EUROPEAN
COMMISSION

Brussels, XXX
[…](2021) XXX draft



**COMMISSION IMPLEMENTING DECISION**

**of XXX**

**pursuant Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by the United Kingdom**

(Text with EEA relevance)

**COMMISSION IMPLEMENTING DECISION**

**of XXX**

**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**

(Text with EEA relevance)

THE EUROPEAN COMMISSION,

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

Having regard to 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) ('Regulation (EU) 2016/679')[1] , and in particular Article 45(3) thereof,

Whereas:

## 1. INTRODUCTION

(1) Regulation (EU) 2016/679 sets out the rules for the transfer of personal data from controllers or processors in the European 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 are laid down in Chapter V of that Regulation, that is in Articles 44 to 50. While the flow of personal data to and from countries outside the European Union is essential for the expansion of international cooperation and cross-border trade, the level of protection afforded to personal data in the European Union must not be undermined by transfers to third countries[2].

(2) Pursuant to Article 45(3) of Regulation (EU) 2016/679, 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, as provided for in Article 45(1) and recital 103 of that Regulation.

(3) As specified in Article 45(2) of Regulation (EU) 2016/679, the adoption of an adequacy decision has to be based on a comprehensive analysis of the third country's legal order, covering both the rules applicable to the data importers and the limitations and safeguards as regards access to personal data by public authorities. 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 104 of Regulation (EU) 2016/679). The standard against which the "essential equivalence" is assessed is that set by European Union

[1] OJ L 119, 4.5.2016, page 1.

[2] See recital 101 of Regulation (EU) 2016/679.

legislation, notably Regulation (EU) 2016/679, 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 data protection rights and their effective implementation, supervision and enforcement, the foreign system as a whole delivers the required level of protection[7].

(5) The Commission has carefully analysed the law and practice of the United Kingdom. Based on the findings developed in recitals (7) to (264), the Commission concludes that the United Kingdom ensures an adequate level of protection for personal data transferred within the scope of Regulation (EU) 2016/679 from the European Union to the United Kingdom.

(6) This Decision should not affect the direct application of Regulation (EU) 2016/679 to organisations established in the United Kingdom where the conditions regarding the territorial scope of that Regulation, laid down in its Article 3, are fulfilled.

## 2. RULES APPLYING TO THE PROCESSING OF PERSONAL DATA

### 2.1. The constitutional framework

(7) The UK is a Parliamentary democracy which has a constitutional sovereign as Head of State. 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 which are responsible for scrutinising the Government and debating and passing laws.

(8) The UK Parliament has devolved responsibility to the Scottish Parliament, the Welsh Parliament (Senedd Cymru), and the Northern Ireland Assembly for legislating on domestic matters in Scotland, Wales and Northern Ireland which the UK Parliament has not reserved to itself. While data protection is a reserved matter, 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, of Scotland and Northern Ireland are devolved to the Scottish Parliament and Northern Ireland Assembly, respectively. The United Kingdom does not have a codified

---

3 See, most recently, Case C-311/18, *Facebook Ireland and Schrems* ("*Schrems II*") ECLI:EU:C:2020:559.

4 European Data Protection Board, Adequacy Referential, WP 254 rev. 01.available at the following link: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614108

5 Case C-362/14, *Schrems* ("*Schrems I"*), ECLI:EU:C:2015:650, paragraph 73.

6 *Schrems I*, paragraph 74.

7 See 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, pages 6-7, available at the following link: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017DC0007&from=EN

constitution in the sense of an entrenched constitutive document. Constitutional principles have emerged over time, drawn from case law and convention in particular. The constitutional value of certain statutes, such as the Magna Carta, the Bill of Rights 1689 and the Human Rights Act 1998 has been recognised by courts. The fundamental rights of individuals have been developed, as part of the constitution, through common law, those statutes, and international treaties, in particular the European Convention on Human Rights 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[8].

(9) The Human Rights Act 1998 incorporates the rights contained in the European Convention on Human Rights into the law of the United Kingdom. The Human Rights Act grants any individual the fundamental rights and freedoms provided in Articles 2 to 12 and 14 of the European Convention on Human Rights, Articles 1, 2 and 3 of its First Protocol and Article 1 of its Thirteenth Protocol, as read in conjunction with Articles 16, 17 and 18 of that Convention. This includes the right to respect for private and family life (and the right to data protection as part of that right) and the right to a fair trial[9]. In particular, pursuant to Article 8 of that Convention, 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.

(10) In accordance with the Human Rights Act 1998, any action of public authorities must be compatible with a Convention Right[10]. In addition, primary and subordinate legislation must be read and given effect in a way that is compatible with the Convention rights[11].

### 2.2. The data protection framework of the United Kingdom

(11) The United Kingdom withdrew from the European 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[12], 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 consisted of the relevant EU legislation (in particular Regulation (EU) 2016/679 and Directive (EU) 2016/680 of the European Parliament and of the

---

8 The principles of Convention 108 were originally implemented into the law of the United Kingdom through the Data Protection Act of 1984, which was 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.

9 Articles 6 and 8 of the ECHR (see also Schedule 1 to the Human Rights Act 1998).

10 Section 6 of the Human Rights Act 1998.

11 Section 3 of the Human Rights Act 1998.

12 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 384I, 12.11.2019, p. 1), available at the following link: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:12019W/TXT(02)&from=EN

Council[13]) and national legislation, in particular the Data Protection Act 2018 (DPA 2018)[14] which provided national rules, where allowed by Regulation (EU) 2016/679, specifying and restricting the application of the rules of Regulation (EU) 2016/679 and transposed Directive (EU) 2016/680.

(12) To prepare for EU withdrawal, the United Kingdom Government enacted the European Union (Withdrawal) Act 2018[15], which incorporates directly applicable Union legislation into the law of the United Kingdom[16]. This so-called "retained EU law" includes Regulation (EU) 2016/679 in its entirety (including its recitals)[17]. In accordance with the that act, the unmodified retained EU law must be interpreted by the courts of the United Kingdom in accordance with the relevant case law of the European Court of Justice and general principles of Union law as they have effect immediately before the end of the transition period (called "retained EU case law" and "retained general principles of EU law" respectively)[18].

(13) Under the European Union (Withdrawal) Act 2018, the ministers of the United Kingdom have the power to introduce secondary legislation, via statutory instruments, to make the necessary modifications to retained European Union law consequential to the United Kingdom's withdrawal from the European Union. The Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019 (DPPEC Regulations) exercise this power[19]. They amend Regulation (EU) 2016/679 as brought into UK law through the European Union (Withdrawal) Act 2018, the DPA 2018, and other data protection legislation to fit the domestic context[20].

---

13 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 (OJ L 119, 4.5.2016, pages 89), available at the following link: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L0680&from=EN .

14 Data Protection Act 2018, available at the following link: https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted

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

16 The intention and effect of the European Union (Withdrawal) Act 2018 is that all direct Union legislation which was incorporated into United Kingdom law at the end of the transition period is incorporated into United Kingdom law as it has effect in EU law immediately before the end of the transition period, see Section 3 of the European Union (Withdrawal) Act 2018.

17 The Explanatory Notes to the European Union (Withdrawal) Act 2018 specifies that: "Where legislation is converted under this Section, it is the text of the legislation itself which will form part of domestic legislation. This will include the full text of any EU instrument (including its recitals)". (Explanatory Notes to the European Union (Withdrawal) Act 2018, paragraph 83, available at the following link: https://www.legislation.gov.uk/ukpga/2018/16/pdfs/ukpgaen_20180016_en.pdf). According to information provided by the UK authorities, as the recitals do not have the status of binding legal rules, it was not necessary to amend them in the same way as the Articles of Regulation (EU) 2016/679 have been amended by the DPPEC Regulations.

