices), the power to carry out inspections in accordance with international obligations, the powers of entry and

([235]) This includes: (i) the Part 4 data protection principles, except for the lawfulness of processing requirement under the first principle and the fact that the processing must meet one of the relevant conditions set out in Schedules 9 and 10; (ii) the rights of data subjects; and (iii) the duties relating to reporting breaches to the ICO.

([236]) According to UK Explanatory Framework the exceptions that are 'class based' are: (i) information about the conferring of Crown honours and dignities; (ii) legal professional privilege; (iii) confidential employment, training or education references; and (iv) exam scripts and marks. The 'prejudice based' exceptions concern the following matters: (i) prevention or detection of crime; apprehension and prosecution of offenders; (ii) parliamentary privilege; (iii) judicial proceedings; (iv) the combat effectiveness of the armed forces of the Crown; (v) the economic well-being of the United Kingdom; (vi) negotiations with the data subject; (vii) scientific or historical research, or statistical purposes; (viii) archiving in the public interest. UK Explanatory Framework for Adequacy Discussions, section H: National Security, page 13, see footnote 222.

([237]) Section 116 of the DPA 2018.

([238]) Pursuant to a combined reading of Section 149(2) and Section 155 of the DPA 2018, enforcement and penalty notices may be issued to a controller or processor in relation to violations of Chapter 2 of Part 4 of the DPA 2018 (principles of processing), a provision of Part 4 of the DPA 2018 conferring rights on a data subject, a requirement to communicate a personal data breach to the Commissioner under Section 108 of the DPA 2018, and the principles for transfers of personal data to third countries, non-Convention countries and international organisations in Section 109 of the DPA 2018. (For further details on enforcement and penalty notice see, recitals 102 to 103).

([239]) Under Section 147(6) of the DPA 2018, the Information Commissioner may not give an assessment notice to a body specified in Section 23(3) of the Freedom of Information Act 2000. That includes the Security Service (MI5), the Secret Intelligence Service (MI6) and the Government Communications Headquarter.

inspection, and the rules on offences ([240]). As explained in recital 136, these exceptions will apply only if necessary and proportionate and on case-by-case basis. The application of these exceptions can be subject to a judicial review ([241]).

(142) The ICO and United Kingdom intelligence services have signed a Memorandum of Understanding ([242]) that establishes a framework for cooperation on a number of issues, including data breach notifications and the handling of data subjects complaints. In particular, it provides that upon receiving a complaint, the ICO will assess whether any national security exemption has been invoked appropriately. Responses to queries made by the ICO in the context of the examination of individual complaints have to be given within 20 working days by the concerned United Kingdom Government Guidance on National Security Certificates under the Data Protection Act, using appropriate secure channels if it involves classified information. From April 2018 to date, the ICO has received 21 complaints from individuals about the intelligence services. Each complaint was assessed and the outcome was communicated to the data subject ([243]).

(143) Moreover, the Intelligence and Security Committee (ISC) carries out parliamentary oversight over data processing by intelligence agencies. This Committee has its statutory basis in the Justice and Security Act 2013 (JSA 2013) ([244]). The Act establishes the ISC as a committee of the United Kingdom Parliament. The ISC consists of members belonging to either House of the Parliament and appointed by the Prime Minister after consulting the leader of the opposition ([245]). The ISC is required to make an annual report to Parliament on the discharge of its functions and other reports that it considers appropriate ([246]).

(144) Since 2013, the ISC has been provided with greater powers including the oversight of operational activities of security services. Under Section 2 of the JSA 2013, the ISC has the task to oversee the expenditure, administration, policy and operations of national security agencies. The JSA 2013 specifies that the ISC is able to conduct

([240]) The provisions that can be exempted are: Section 108 (communication of a personal data breach to the Commissioner), Section 119 (inspection in accordance with international obligations); Sections 142 to 154 and Schedule 15 (Commissioner's notices and powers of entry and inspection); and Sections 170 to 173 (offences relating to personal data). In addition in relation to processing by the intelligence services in Schedule 13 (other general functions of the Commissioner), paragraphs 1(a) and (g) and 2.