18 Section 6 of the European Union (Withdrawal) Act 2018.

19 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 the DPPEC Regulations 2020, available at the following link: https://www.legislation.gov.uk/ukdsi/2020/9780348213522

20 These amendments to the UK GDPR and DPA 2018 are mostly of a technical nature, such as deleting references to "Member States" or adjusting terminology, e.g. replacing references to Regulation (EU) 2016/679 by references to the UK GDPR. In some instances, changes were required in order to reflect

(14) Consequently, the legal framework on the protection of personal data in the United Kingdom after the end of the transition period consists of:

– the United Kingdom General Data Protection Regulation (UK GDPR), as incorporated into the law of the United Kingdom under the European Union (Withdrawal) Act 2018 and amended by the DPPEC Regulations[21], and

– the DPA 2018, as amended by the DPPEC Regulations[22].

(15) As the UK GDPR is based on retained EU legislation, the data protection rules in the United Kingdom in many aspects closely mirror the corresponding rules applicable within the European Union.

(16) In addition to the powers afforded to the Secretary of State by the European Union (Withdrawal) Act 2018, several provisions of the DPA 2018 give powers to the Secretary of State to adopt secondary legislation to amend certain provisions of the Act or provide supplementary and additional rules[23]. The Secretary of State has so far only exercised the power under Section 137 of the DPA 2018 to adopt the Data Protection (Charges and Information) (Amendment) Regulations 2019, which set out the circumstances in which data controllers are required to pay an annual charge to the UK's independent data protection authority, the Information Commissioner.

(17) Finally, further guidance on the data protection legislation of the United Kingdom is provided in the codes of practice and other guidance adopted by the Information Commissioner. Although not formally legally binding, this guidance carries interpretative weight and demonstrates how the data protection legislation applies and is enforced by the Commissioner in practice. In particular, Sections 121-125 of the DPA 2018 require the Commissioner to prepare codes of practice on data-sharing, direct marketing, age-appropriate design and data protection and journalism.

(18) In its structure and main components, the UK legal framework applying to data transferred under this Decision is thus very similar to the one applying in the European Union. 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 UK 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

---

the purely domestic context of the provisions, for example with respect to "who" adopts "adequacy regulations" for the purposes of the UK's data protection legislative framework (see Section 17A of the DPA 2018), i.e. the Secretary of State instead of the European Commission.

[21] General Data Protection Regulation, Keeling Schedule, available at the following link: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/946117/20201102_-_GDPR_-__MASTER__Keeling_Schedule__with_changes_highlighted__V3.pdf

[22] Data Protection Act 2018, Keeling Schedule, available at the following link: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/946100/20201102_-_DPA_-__MASTER__Keeling_Schedule__with_changes_highlighted__V3.pdf

[23] Such powers are contained for example in Section 16 (power to make, in specific, narrowly circumscribed situations, further exemptions to specific provisions of the UK GDPR), 17A (power to adopt adequacy regulations), 212 and 213 (powers to commence legislation and make transitional provision), and 211 (power to make minor and consequential amendments) of the DPA 2018.

(19) Similarly to Regulation (EU) 2016/679, the UK GDPR applies to the processing of personal data wholly or partly by automated means, or to other processing, if the personal data forms part of a filing system[24]. The definitions of "personal data", of "data subject" and of "processing" of the UK GDPR are identical to those of Regulation (EU) 2016/679[25]. In addition, the UK GDPR applies to the processing of manual unstructured personal data[26] held by certain United Kingdom public authorities[27], although UK GDPR principles and rights that are not relevant to such personal data are disapplied by Sections 24 and 25 of the DPA 2018. Similarly to what is provided under Regulation (EU) 2016/679, the UK GDPR does not apply to the processing of personal data by an individual in the course of a purely personal or household activity[28].

(20) The UK GDPR extends its scope also to the processing in the course of an activity which, immediately before the end of the transition period, fell outside the scope of European Union law (e.g. national security)[29], or was within the scope of Chapter 2 of Title 5 of the Treaty on European Union (Common Foreign and Security Policy activities)[30]. As in the European Union system, the UK GDPR does not apply to the processing of personal data by a competent authority for 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 (so called "law enforcement purposes") – such processing is instead governed by Part 3 of the DPA 2018, as it is the case for Directive (EU) 2016/680 under European Union law – or the processing of personal data by intelligence services (the Security Service, the Secret Intelligence Service and the Government Communications Headquarters) which is covered by Part 4 of the DPA 2018[31].

(21) The territorial scope of the UK GDPR includes the processing of personal data (regardless of where it takes place) in the context of the activities of an establishment of a controller or a processor in the United Kingdom as well as to the processing of personal data of data subjects who are in the United Kingdom, where the processing

---

24 Article 2(1) and (5) of the UK GDPR.

25 Article 4(1) and 2 of the UK GDPR.

26 The manual unstructured processing of personal data is defined in Article 2(5)(b) as the processing of personal data which is not the automated or structured processing of personal data.

27 Article 2(1A) of the UK GDPR provides that the Regulation also applies to the manual unstructured processing of personal data held by an FOI public authority. The reference to FOI public authorities means any public authorities as defined in the Freedom of Information Act 2000, or any Scottish public authorities as defined in the Freedom of Information (Scotland) Act 2002 (asp 13). Section 21(5) of the DPA 2018.

28 Article 2(2)(a) of the UK GDPR.

29 National security activities are only covered by the scope of the UK GDPR as far as they are not carried out by a competent authority for law enforcement purposes, in which case Part 3 of the DPA 2018 applies, or by or on behalf of an intelligence service, whose activities are carved out from the scope of the UK GDPR and subject to Part 4 of the DPA 2018 pursuant to Article 2(2)(c) of the UK GDPR. For example, a police force may conduct security checks against an employee to ensure he can be trusted to access national security material. Despite the police being a competent authority for law enforcement purposes, the processing in question is not for a law enforcement purpose and the UK GDPR would apply. See UK Explanatory Framework for Adequacy Discussions, section H: National Security Data Protection and Investigatory Powers Framework, page 8, available at the following link https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/872239/H_-_National_Security.pdf

30 Article 2(1)(a)&(b) of the UK GDPR.

31 Article 2(2)(b)&(c) of the UK GDPR.

activities are related to the offering of goods or services to such data subjects or the monitoring of their behaviour[32]. This reflects the approach taken in Article 3 of Regulation (EU) 2016/679.

### 2.4. Definitions of personal data and concepts of controller and processor

(22) The definitions of personal data, processing, controller, processor, as well as the definition of pseudonymisation, laid down in Regulation (EU) 2016/679 have been retained without material modifications in the UK GDPR[33]. Moreover, special categories of data are defined in Article 9(1) of the UK GDPR in the same way as under Regulation (EU) 2016/679 ("revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation"). Section 205 of the DPA 2018 provides the definition of "biometric data"[34], "data concerning health"[35] and "genetic data"[36].

### 2.5. Safeguards, rights and obligations

#### *2.5.1. Lawfulness and fairness of processing*

(23) Personal data should be processed lawfully and fairly.

(24) The principles of lawfulness, fairness and transparency and the grounds for lawful processing are guaranteed in the law of the United Kingdom through Articles 5(1)(a) and 6(1) of the UK GDPR, which are identical to the respective provisions in Regulation (EU) 2016/679[37]. Section 8 of the DPA 2018 complements Article 6(1)(e) by providing that the processing of personal data under Article 6(1)(e) of the UK GDPR (necessary for the performance of a task carried out in the public interest, or in the exercise of the controller's official authority), includes processing of personal data that is necessary for the administration of justice, the exercise of a function of either House of Parliament, the exercise of a function conferred on a person by an enactment or rule of law, the exercise of a function of the Crown, a Minister of the

---

32 Article 3 of the UK GDPR. The same territorial scope applies to the processing of personal data under Part 2 of the DPA 2018 that supplements the UK GDPR (Section 207(1A)).

33 Articles 4(1), 4(2), 4(5), 4(7) and 4(8) of the UK GDPR.

34 "Biometric data" means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of an individual, which allows or confirms the unique identification of that individual, such as facial images or dactyloscopic data.

35 "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.

36 "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.

37 Pursuant to Article 6(1) of the UK GDPR, processing is lawful only if and to the extent that: (a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes; (b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; (c) processing is necessary for compliance with a legal obligation to which the controller is subject; (d) processing is necessary in order to protect the vital interests of the data subject or of another natural person; (e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; or (f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

Crown or a government department, or an activity that supports or promotes democratic engagement.

(25) With respect to consent (one of the grounds for lawful processing), the UK GDPR also retains the conditions provided for in the Article 7 of Regulation (EU) 2016/679 unmodified, that is to say the controller must be able to demonstrate that the data subject has consented, a written request for consent must be presented using clear and plain language, the data subject must have the right to withdraw consent at any time, and when assessing whether consent is freely given, it should be taken into account whether the performance of a contract is conditional on consent to the processing of personal data that is not necessary for the performance of that contract. Moreover, pursuant to Article 8 of the UK GDPR, in the context of the provision of information society services a child's consent is lawful only when the child is at least 13 years old. This falls within the age bracket set in Article 8 of Regulation (EU) 2016/679.

*2.5.2. Processing of special categories of personal data*

(26) Specific safeguards should exist where "special categories" of data are being processed.

(27) The UK GDPR and the DPA 2018 contain specific rules as regards the processing of special categories of personal data, which are defined in Article 9(1) of the UK GDPR in the same way as under Regulation (EU) 2016/679 (see recital (22) above). According to Article 9 of the UK GDPR, the processing of special categories of data is in principle prohibited, unless a specific exception applies.

(28) These exceptions (listed in Article 9(2) and (3) of the UK GDPR) do not make any changes of substance to those in Article 9(2) and (3) of Regulation (EU) 2016/679. Unless the data subject has given its explicit consent to the processing of those personal data, the processing of special categories of personal data is only permitted in specific and limited circumstances. In most instances, processing of sensitive data must be necessary for a specific purpose defined in the relevant provision (see Article 9(2)(b), (c), (f), (g), (h), (i) and (j)).

(29) Moreover, where an exception under Article 9(2) of the UK GDPR requires an authorisation by law or refers to the public interest, Section 10 of the DPA 2018 together with Schedule 1 to the DPA 2018 further specify the conditions that must be met for the exceptions to be relied upon. For example, in the case of processing of sensitive data for protecting "public health" (Section 9(2)(i) of the UK GDPR), paragraph 3(b) of Part 1 of Schedule 1 requires that, in addition to the necessity test, such processing is carried out "by or under the responsibility of a health professional" or "by another person who owes a duty of confidentiality under an enactment or rule of law", including under the well-established common law duty of confidentiality.

(30) Where sensitive data is processed for reasons of substantial public interest (Article 9(2)(g) of the UK GDPR), Part 2 of Schedule 1 to the DPA 2018 provides an exhaustive list of purposes that can be considered as of substantial public interest, and, for each of these purposes, sets out specific additional conditions. For instance, promoting racial and ethnic diversity at senior levels of organisations is recognised as a substantial public interest. Processing of sensitive data for this specific purpose is subject to detailed requirements, including that the processing is carried out as part of a process of identifying suitable individuals to hold senior positions, is necessary

to promote racial and ethnic diversity and is not likely to cause substantial damage or substantial distress to the data subject.

(31) Section 11(1) of the DPA 2018 sets out conditions for personal data to be processed in the circumstances described in Article 9(3) of the UK GDPR relating to the obligation of secrecy. This includes circumstances in which it is carried out by or under the responsibility of a health professional or a social work professional, or by another person who in the circumstances owes a duty of confidentiality under an enactment or rule of law.

(32) In addition, many of the exceptions listed in Article 9(2) of the UK GDPR require suitable and specific safeguards in order to be used. Depending on the nature of the processing and the level of risk for the rights and freedoms of data subjects, the conditions for processing provided for in Schedule 1 to the DPA 2018 establish different safeguards. Schedule 1 sets out the conditions for each processing situation in turn.

(33) In some cases, the DPA 2018 regulates and limits the type of sensitive data that may be processed for a particular legal basis to be complied with. For example, paragraph 8 of Schedule 1 authorises the processing of sensitive data for the purpose of the promotion of equality of opportunity or treatment. This processing condition can only be used if the data reveals racial or ethnic origin, religious or philosophical beliefs, sexual orientation, or if it is health data.

(34) In some cases, the DPA 2018 limits the type of controller that may use the processing condition. For example, paragraph 23 of Schedule 1 provides for processing of sensitive data in relation to elected representatives' responses to the public. This processing condition can only be used if the controller is the elected representative or is acting under their authority.

(35) In some other cases, the DPA 2018 sets limits on the categories of data subject for the processing condition to be used. For example, paragraph 21 of Schedule 1 regulates the processing of sensitive data for occupational pension schemes. This condition can only be used if the data subject in question is a sibling, parent, grandparent, or great-grandparent of the scheme member.

(36) In addition, when relying on the exceptions in Article 9(2) of the UK GDPR that are further specified in Section 10 of the DPA 2018 together with Schedule 1 to the DPA 2018, the controller in most instances is required to draft an "Appropriate Policy Document". It must outline the controller's procedures for securing compliance with the principles in Article 5 of the UK GDPR. It must also set out policies for retention and erasure, with an indication of the likely storage period. Controllers must review and update this document as appropriate. The controller must keep the policy document for six months after processing is finished and must make it available to the Information Commissioner on request[38].

(37) Pursuant to paragraph 41 of Schedule 1 to the DPA 2018, the Policy Document must always be accompanied by an augmented record of processing. This record must track the commitments included in the Policy Document, i.e. whether data is being erased or retained in accordance with the policies. If the policies have not been followed, the log must record the reasons. The record must also describe how the

[38] Paragraphs 38-40 of Schedule 1 to the DPA 2018.

processing satisfies Article 6 of the UK GDPR (lawfulness of processing) and the specific condition in Schedule 1 to the DPA 2018 relied on.

(38) Finally, like Regulation (EU) 2016/679, the UK GDPR also provides general safeguards for certain processing operations of special categories of data. Article 35 of the UK GDPR requires a data protection impact assessment if special categories of data are processed on a large scale. Pursuant to Article 37 of the UK GDPR, a controller or processor must designate a data protection officer where its core activities consist of processing special categories of data on a large scale.

(39) With respect to personal data relating to criminal convictions and offences, Article 10 of the UK GDPR is identical to Article 10 of Regulation (EU) 2016/679. It allows the processing of personal data relating to criminal convictions and offences only under the control of official authority or when the processing is authorised by domestic law providing for appropriate safeguards for the rights and freedoms of data subjects.

(40) Where the processing of data relating to criminal convictions and offences is not carried out under the control of official authority, Section 10(5) of the DPA 2018 provides that such processing can take place only for the specific purposes/ in the specific situations set out in Parts 1, 2 and 3 of Schedule 1 to the DPA 2018 and is subject to the specific requirements that are set out for each of these purposes/situations. For example, criminal convictions data can be processed by not-for-profit bodies if the processing is carried out (a) in the course of its legitimate activities with appropriate safeguards by a foundation, association or other not-for-profit body with a political, philosophical, religious or trade union aim, and (b) on condition that (i) the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes, and (ii) the personal data is not disclosed outside that body without the consent of the data subjects.

(41) Moreover, Part 3 of Schedule 1 to the DPA sets out further circumstances in which criminal convictions data may be used which correspond to the legal grounds for processing of sensitive data in Article 9(2) of Regulation (EU) 2016/679 and the UK GDPR (e.g. consent of the data subject, vital interests of an individual if the data subject is legally or physically unable to give consent, if data has already manifestly been made public by the data subject, if processing is necessary for the establishment, exercise or defence of a legal claim etc.).

*2.5.3 Purpose limitation, accuracy, data minimisation, storage limitation and data security*

(42) Personal data should be processed for a specific purpose and subsequently used only insofar as this is not incompatible with the purpose of processing.