([241]) See for example case *Baker v Secretary of State for the Home Department* (see footnote 221).

([242]) Memorandum of Understanding between ICO and United Kingdom Intelligence Community, see footnote 231.

([243]) In seven of these cases, the ICO advised the complainant to raise the concern with the data controller (this is the case when an individual has raised a concern with the ICO, but should have first raised it with the data controller), in one of these cases, the ICO provided general advice to the data controller (this is used when the actions of the controller do not appear to have breached the legislation, but an improvement of the practices may have avoided the concern being raised with the ICO), and in the other 13 cases, there was no action required from the data controller (this is used when concerns raised by the individual do fall under the Data Protection Act 2018 because they concern the processing of personal information, but based on the information provided the controller does not appear to have breached the legislation).

([244]) As explained by United Kingdom authorities, the JSA expanded the remit of ISC to include a role in overseeing intelligence community beyond the three agencies and allowing retrospective oversight of the operational activities of the Agencies on matters of significant national interest.

([245]) Section 1 of the JSA 2013. Ministers are not eligible for members. Members hold their position on the ISC for the duration of the Parliament during which they were appointed. They can be removed by a resolution of the House by which they were appointed, or if they cease to be an MP, or they become a Minister. A member may also resign.

([246]) Reports and statements of the Committee are available online at the following link: http://isc.independent.gov.uk/committee-reports In 2015 the ISC issued a report on 'Privacy and Security: A modern and transparent legal framework' (see: https://b1cba9b3-a-5e6631fd-s-sites.googlegroups.com/a/independent.gov.uk/isc/files/20150312_ISC_P%2BS%2BRpt%28web%29.pdf) in which it considered the legal framework for surveillance techniques used by the intelligence agencies and issued a series of recommendation that were then considered and integrated in the draft Investigatory Powers Bill that was converted into law, the IPA 2016. The government's answer to the Privacy and Security report is available at the following link: https://b1cba9b3-a-5e6631fd-s-sites.googlegroups.com/a/independent.gov.uk/isc/files/20151208_Privacy_and_Security_Government_Response.pdf

investigations on operational matters when they do not relate to ongoing operations ([247]). The Memorandum of Understanding agreed between the Prime Minister and the ISC ([248]) specifies in detail the elements to be taken into account when considering whether an activity is not part of any ongoing operation ([249]). The ISC can also be asked to investigate ongoing operations by the Prime Minister and can review information voluntarily provided by the agencies.

(145) Under Schedule 1 of the JSA 2013 the ISC may ask the heads of any of the three intelligence services to disclose any information. The agency must make such information available, unless the Secretary of State vetoes it ([250]). The United Kingdom authorities explained that in practice very little information is withheld from the ISC ([251]).

(146) With respect to redress, first of all, under Section 165(2) of the DPA 2018, a data subject may bring a complaint before the ICO if he or she believes that, in connection to personal data relating to him or her, there is a violation of Part 4 of the DPA 2018, including any abusive use of the national security derogations and restrictions.

(147) Moreover, under Part 4 of the DPA 2018, individuals are entitled to apply to the High Court (or Court of Session in Scotland) for an order requiring the controller to comply with the rights of access to data ([252]), to object to processing ([253]) and to rectification or erasure.

(148) Individuals are also entitled to seek compensation for damage suffered due to a contravention of a requirement of Part 4 of the DPA 2018 from the controller or a processor ([254]). Damage includes both financial loss and damage not involving financial loss, such as distress ([255]).

(149) Finally, an individual can submit a complaint to the Investigatory Powers Tribunal for any conduct by or on behalf of the United Kingdom intelligence agencies ([256]).The Investigatory Powers Tribunal (IPT) is established by the Regulation of Investigatory Powers Act 2000 for England, Wales and Northern Ireland and the Regulation of Investigatory Powers (Scotland) Act 2000 for Scotland (RIPA 2000) and is independent from the executive ([257]). In accordance with Section 65 of the RIPA 2000, the members of the IPT are appointed by Her Majesty for a period of five years.