(43) This principle is provided in Article 5(1)(b) of Regulation (EU) 2016/679 and has been retained without changes in Article 5(1)(b) of the UK GDPR. The conditions on further compatible processing pursuant to Article 6(4) of Regulation (EU) 2016/679 have also been retained with no material modifications in Article 6(4)(a) - (e) of UK GDPR.

(44) Moreover, data should be accurate and, where necessary, kept up to date. It should also be adequate, relevant and not excessive in relation to the purposes for which it is processed, and in principle be kept for no longer than is necessary for the purposes for which the personal data is processed.

(45) These principles of data minimisation, accuracy and storage limitation are set out in Article 5(1)(c) to (e) of Regulation (EU) 2016/679 and are retained without modifications in Article 5(1)(c) to (e) in the UK GDPR.

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

(47) Data security is enshrined in the law of the United Kingdom through the principle of integrity and confidentiality in Article 5(1)(f) of the UK GDPR and in Article 32 of the UK GDPR on security of processing. Those provisions are identical to the respective provisions of Regulation (EU) 2016/679. Moreover, under the same conditions as those set out in Articles 33 and 34 of Regulation (EU) 2016/679, the UK GDPR requires the notification of a personal data breach to the supervisory authority (Article 33 of the UK GDPR) and the communication of a personal data breach to the data subject (Article 34 of the UK GDPR).

*2.5.4 Transparency*

(48) Data subjects should be informed of the main features of the processing of their personal data.

(49) This is ensured by Articles 13 and 14 of the UK GDPR, which, in addition to a general principle of transparency, provide rules on the information to be provided to the data subject[39]. The UK GDPR introduces no material modifications to these rules compared to the corresponding articles of Regulation (EU) 2016/679. However, like under Regulation (EU) 2016/679, the transparency requirements of those articles are subject to several exceptions laid down in the DPA 2018 (see recitals (54) to (74)).

*2.5.5 Individual rights*

(50) Data subjects should have certain rights which can be enforced against the controller or processor, in particular the right of access to data, the right to object to the processing and the right to have data rectified and erased. At the same time, such rights may be subject to restrictions, as far as these restrictions are necessary and proportionate to safeguard public security or other important objectives of general public interest.

2.5.5.1 The substantive rights

[39] In Articles 13(1)(f) and 14(1)(f) the references to adequacy decisions by the Commission have been replaced with references to equivalent United Kingdom instrument i.e. adequacy regulations under the DPA 2018. In addition, in Articles 14(5)(c)-(d) the references to EU or Member State law have been replaced with a reference to domestic law (as examples of such domestic law that may fall under Article 14(5)(c), the United Kingdom has mentioned Section 7 of the Scrap Metal Dealers Act 2013 that provides rules for register of scrap metal licences or Part 35 of the Companies Act 2006 providing the rules for the registrar of companies. Similarly, an example of domestic law that may fall under Art 14(5)(d) could include legislation laying down rules on professional confidentiality, or obligations reflected in contracts of employment or the common law duty of confidentiality (such as personal data processed by health professionals, human resources, social workers etc.).

(51) The UK GDPR grants individuals the same enforceable rights as Regulation (EU) 2016/679. The provisions providing the rights of the individuals have been maintained in the UK GDPR without material changes.

(52) The rights include the right of access by the data subject (Article 15 of the UK GDPR), the right to rectification (Article 16 of the UK GDPR), the right to erasure (Article 17 of the UK GDPR), the right to restriction of processing (Article 18 of the UK GDPR), a notification obligation regarding rectification or erasure of personal data or restriction of processing (Article 19 of the UK GDPR), the right to data portability (Article 20 of the UK GDPR), and the right to object (Article 21 of the UK GDPR)[40]. The latter also includes the right of a data subject to object to the processing of personal data for the purpose of direct marketing provided in paragraphs 2 and 3 of Article 21 of Regulation (EU) 2016/679. Moreover, under Section 122 of the DPA 2018, the Information Commissioner must prepare a code of practice in relation to the carrying out of direct marketing in accordance with the requirements of the data protection legislation (and the Privacy and Electronic Communications (EC Directive) Regulations 2003) and such other guidance to promote good practice in direct marketing that the Commissioner considers appropriate. The Information Commissioner's Office is currently developing the direct marketing code[41].

(53) The data subject's right not to be subject to a decision based solely on automated processing that produces legal effects concerning them, or similarly affects them significantly, as provided in Article 22 GDPR, has also been retained in UK GDPR without substantial changes. However, a new paragraph 3A has been added to reference that Section 14 of the DPA 2018 sets out safeguards for data subjects' rights, freedoms and legitimate interests when the processing is carried out under Article 22(2)(b) of the UK GDPR. This only applies when the basis for such a decision is an authorisation or requirement under UK law, and does not apply where the decision is necessary under a contract or made with the data subject's explicit consent. Where Section 14 of the DPA 2018 applies, the controller must, as soon as reasonably practicable, notify the data subject in writing that a decision has been taken based solely on automated processing. The data subject has a right to request that the controller - within one month of receipt of the notice - or reconsider the decision, or to take a new decision that is not based solely on automated processing. The Secretary of State is empowered to adopt further safeguards as regards automated decision-making. This power has not yet been exercised.

2.5.5.2 Restrictions to individual rights and other provisions

(54) The DPA 2018 sets out several restrictions to individual rights, fitting within the framework of Article 23 of the UK GDPR. No restrictions are introduced within this framework concerning the right to object to direct marketing as provided in Article

[40] In Articles 17(1)(e) and 17(3)(b) the references to EU or Member State law have been replaced with a reference to domestic law (as examples of such domestic law under Article 17(1)(e), the United Kingdom has mentioned the Education (Pupil Information) (England) Regulations 2006 that requires the names of the pupils to be erased from the school registries after they have left the school or Medical Act 1983, Section 34F, which set outs the rules on the removal of names from the General Practitioner Register and the Specialist Register.

[41] The draft code of practice can be found at the following link: https://ico.org.uk/media/about-the-ico/consultations/2616882/direct-marketing-code-draft-guidance.pdf

21(2) and (3) of the UK GDPR or to the right not to be subject to automated decision making as provided in Article 22 of the UK GDPR.

(55) The restrictions are detailed in Schedules 2-4 to the DPA 2018. The UK authorities have explained that they are guided by two principles: the principle of specificity (taking a granular approach, splitting broad restrictions into multiple, more specific provisions) and the principle of conditionality (each provision is complemented by safeguards in the form of limitations or conditions to prevent abuse)[42].

(56) The restrictions described in Article 23(1) of the UK GDPR are designed to ensure they only apply in specified circumstances where necessary in a democratic society and proportionate to the legitimate aim they pursue. Furthermore, in accordance with established case law on the interpretation of restrictions, an exemption from the data protection regime can only be applied in any particular case if it is necessary and proportionate to do so[43]. The test of necessity has been required to be "a strict one, requiring any interference with the subject's rights to be proportionate to the gravity of the threat to the public interest. The exercise therefore involves a classic proportionality analysis[44]."

(57) The aim pursued by these restrictions correspond to the ones listed in Article 23 of Regulation (EU) 2016/679, except for the restrictions for national security and defence that are instead regulated by Section 26 of the DPA 2018, but are subject to the same requirements of necessity and proportionality (see recitals (66) to (68)).

(58) Some of the restrictions, for example those related to the prevention or detection of crime, to the apprehension or prosecution of offenders, and to the assessment or collection of tax or duty[45] permit restrictions to all the individual rights and transparency obligations (excluding rights under Article 21(2) and Article 22). The scope of other restrictions is limited to transparency obligations and access rights, such as the restrictions relating to legal professional privilege[46], to the right to freedom from a requirement to provide information that would lead to self-incrimination[47], and to corporate finance, notably the prevention of insider trading[48]. Few of the restrictions permit a restriction to the controller's obligation to communicate a data breach to a data subject and the principles of purpose limitation, and lawfulness, fairness and transparency of the processing[49].

---

42 UK Explanatory Framework for Adequacy Discussions, Section E: Restrictions, page 1, available at the following link: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/872232/E_-_Narrative_on_Restrictions.pdf

43 *Open Rights Group & Anor, R (On the Application Of) v Secretary of State for the Home Department & Anor* [2019] EWHC 2562 (Admin), paragraphs 40 and 41.

44 *Guriev v Community Safety Development (United Kingdom) Ltd* [2016] EWHC 643 (QB), paragraph 43. On this see also *Lin v Commissioner of Police for the Metropolis* [2015] EWHC 2484 (QB), paragraph 80.

45 Paragraph 2 of Schedule 2 to the DPA 2018.

46 Paragraph 19 of Schedule 2 to the DPA 2018.

47 Paragraph 20 of Schedule 2 to the DPA 2018.

48 Paragraph 21 of Schedule 2 to the DPA 2018.

49 For instance, restrictions to the right to a data breach notification are permitted only in relation to crime and taxation (paragraph 2 of Schedule 2 to the DPA 2018), parliamentary privilege (paragraph 13 of Schedule 2 to the DPA 2018) and processing for journalistic, academic, artistic and literary purposes (paragraph 26 of Schedule 2 to the DPA 2018).

(59) Some of the restrictions apply automatically "in full" to a certain type of processing of personal data (for example, the application of transparency obligations and individual rights is excluded when personal data is processed for the purposes of assessing a person's suitability for judicial office or personal data is processed by a court, tribunal, or individual, acting in a judicial capacity).

(60) However, in the majority of cases, the relevant paragraph in Schedule 2 to the DPA 2018 specifies that the restriction applies only when (and to the extent) that the application of the provisions "would be likely to prejudice" the legitimate aim pursued by that restriction: for example, the listed provisions of the UK GDPR do not apply to personal data processed for the prevention or detection of crime, the apprehension or prosecution of offenders, or the assessment or collection of a tax or duty "to the extent that the application of those provisions would be likely to prejudice" any of these matters[50].

(61) The "would be likely to prejudice" standard has been interpreted by UK courts to mean "a very significant and weighty chance of prejudice to the identified public interests"[51]. The controller is responsible for assessing on case-by-case basis whether the application of the provision would be likely to prejudice the legitimate aim pursued[52].

(62) One of the restrictions subject to the prejudice test relates to the "the maintenance of effective immigration control"[53] or "the investigation or detection of activities that would undermine the maintenance of effective immigration control"[54] and applies to several rights[55]. Its application and scope have been interpreted by United Kingdom courts[56]. In particular, the High Court of Justice considered that the restriction "is plainly a matter of "important public interest" and "pursues a legitimate aim"[57]. Importantly, its scope is limited by the prejudice test mentioned above, meaning that the exemption can only be relied upon if and to the extent that compliance with the relevant GDPR provisions would be likely to prejudice the maintenance of effective immigration control or the investigation or detection of activities that would undermine the maintenance of effective immigration control. As noted in recital (62), this is a high standard[58] which moreover requires a case-by-case assessment.

---

50 Paragraph 2 of Schedule 2 to the DPA 2018.

51 *R (Lord) v Secretary of State for the Home Department* [2003] EWHC 2073 (Admin), paragraph 100, and *Guriev v Community Safety Development (United Kingdom) Ltd* [2016] EWHC 643 (QB), paragraph 43.

52 *Open Rights Group & Anor, R (On the Application Of) v Secretary of State for the Home Department & Anor*, paragraph 31.

53 Paragraph 4(1)(a) of Schedule 2 to the DPA 2018.

54 Paragraph 4(1)(b) of Schedule 2 to the DPA 2018.

55 See Paragraph 4(2) of Schedule 2 to the DPA 2018.

56 See in particular *Open Rights Group & Anor, R (On the Application Of) v Secretary of State for the Home Department & Anor*, see footnote 43.

57 *Open Rights Group & Anor, R (On the Application Of) v Secretary of State for the Home Department & Anor*, paragraph 30.

58 In this case the Court interpreted the words "would be likely to prejudice" by analogy with a previous case in which, in the context of DPA 1998, such words had been interpreted to mean "a very significant and weighty chance of prejudice to the particular public interest. The degree of risk must be such that there "may very well" be prejudice to those interests, even if the risk falls far short of being more probable than not". *Open Rights Group & Anor, R (On the Application Of) v Secretary of State for the Home Department & Anor*, paragraph 39.

(63) The High Court further confirmed the application of the restriction is subject to the requirements of necessity and of proportionality as set out in Regulation (EU) 2016/679[59]. The High Court upheld that an exception from the data protection regime can only be applied in any particular case if it is "necessary" to do so, where necessary means that doing otherwise would be "likely to prejudice" the important public interest at stake, and thus subject to a necessity test requiring any interference with the subject's rights to be proportionate to the gravity of the threat to the public interest[60]. The High Court maintained that the "likely to prejudice" test and the requirements of necessity and proportionality provide an adequate set of safeguards to protect individual data subject rights.[61]

(64) In addition, the UK's Information Commissioner (ICO) has issued guidance on the use of this specific restriction[62]. The guidance states in particular that "You should not apply the immigration exemption as a blanket exemption to restrict [….] rights for all the data you hold. The scope of the exemption is limited to those rights which, if exercised for the data held, would prejudice the identified immigration purposes. […]. Therefore the default position of the controller should be to comply with the requirements of Regulation (EU) 2016/679 and the DPA as far as possible. […] The prejudice test has a high threshold and you should not apply the exemption in a blanket fashion. […] You must consider whether the application of the exemption is a proportionate response to the individual's data protection request. You may consider that there is a pressing social need to apply the immigration exemption, but you must also take into account whether this outweighs your obligation to individuals under Regulation (EU) 2016/679. They have rights over their personal data which you must consider in all circumstances, in particular, the right of access. It is therefore important in every case that you consider whether the data protection rights of the individual override the identified risk of prejudice. Your application of the exemption must be proportionate to the circumstances and you must carefully consider and document each instance." [63]

(65) Although formulated rather broadly, the immigration restriction as interpreted by the case-law and the ICO's guidance is subject to a number of strict conditions – very similar to the ones set in EU law for restrictions to data protection rights and obligations – that frame its application. In particular, it must be applied on a case-by-case basis, only to the extent necessary to achieve a legitimate aim and in a proportionate manner.

(66) In addition to the restrictions contained in Schedule 2 to the DPA 2018, Section 26 of the DPA 2018 provides an exemption which may be applied to certain provisions of

---

59 *Open Rights Group & Anor, R (On the Application Of) v Secretary of State for the Home Department & Anor*, paragraph 40.

60 *Open Rights Group & Anor, R (On the Application Of) v Secretary of State for the Home Department & Anor*, paragraph 41; *Guriev v Community Safety Development (United Kingdom) Ltd* [2016] EWHC 643 (QB), paragraph 45; *Lin v Commissioner of the Police for the Metropolis* [2015] EWHC 2484 (QB), paragraph 80.

61 *Open Rights Group & Anor, R (On the Application Of) v Secretary of State for the Home Department & Anor*, paragraph 42.

62 ICO guide on immigration exemption, available at the following link: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/exemptions/immigration-exemption/

63 ICO guide on immigration exemption, "When should this exemption be used?", "What is the prejudice test?", available at the following link: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/exemptions/immigration-exemption/

the UK GDPR and of the DPA 2018 if that exemption is required for the purpose of safeguarding national security or for defence purposes. This exemption applies to the data protection principles (except the principle of lawfulness), the transparency obligations, the rights of the data subject, the obligation to notify a data breach, rules on international transfers, some of the duties and powers of the Information Commissioner, and the rules on remedies, liabilities and penalties, except for the provision on the general conditions for imposing administrative fines set out in Article 83 of the UK GDPR and the provision on penalties in Article 84 of the UK GDPR. Moreover Section 28 of the DPA 2018 modifies the application of Article 9(1) to enable the processing of special categories of data in Article 9(1) of the UK GDPR to the extent that the processing is carried out for safeguarding national security or for defence purposes, and with appropriate safeguards for the rights and freedoms of data subjects[64].