(150) A member of the Tribunal may be removed from office by Her Majesty on an Address ([258]) by both Houses of Parliament ([259]).

(151) To bring an action before the IPT ('standing requirement'), according to Section 65 of the RIPA 2000, an individual has to believe (i) that the conduct of an intelligence service has taken place in relation to him, any of his property, any communications sent by or to him, or intended for him, or his use of any postal service, telecommunications service or telecommunications system ([260]), and (ii) that the conduct has taken place in 'challengeable

([247]) Section 2 of the JSA 2013.
([248]) Memorandum of Understanding between the Prime Minister and the ISC, available at the following link: http://data.parliament.uk/DepositedPapers/Files/DEP2013-0415/AnnexA-JSBill-summaryofISCMoU.pdf
([249]) Memorandum of Understanding between the Prime Minister and the ISC, para 14, see footnote 248.
([250]) The Secretary of State may only veto disclosure of information on two grounds: the information is sensitive and should not be disclosed to the ISC in the interests of national security; or it is information of such a nature that, if the Secretary of State were requested to produce it before a Departmental Select Committee of the House of Commons, the Secretary of State would consider (on grounds not limited to national security) it proper not to do so. (Schedule 1 paragraph 4(2) of the JSA 2013).
([251]) UK Explanatory Framework – section H: National Security, p. 43.
([252]) Section 94(11) of the DPA 2018.
([253]) Section 99(4) of the DPA 2018.
([254]) Section 169 of the DPA 2018, which allows claims from 'A person who suffers damage by reason of a contravention of a requirement of the data protection legislation'.
([255]) Section 169(5) of the DPA 2018.
([256]) See Section 65(2)(b) of the RIPA.
([257]) Under Schedule 3 to the RIPA 2000, the members must have specified judicial experience and are eligible for reappointment.
([258]) On the notion of 'Address', see footnote 183.
([259]) Schedule 3 paragraph 1(5) to the RIPA 2000.
([260]) Section 65(4) of the RIPA 2000.

circumstances' ([261]) or 'been carried out by or on behalf of the intelligence services ([262]). As in particular this 'belief' standard has been interpreted quite broadly ([263]), bringing a case before the Tribunal is subject to relatively low standing requirements.

(152) Where the Tribunal considers a complaint made to them, it is the duty of the Tribunal to investigate whether the persons against whom any allegation is made in the complaint have engaged in relation to the complainant as well as to investigate the authority that has allegedly engaged in the violations and whether the alleged conduct has taken place ([264]). Where the Tribunal hears any proceedings, it must apply the same principles for making their determination in those proceedings as would be applied by a court on an application for judicial review ([265]).

(153) The Tribunal must give notice to the complainant whether there has been determination in his or her favour or not ([266]). Under Section 67(6) and (7) of the RIPA 2000, the Tribunal has the power to issue interim orders and to provide any such award of compensation or other order as it thinks fit ([267]). According to Section 67A of the RIPA 2000, a determination of the Tribunal can be appealed, subject to leave granted by the Tribunal or relevant appellate court.

(154) In particular, individuals can bring a claim – and obtain redress – before the IPT in case where they consider that a public authority has acted (or proposes to act) in a way which is incompatible with a ECHR rights, including the right to privacy and data protection, and is consequently unlawful under Section 6(1) of the Human Rights Act 1998. The IPT that has been granted exclusive jurisdiction for all Human Rights Act claims in relation to the intelligence agencies. This means, as noted by the High Court, 'whether there has been a breach of the HRA on the facts of a particular case is something that can in principle be raised and adjudicated by an independent tribunal which can have access to all relevant material, including secret material. […] We also bear in mind in this context that the IPT is itself now subject to the possibility of an appeal to an appropriate appellate court (in England and Wales that would be the Court of Appeal); and that the Supreme Court has recently decided that the IPT is in principle amenable to judicial review: see R (Privacy International) v Investigatory Powers Tribunal [2019] UKSC 22; [2019] 2 WLR 1219' ([268]). If the IPT finds any act of a public authority to be unlawful, it can grant such relief or remedy, or make such order, within its powers as it considers just and appropriate ([269]).