(67) The exemption can only be applied to the extent that it is required to safeguard national security or defence. As it is also the case for the other exemptions provided for by the DPA 2018, it must be considered and invoked by the controller on a case-by-case basis[65]. Moreover, any application of the exemption must be in compliance with human right standards (underpinned by the Human Rights Act 1998), according to which any interference with privacy rights should be necessary and proportionate in a democratic society[66].

(68) The fact that the data is processed for national security or defence purposes is therefore not on its own sufficient for the exemption to be applied. A controller must consider the actual consequences to national security if it had to comply with the particular data protection provision. The exemption can only be applied to those specific provisions which have been identified as posing the risk and must be applied as restrictively as possible[67].

---

64 According to the information provided by the UK authorities, where processing is in the national security context, controllers will typically be applying enhanced safeguards and security measures to the processing, reflecting the sensitive nature of the processing. Which safeguards are appropriate will depend on the risks posed by the processing being undertaken. This could include restrictions on access to the data so it can only be accessed by authorised persons with appropriate security clearance, strict restrictions on sharing the data, and the high standard of security applied to the storage and handling procedures.

65 *Open Rights Group & Anor, R (On the Application Of) v Secretary of State for the Home Department & Anor*, paragraph 31.

66 See also *Guriev v Community Safety Development (United Kingdom) Ltd* [2016] EWHC 643 (QB), paragraph 45; *Lin v Commissioner of the Police for the Metropolis* [2015] EWHC 2484 (QB), paragraph 80.

67 According to an example provided by the UK authorities, if a suspected terrorist under active investigation by MI5 made an access request to the Home Office (for instance, because he is engaged in a dispute with the Home Office over immigration matters), it would be necessary to protect from disclosure to the data subject any data that MI5 may have shared with the Home Office relating to ongoing investigations that could prejudice sensitive sources, methods or techniques and/or lead to an increase in the threat posed by the individual. In such circumstances it is likely that the threshold to apply the Section 26 exemption would have been met and an exemption from disclosing the information would be required in order to safeguard national security. However, if the Home Office also held personal data about the individual which did not relate to the MI5 investigation and that information could be provided without risk of damage to national security, then the national security exemption would not be applicable when considering disclosure of information to the individual. The ICO is currently preparing guidance on how controllers should approach the use of the exemption at Section 26. The guidance is expected to be published by the end of March 2021.

(69) This approach has been confirmed by the Information Tribunal[68]. In the case of *Baker v Secretary of State for the Home Department* ("*Baker v Secretary of State"*), it determined that it was unlawful to apply the national security exemption as a blanket exemption to access requests received by the intelligence services. Instead, the exemption had to be applied on a case-by-case basis, by looking at each request on its merit and in view of the right of individuals to respect for their private lives[69].

*2.5.6 Restrictions for personal data processed for journalistic, artistic, academic and literary purposes as well as archiving and research*

(70) Article 85(2) of the UK GDPR allows for provision to be made for personal data processed for journalistic, artistic, academic and literary purposes to be exempt from several provisions of the UK GDPR. Part 5 of Schedule 2 to the DPA 2018 sets out the exemptions for processing for these purposes. It provides for exemptions from the data protection principles (except the principle of integrity and confidentiality), the legal grounds for processing (incl. special categories of data and criminal convictions etc. data), the conditions for consent, the transparency obligations, the rights of the data subjects, the obligation to notify data breaches, the requirement to consult the Information Commissioner prior to high risk processing, and the rules on international transfers[70]. In this regard, the UK GDPR does not depart in a substantive manner from Regulation (EU) 2016/679, which in its Article 85 also provides for the possibility to exempt processing carried out for journalistic purposes or the purposes of academic, artistic or literary expression from a number of requirements of Regulation (EU) 2016/679. The provisions of the DPA 2018, notably Schedule 2, Part 5, are compatible with the UK GDPR.

(71) The core balancing exercise to be carried out under Article 85 of the UK GDPR relates to whether an exemption to the data protection rules mentioned in the previous recital is "necessary to reconcile the right to the protection of personal data with the freedom of expression and information"[71]. According to Schedule 2, paragraphs 26(2) and (3) to the DPA 2018, the United Kingdom applies a "reasonable belief" test in order for this balance to be struck. For an exemption to be justified, the controller must reasonably believe (i) that publication is in the public interest; and (ii) that the application of the relevant GDPR provision would be incompatible with journalistic, academic, artistic or literary purposes. As confirmed

68 The Information Tribunal was established to hear data protection appeals under the Data Protection Act 1984. In 2010 the Information Tribunal became part of the General Regulatory Chamber of the First Tier Tribunal, as part of the reform of the structure of the UK system of tribunals.

69 See *Baker v Secretary of State for the Home Department* [2001] UKIT NSA2 ("*Baker v Secretary of State").*

70 See Article 85 of the UK GDPR and Schedule 2, Part 5, paragraph 26(9) to the DPA 2018.

71 In accordance with Schedule 2, Part 5, paragraph 26(2) to the DPA 2018, the exception applies to the processing of personal data carried out for special purposes (the purposes of journalism, academic purposes, artistic purposes and literary purposes), if the processing is being carried out with a view to the publication by a person of journalistic, academic, artistic or literary material, and the controller reasonably believes that the publication of that material would be in the public interest. In determining whether a publication would be in the public interest, the controller must take into account the special importance of the public interest in the freedom of expression and information. Moreover, the controller must have regard to codes of practice or guidelines relevant to the publication in question (the BBC Editorial Guidelines, Ofcom Broadcasting Code, and Editors' Code of Practice). Furthermore, for an exemption to apply, the controller must reasonably believe that compliance with the relevant provision would be incompatible with the special purposes (paragraph 26(3) of Schedule 2 to the DPA 2018).

by case law[72], the "reasonable belief" test has both a subjective and an objective component: it is insufficient for the controller to demonstrate that he himself believed compliance was incompatible. His belief must be reasonable, i.e. it could be believed by a reasonable person, knowing the relevant facts. The controller must therefore exercise due diligence when forming his belief in order to be able to demonstrate reasonableness. According to the explanations provided by the United Kingdom authorities, the "reasonable belief" test must be carried out on an exemption-by-exemption basis[73]. If the conditions are met, the exemption is considered necessary and proportionate under United Kingdom law.

(72) According to Section 124 of the DPA 2018, the ICO is to prepare a Code of Practice on Data Protection and Journalism. Work on this Code is ongoing. Guidance on the matter under the Data Protection Act 1998 has been issued which notably stresses that, to rely on this exemption, it is insufficient to merely state that compliance would be an inconvenience for journalist activities, but there must be a clear argument that the provision in question presents an obstacle to responsible journalism[74]. Guidance on the application of the public interest test and the balancing of public interest against an individual's interest in privacy has also been published by the United Kingdom's telecommunications regulator OFCOM and the BBC in its editorial guidelines[75]. The guidelines notably provide examples of information that can be considered in the public interest, and explain the need to be able to demonstrate that the public interest outweighs privacy rights in the particular circumstances of the case.

(73) Similarly to what is provided in Article 89 GDPR, personal data processed for archiving purposes in the public interest, scientific or historical research purposes or

---

72 The judgment in *NT1* v. *Google* [2018] EWHC 799 (QB), paragraph 102 addressed a discussion of whether the data controller held a reasonable belief that publication was in the public interest, and that compliance with the relevant provisions was incompatible with the special purposes. The court stated that Sections 32(1) (b) and (c) of Data Protection Act 1998 had a subjective and an objective element: the data controller must establish that it held a belief that publication would be in the public interest, and that this belief was objectively reasonable; it must establish a subjective belief that compliance with the provision from which it seeks exemption would be incompatible with the special purpose in question.