([261]) Such circumstances refer to conduct of public authorities taking place with authority (e.g. an warrant, an authorisation/notice for the acquisition of communications, etc.), or if the circumstances are such that (whether or not there is such authority) it would not have been appropriate for the conduct to take place without it, or at least without proper consideration having been given to whether such authority should be sought. Conduct authorised by a Judicial Commissioner are considered as to have taken place in challengeable circumstance (Section 65 (7ZA) of the RIPA 2000) while other conducts that take place with the permission of a person holding judicial office are considered not to have taken place in challengeable circumstance (Section 65(7) and (8) of the RIPA 2000).

([262]) According to the information provided by United Kingdom authorities, the low threshold for making a complaint determines that it is not unusual for the Tribunal's investigation to determine that the complainant was in fact never subject to investigation by a public authority. The latest Statistical Report of the IPT specifies that in 2016 the Tribunal received 209 complaints, 52 % of those were considered frivolous or vexatious and 25 % received a 'no determination' outcome. United Kingdom authorities explained that this either means that no covert activity/powers were used in relation to the complainant, or that covert techniques were used and the Tribunal determined that the activity was lawful. Additionally, 11 % were ruled out of jurisdiction, withdrawn or not valid, 5 % were ruled out of time, 7 % were found in favour of the complainant. Statistical Report of the Investigatory Powers Tribunal 2016, available at the following link: https://www.ipt-uk.com/docs/IPT%20Statisical%20Report%202016.pdf

([263]) See case *Human Rights Watch v Secretary of State* [2016] UKIPTrib15_165-CH. In this case, the IPT, by referring to the ECtHR case-law, held that the appropriate test in respect of the belief that any conduct falling within Subsection 68(5) of RIPA 2000 has been carried out by or on behalf of any of the intelligence services is whether there is any basis for such belief, including the fact that an individual may claim to be a victim of a violation occasioned by the mere existence of secret measures or legislation permitting secret measures, only if he is able to show that due to his personal situation, he is potentially at risk of being subjected to such measures (see *Human Rights Watch v Secretary of State*, paragraph 41).

([264]) Section 67(3) of the RIPA 2000.

([265]) Section 67(2) of the RIPA 2000.

([266]) Section 68(4) of the RIPA 2000.

([267]) This may include an order requiring the destruction of any records of information held by any public authority in relation to any person.

([268]) High Court of Justice, *Liberty*, [2019] EWHC 2057 (Admin), paragraph 170.

([269]) Section 8(1) of the Human Rights Act 1998.

(155) After exhausting national remedies, an individual can obtain redress before the European Court of Human Rights for violations of the rights guaranteed under the ECHR, including the right to privacy and data protection.

(156) It follows from the above that the sharing by United Kingdom criminal law enforcement authorities of data transferred under this Decision with other public authorities, including intelligence agencies, is framed by limitations and conditions ensuring that such onward sharing will be necessary and proportionate and subject to specific data protection safeguards under the DPA 2018. Moreover, processing of data by the concerned public authorities is overseen by independent bodies and affected individuals have access to effective judicial remedies.

3. **CONCLUSION**

(157) The Commission considers that Part 3 of the DPA 2018 ensures a level of protection for personal data transferred for criminal law enforcement purposes from competent authorities in the Union to United Kingdom competent authorities which is essentially equivalent to the one guaranteed by Directive (EU) 2016/680.

(158) Moreover, the Commission considers that, taken as a whole, the oversight mechanisms and redress avenues in United Kingdom law enable infringements to be identified and sanctioned in practice and offer legal remedies to the data subject to obtain access to personal data relating to him/her and, eventually, the rectification or erasure of such data.

(159) Finally, on the basis of the available information about the United Kingdom legal order, the Commission considers that any interference with the fundamental rights of the individuals whose personal data are transferred from the European Union to the United Kingdom by United Kingdom public authorities for public interest purposes, including in the context of the sharing of personal data between law enforcement authorities and other public authorities such as national security bodies, will be limited to what is strictly necessary to achieve the legitimate objective in question, and that effective legal protection against such interference exists.

(160) Therefore, it should be decided that the United Kingdom ensures an adequate level of protection within the meaning of Article 36(2) of Directive (EU) 2016/680, interpreted in light of the Charter of Fundamental Rights.

(161) This conclusion is based on both the relevant United Kingdom domestic regime and its international commitments, in particular adherence to the European Convention of Human Rights and submission to the jurisdiction of the European Court of Human Rights. Continued adherence to such international obligations is therefore a particularly important element of the assessment on which this Decision is based.

4. **EFFECTS OF THIS DECISION AND ACTION OF DATA PROTECTION AUTHORITIES**

(162) Member States and their organs are required to take the measures necessary to comply with acts of the Union institutions, as the latter are presumed to be lawful and accordingly produce legal effects until such time as they expire, are withdrawn, annulled in an action for annulment or declared invalid following a reference for a preliminary ruling or a plea of illegality.

(163) Consequently, a Commission adequacy decision adopted pursuant to Article 36(3) of Directive (EU) 2016/680 is binding on all organs of the Member States to which it is addressed, including their independent supervisory authorities. In particular, during the period of application of this Decision, transfers from a controller or processor in the Union to controllers or processors in the United Kingdom may take place without the need to obtain any further authorisation.

(164) At the same time, it should be recalled that, pursuant to Article 47(5) of Directive (EU) 2016/680, and as explained by the Court of Justice in the *Schrems* judgment, where a national data protection authority questions, including upon a complaint, the compatibility of a Commission adequacy decision with the fundamental rights of the individual to privacy and data protection, national law must provide it with a legal remedy to put those objections before a national court, which may be required to make a reference for a preliminary ruling to the Court of Justice ([270]).

([270]) *Schrems*, paragraph 65.

5. MONITORING, SUSPENSION, REPEAL OR AMENDMENT OF THIS DECISION

(165) Pursuant to Article 36(4) of Directive (EU) 2016/680, the Commission is to monitor, on an ongoing basis, relevant developments in the United Kingdom after the adoption of this Decision in order to assess whether it still ensures an essentially equivalent level of protection. Such monitoring is particular important in this case, as the United Kingdom will administer, apply and enforce a new data protection regime no longer subject to Union law, which may be liable to evolve. In that respect, special attention will be paid to the application in practice of the United Kingdom rules on transfers of personal data to third countries, including through the conclusion of international agreements, and the impact it may have on the level of protection afforded to data transferred under this Decision; as well as to the effectiveness of the exercise of individual rights in the areas covered by this Decision. Amongst other elements, case-law developments and oversight by the ICO and other independent bodies will inform the Commission's monitoring.

(166) In order to facilitate this monitoring, the United Kingdom authorities should promptly and regularly inform the Commission of any material change to the United Kingdom legal order that has an impact on the legal framework that is the object of this Decision, as well as any evolution in practices related to the processing of the personal data assessed in this Decision, in particular with respect to the elements mentioned in recital 165.

(167) Moreover, in order to allow the Commission to effectively carry out its monitoring function, the Member States should inform the Commission about any relevant action undertaken by the national data protection authorities, in particular regarding queries or complaints by EU data subjects concerning the transfer of personal data from the Union to competent authorities in the United Kingdom. The Commission should also be informed about any indications that the actions of United Kingdom public authorities responsible for the prevention, investigation, detection or prosecution of criminal offences, including any oversight bodies, do not ensure the required level of protection.