73 An example of how the "reasonable belief" test is applied is included in the ICO's decision to fine *True Visions Productions*, which was made under the Data Protection Act 1998. The ICO accepted that the media controller had a subjective belief that compliance with the first data protection principle (fairness and lawfulness) was incompatible with journalistic purposes. However, the ICO did not accept this belief was objectively reasonable. The ICO decision is available at the following link: https://ico.org.uk/media/action-weve-taken/mpns/2614746/true-visions-productions-20190408.pdf

74 Pursuant to the guidance, organisations must be able to explain why complying with the relevant provision of the Data Protection Act 1998 is incompatible with the purposes of journalism. In particular, controllers must balance the detrimental effect compliance would have on journalism against the detrimental effect non-compliance would have on the rights of the data subject. If a journalist can reasonably achieve their editorial aims in a way that complies with the standard provisions of the DPA, they must. Organisations must be able to justify their use of the restriction in respect of every provision they have not complied with. "Data protection and journalism: a guide for the media", available at the following link: https://ico.org.uk/media/for-organisations/documents/1552/data-protection-and-journalism-media-guidance.pdf

75 Examples of public interest would include revealing or detecting crime, protecting public health or safety, exposing misleading claims made by individuals or organisations or disclosing incompetence that affects the public. See OFCOM's guidance available at the following link: https://www.ofcom.org.uk/__data/assets/pdf_file/0017/132083/Broadcast-Code-Section-8.pdf and BBC's editorial guidelines available at the following link: https://www.bbc.com/editorialguidelines/guidelines/privacy

statistical purposes can also be exempted from a number of listed provisions of the UK GDPR[76]. As regards research and statistics, exemptions are possible to the provisions of the UK GDPR related to confirmation of processing, access to data and safeguards for third country transfers; right to rectification; restriction of processing and objection to processing. As regards archiving in the public interest, exemptions are also possible to the notification obligation regarding rectification or erasure of personal data or restriction of processing and to the right to data portability.

(74) According to paragraphs 27(1) and 28(1) of Schedule 2 to the DPA 2018, the exemptions to the listed provisions of the UK GDPR are possible where the application of the provisions would "prevent or seriously impair the achievement" of the purposes in question[77].

*2.5.7 Restrictions on onward transfers*

(75) The level of protection afforded to personal data transferred from the European Union to controllers or processors in the United Kingdom 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 the United Kingdom controller or processor 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. For this reason, the application of the rules of the UK GDPR and the DPA 2018 on international transfers of personal data is an important factor to ensure the continuity of protection in the case of personal data transferred from the European Union to the United Kingdom under this Decision.

(76) The regime on international transfers of personal data from the United Kingdom is set out in Articles 44-49 of the UK GDPR, supplemented by the DPA 2018, and mirrors the one set out in Chapter V of Regulation (EU) 2016/679. In particular, transfers of personal data to a third country or international organisation can only take place on the basis of adequacy regulations (the UK equivalent to an adequacy decision under Regulation (EU) 2016/679), or in the absence of adequacy regulations, where the controller or processor has provided appropriate safeguards in accordance with Article 46 of the UK GDPR. In the absence of adequacy regulations or appropriate safeguards, a transfer can only take place based on derogations set out in Article 49 of the UK GDPR.[78]

---

76 See Article 89 of the UK GDPR and paragraphs 27(2) and 28(2) of Part 6 of Schedule 2 to the DPA 2018.

77 This is subject to the requirement that personal data is processed in accordance with Article 89(1) of the UK GDPR as supplemented by Section 19 of the DPA 2018.

78 With the exception of Article 48 of Regulation (EU) 2016/679 that the United Kingdom has chosen not to include in the UK GDPR. The UK authorities have explained that they did not consider necessary to introduce such a provision clarifying that requests to transfer data to a third country from a court or an administrative authority of that third country are enforceable only if an international agreement to that effect exists with the country in question, given that the UK legal order already provides sufficient safeguards in that respect. First, in order to enforce a foreign judgment, courts in the United Kingdom need to be able to point to common law or to a statute that allows its enforceability. However, according to the UK authorities, neither common law nor statutes provide for the enforcement of foreign judgments requiring the transfer of data without an international agreement in place. As a consequence, requests for data are unenforceable and a provision such as Article 48 of Regulation (EU) 2016/679 would have no legal added value under United Kingdom law. Second, the United Kingdom authorities have explained that any transfer of personal data to third countries – including if upon request from a

(77) The **adequacy regulations** made by the Secretary of State can stipulate that a third country (or a territory or a sector within a third country), an international organisation, or a description[79] of such a country, territory, sector, or organisation ensures an adequate level of protection of personal data. When assessing the adequacy of the level of protection, the Secretary of State must take into account the same elements that the Commission is required to assess under Article 45(2)(a)-(c) of Regulation (EU) 2016/679, interpreted together with recital 104 of Regulation (EU) 2016/679 and the retained EU case law. This means that, when assessing the adequate level of protection of a third country, the relevant standard will be whether that third country in question ensures a level of protection "essentially equivalent" to that guaranteed within the United Kingdom.

(78) As for the procedure, adequacy 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 proposing to adopt UK adequacy regulations[80]. Once adopted by the Secretary of State, those regulations are laid before Parliament and subject to the "negative resolution" procedure under which both Houses of Parliament can scrutinise the regulations and have the ability to pass a motion annulling the regulations within a 40 day period[81].

(79) According to Section 17B(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 country or organisation specified 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. These procedural aspects also mirror the corresponding requirements of Regulation (EU) 2016/679.

(80) In the absence of adequacy regulations, international transfers can take place where the controller or processor has provided **appropriate safeguards** in accordance with Article 46 of the UK GDPR. These safeguards are similar to those under Article 46 of Regulation (EU) 2016/679. They include legally binding and enforceable instruments between public authorities or bodies, binding corporate rules[82], standard data protection clauses, approved codes of conduct, approved certification

---

foreign court or administrative authority – remains subject to the restrictions in Chapter V of the UK GDPR and therefore requires a transfer tool such as an adequacy regulation or appropriate safeguards, unless one of the derogations in Article 49 of the UK GDPR applies.

79 The UK 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 adequacy regulations in relation to only certain types of data transfers).

80 During the adequacy talks, the UK Authorities have specified that they intend to put in place a Memorandum of Understanding between the Secretary of State for the Department for Digital, Culture, Media and Sport and the Information's Commissioner's Office that will set out mutually agreed ways of working between DCMS and the ICO on future UK adequacy assessments.

81 If such a vote is passed the regulations will ultimately cease to have any further legal effect.

82 The UK GDPR retains the rules in Article 47 of Regulation (EU) 2016/679 subject to only modifications to fit the rules into domestic context, for example by replacing the references to competent supervisory authority to the Information Commissioner, deleting reference to consistency mechanism from paragraph 1 and deleting the entire paragraph 3.

mechanisms, and with authorisation from the Information Commissioner, contractual clauses between controllers (or processors) or administrative arrangements between public authorities. However, the rules have been modified, from a procedural point of view, to work within the United Kingdom framework, in particular the standard data protection clauses can be adopted by the Secretary of State (Section 17C) or the Information Commissioner (Section 119A) in accordance with the DPA 2018.

(81) In absence of an adequacy decision or appropriate safeguards, a transfer can only take place based on **derogations** set out in Article 49 of the UK GDPR[83]. The UK GDPR introduces no material changes to the derogations, compared to the corresponding rules of Regulation (EU) 2016/679. Under the UK GDPR, as under Regulation (EU) 2016/679, certain derogations can only be relied on if the transfer is occasional[84]. Moreover, the ICO in its guidance on international transfers, clarifies that: "You should only use these as true 'exceptions' from the general rule that you should not make a restricted transfer unless it is covered by an adequacy decision or there are appropriate safeguards in place"[85]. With respect to transfers that are necessary for important reasons of public interest (Article 49(1)(d)), the Secretary of State can make regulations to specify circumstances in which a transfer of personal data to a third country or international organisation is / is not necessary for important reasons of public interest. Furthermore, the Secretary of State can by regulations restrict the transfer of a category of personal data to a third country or international organisation where the transfer cannot take place based on adequacy regulations, and the Secretary of State considers the restriction to be necessary for important reasons of public interest. No such regulations have been adopted so far.