(168) Where available information, in particular information resulting from the monitoring of this Decision or provided by United Kingdom or Member States' authorities, reveals that the level of protection afforded by the United Kingdom may no longer be adequate, the Commission should promptly inform the competent United Kingdom authorities thereof and request that appropriate measures be taken within a specified timeframe, which may not exceed three months. Where necessary, this period may be extended for a specified period of time, taking into account the nature of the issue at stake and/or of the measures to be taken.

(169) If, at the expiry of that specified timeframe, the competent United Kingdom authorities fail to take those measures or otherwise demonstrate satisfactorily that this Decision continues to be based on an adequate level of protection, the Commission will initiate the procedure referred to in Article 58(2) of the Directive (EU) 2016/680 with a view to partially or completely suspend or repeal this Decision.

(170) Alternatively, the Commission will initiate this procedure with a view to amend the Decision, in particular by subjecting data transfers to additional conditions or by limiting the scope of the adequacy finding only to data transfers for which an adequate level of protection continues to be ensured.

(171) On duly justified imperative grounds of urgency, the Commission will make use of the possibility to adopt, in accordance with the procedure referred to in Article 58(3) of the Directive (EU) 2016/680, immediately applicable implementing acts suspending, repealing or amending the Decision.

6. DURATION AND RENEWAL OF THIS DECISION

(172) It should be taken into account that, with the end of the transition period provided by the Withdrawal Agreement and as soon as the interim provision under Article 782 of the EU-UK Trade and Cooperation Agreement will cease to apply, the United Kingdom will administer, apply and enforce a new data protection regime compared to the one in place when it was bound by European Union law. This may notably involve amendments or changes to the data protection framework assessed in this Decision, as well as other relevant developments.

(173) It is therefore appropriate to provide that this Decision will apply for a period of four years as of its entry into force.

(174) Where in particular information resulting from the monitoring of this Decision reveals that the findings relating to the adequacy of the level of protection ensured in the United Kingdom are still factually and legally justified, the Commission should, at the latest six months before this Decision ceases to apply, initiate the procedure to amend this Decision by extending its temporal scope, in principle, for an additional period of four years Any such implementing act amending this Decision is to be adopted in accordance with the procedure referred to in Article 58(2) of Directive (EU) 2016/680.

7. **FINAL CONSIDERATIONS**

(175) The European Data Protection Board published its opinion ([271]), which has been taken into consideration in the preparation of this Decision.

(176) The measures provided for in this Decision are in accordance with the opinion of the Committee established under Article 58 of Directive (EU) 2016/680.

(177) In accordance with Article 6a of Protocol No 21 on the position of the United Kingdom and Ireland in respect of the area of freedom, security and justice, as annexed to the TEU and to the TFEU, Ireland is not bound by the rules laid down in Directive (EU) 2016/680, and hence this implementing decision, which relate to the processing of personal data by the Member States when carrying out activities which fall within the scope of Chapter 4 or Chapter 5 of Title V of Part Three of the TFEU where Ireland is not bound by the rules governing the forms of judicial cooperation in criminal matters or police cooperation which require compliance with the provisions laid down on the basis of Article 16 TFEU. Moreover, by virtue of Council Implementing Decision (EU) 2020/1745 ([272]), Directive (EU) 2016/680 is to be put into effect and applied on a provisional basis in Ireland as of 1 January 2021. Ireland is therefore bound by this Implementing Decision, under the same conditions as apply to the application of Directive (EU) 2016/680 in Ireland as set out in Implementing Decision (EU) 2020/1745, as regards the Schengen *acquis* it participates in.

(178) In accordance with Articles 2 and 2a of Protocol No 22 on the position of Denmark, annexed to the Treaty on European Union and to the Treaty on the Functioning of the European Union, Denmark is not bound by the rules laid down in Directive (EU) 2016/680, and hence this Implementing Decision, or subject to their application which relate to the processing of personal data by the Member States when carrying out activities which fall within the scope of Chapter 4 or Chapter 5 of Title V of Part Three of the TFEU. However, given that Directive (EU) 2016/680 builds upon the Schengen *acquis*, Denmark, in accordance with Article 4 of that Protocol, notified on 26 October 2016 its decision to implement Directive (EU) 2016/680. Denmark is therefore bound under international law to implement this Implementing Decision.

(179) As regards Iceland and Norway, this Implementing Decision constitutes a development of provisions of the Schengen *acquis*, as provided for by the Agreement concluded by the Council of the European Union and the Republic of Iceland and the Kingdom of Norway concerning the association of those two States with the implementation, application and development of the Schengen *acquis* ([273]).

(180) As regards Switzerland, this Implementing Decision constitutes a development of provisions of the Schengen *acquis*, as provided for by the Agreement between the European Union, the European Community and the Swiss Confederation concerning the association of the Swiss Confederation with the implementation, application and development of the Schengen *acquis* ([274]).

(181) As regards Liechtenstein, this Implementing Decision constitutes a development of provisions of the Schengen *acquis*, as provided for by the Protocol between the European Union, the European Community, the Swiss Confederation and the Principality of Liechtenstein on the accession of the Principality of Liechtenstein to the Agreement between the European Union, the European Community and the Swiss Confederation on the Swiss Confederation's association with the implementation, application and development of the Schengen *acquis* ([275]),

([271]) Opinion 15/2021 regarding the European Commission draft implementing decision pursuant to Directive (EU) 2016/680 on the adequate protection of personal data in the United Kingdom, available at the following link: https://edpb.europa.eu/our-work-tools/our-documents/opinion-led/opinion-152021-regarding-european-commission-draft_en

([272]) Council Implementing Decision (EU) 2020/1745 of 18 November 2020 on the putting into effect of the provisions of the Schengen *acquis* on data protection and on the provisional putting into effect of certain provisions of the Schengen *acquis* in Ireland (OJ L 393, 23.11.2020, p. 3).

([273]) OJ L 176, 10.7.1999, p. 36.

([274]) OJ L 53, 27.2.2008, p. 52.

([275]) OJ L 160, 18.6.2011, p. 21.

HAS ADOPTED THIS DECISION:

Article 1

For the purposes of Article 36 of Directive (EU) 2016/680, the United Kingdom ensures an adequate level of protection for personal data transferred from the European Union to United Kingdom public authorities responsible for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties.

Article 2

Whenever the competent supervisory authorities in Member States, in order to protect individuals with regard to the processing of their personal data, exercise their powers pursuant to Article 47 of Directive (EU) 2016/680 with respect to data transfers to public authorities in the United Kingdom within the scope of application set out in Article 1, the Member State concerned shall inform the Commission without delay.

Article 3

1. The Commission shall continuously monitor the application of the legal framework upon which this Decision is based, including the conditions under which onward transfers are carried out and individual rights are exercised, with a view to assessing whether the United Kingdom continues to ensure an adequate level of protection within the meaning of Article 1.

2. The Member States and the Commission shall inform each other of cases where the Information Commissioner, or any other competent United Kingdom authority, fails to ensure compliance with the legal framework upon which this Decision is based.

3. The Member States and the Commission shall inform each other of any indications that interferences by United Kingdom public authorities with the right of individuals to the protection of their personal data go beyond what is strictly necessary, or that there is no effective legal protection against such interferences.

4. Where the Commission has indications that an adequate level of protection is no longer ensured, the Commission shall inform the competent United Kingdom authorities and may suspend, repeal or amend this Decision.

5. The Commission may suspend, repeal or amend this Decision if the lack of cooperation of the government of the United Kingdom prevents the Commission from determining whether the finding in Article 1 is affected.

Article 4

This Decision shall expire on 27 June 2025, unless extended in accordance with the procedure referred to in Article 58(2) of Directive (EU) 2016/680.

Article 5

This Decision is addressed to the Member States.

Done at Brussels, 28 June 2021.

For the Commission
Didier REYNDERS
Member of the Commission