(82) This framework for international transfers has become applicable at the end of the transition period[86]. However, paragraph 4 of Schedule 21 to the DPA 2018

---

83 Under Article 49 of the UK GDPR, transfers are possible if one of the following conditions is satisfied: (a) the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards; (b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request; (c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person; (d) the transfer is necessary for important reasons of public interest; (e) the transfer is necessary for the establishment, exercise or defence of legal claims; (f) the transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent; (g) the transfer is made from a register which according to domestic law is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, but only to the extent that the conditions laid down by domestic law for consultation are fulfilled in the particular case. Furthermore, where none of the above conditions are applicable, a transfer may take place only if it is not repetitive, concerns only a limited number of data subjects, is necessary for the purposes of compelling legitimate interests pursued by the controller which are not overridden by the interests or rights and freedoms of the data subject, and the controller has assessed all the circumstances surrounding the data transfer and has on the basis of that assessment provided suitable safeguards with regard to the protection of personal data.

84 Recital 111 of the UK GDPR specifies that transfers in relation to a contract or a legal claim can only take place where they are occasional.

85 ICO guidance on international transfers, available at the following link: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-transfers/#ib7

86 During a period of maximum six months ending at the latest on 30 June 2021, the applicability of this new framework must be read in the light of Article FINPROV.10A of the Trade and Cooperation Agreement between the European Union and the European Atomic Energy Community, of the one part,

(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 an EEA State, Gibraltar, a Union institution, body, office or agency set up by, or on the basis of the EU Treaty, and third countries which were the subject of an EU adequacy decision at the end of the transition period. Consequently, the transfers to these countries can continue as before the UK's withdrawal from the EU. 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 UK 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.

*2.5.8 Accountability*

(83) Under the accountability principle, entities 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.

(84) The principle of accountability provided for in Regulation (EU) 2016/679 has been retained in Article 5(2) of the UK GDPR without material change and the same applies to Article 24 on the responsibility of the controller, Article 25 on data protection by design and by default and Article 30 on records of processing activities. Articles 35 and 36 on data protection impact assessment and prior consultation of supervisory authority have also been retained. Articles 37-39 of Regulation (EU) 2016/679 on designation and the tasks of the data protection officers have been retained in the UK GDPR with no material changes. Furthermore, the provisions of the Articles 40 and 42 of Regulation (EU) 2016/679 on codes of conduct and certification have been retained in the UK GDPR[87].

## 2.6 Oversight and enforcement

*2.6.1 Independent Oversight*

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

(86) 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. The Information Commissioner is a "Corporation Sole": a separate legal entity constituted in a single person. The Information Commissioner is supported in her

---

and the United Kingdom of Great Britain and Northern Ireland, of the other part (L 444/14 of 31.12.2020) ("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

87 Where necessary, these references are replaced with references to the United Kingdom authorities. For example, under Section 17 of the DPA 2018, the Information Commissioner or United Kingdom national accreditation body can accredit a person meeting the requirements set out in Article 43 of the UK GDPR to monitor compliance with a certification.

work by an office. On 31 March 2020 the Information Commissioner's Office had 768 permanent staff[88]. The sponsor-department of the Information Commissioner is the Department for Digital, Culture, Media and Sport[89].

(87) The independence of the Commissioner is explicitly established in Article 52 of the UK GDPR which does not make any substantive changes to Article 52(1)-(3) GDPR. 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.

(88) 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 Her Majesty 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[90], 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[91].

(89) The Information Commissioner holds office for a term of up to seven years. A person cannot be appointed as the Information Commissioner more than once. The Information Commissioner can be removed from office by Her Majesty following an Address by both Houses of Parliament[92]. No request for dismissal of the Information Commissioner can be presented to either House of Parliament unless a Minister has presented a report 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[93].

---

88 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

89 A Management Agreement regulates the relation between the two. In particular, the key responsibilities of DCMS, as sponsoring department, include: ensuring that the Information Commissioner is adequately funded and resourced; representing the interests of the Information Commissioner 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 Information Commissioner's Office 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)

90 Governance Code on Public Appointments, available at the following link: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/578498/governance_code_on_public_appointments_16_12_2016.pdf

91 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

92 An "Address" is a motion laid before Parliament which seeks to make the Monarch aware of Parliament's opinions on a particular issue.

93 Paragraph 3(3) of Schedule 12 to the DPA 2018.

(90) The funding of the Information Commissioner comes from three sources: (i) data protection charges paid by controllers, which are set by Secretary of State's regulations[94] (the Data Protection (Charges and Information) Regulations 2018), and amount to 85% - 90% of the Office's annual budget[95]; (ii) grant in aid paid by the Government to the Information Commissioner. Grant in aid is mainly used to finance the operating costs of the Information Commissioner as regards non-data protection related tasks[96]; and (iii) fees charged for services[97]. At present, no such fees are charged.

(91) The general functions of the Information Commissioner in relation to the processing of personal data that the UK GDPR applies to, are laid down in Article 57 of the UK GDPR, mirroring closely the corresponding rules of Regulation (EU) 2016/679. Its functions include monitoring and enforcement of the UK GDPR, promoting public awareness, handling complaints lodged by the data subjects, conducting investigations etc.. In addition, Section 115 of the DPA 2018 sets out other general functions of the Commissioner, which include a duty to advise Parliament, the government and other institutions and bodies on legislative and administrative measures relating to the protection of individuals' rights and freedoms with regard to the processing of personal data, and a power to issue, on the Commissioner's own initiative or on request, opinions to Parliament, the government or other institutions and bodies as well as to the public on any issue related to the protection of personal data. To maintain the independence of the judiciary, the Information Commissioner is not authorised to exercise her functions in relation to the 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 (see recitals (99) to (103).

*2.6.2 Enforcement, including sanctions*

(92) The powers of the Information Commissioner are set out in Article 58 of the UK GDPR, which introduces no material changes to the corresponding article of Regulation (EU) 2016/679. The DPA 2018 sets out supplementary rules on how these powers can be exercised. In particular, the Commissioner has powers to: (a) order the controller and the processor (and in certain circumstances any other person)

94 Section 137 of the DPA 2018, see recital (16).

95 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) lists the matters which the Secretary of State must have regard to when making regulations which specify the amount different organisations must pay; Secondly, 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.

96 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 89).

97 See Section 134 of the DPA 2018.

to provide necessary information by giving an information notice ("information notice")[98]; (b) 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 etc. ("assessment notice")[99]; (c) obtain otherwise access to documents etc. of controllers and processors and access to their premises in accordance with Section 154 of the DPA 2018 ("powers of entry and inspection"); (d) exercise corrective powers including by means of warnings and reprimands or give orders by means of an enforcement notice, which requires controllers/processors to take or refrain from taking specified steps, including ordering the controller or processor to do anything specified in Article 58(2)(c)-(g) and (j) of the UK GDPR ("enforcement notice")[100]; (e) and issue administrative fines in the form of a penalty notice ("penalty notice")[101].

(93) The ICO's Regulatory Action Policy sets out the circumstances under which it will issue an information, assessment, enforcement or penalty notice[102]. An enforcement notice given in response to a failure by a controller or processor may only impose requirements which the Commissioner considers appropriate for the purpose of remedying the failure. Enforcement and penalty notices may be issued to a controller or processor in relation to violations of Chapter II of the UK GDPR (principles of processing), Articles 12 -22 (rights of the data subject), Articles 25-39 (obligations of controllers and processors) and Articles 44-49 (international transfers) of the UK GDPR. An enforcement notice may also be given where a controller has failed to comply with the requirement to pay a charge in regulations made under Section 137 of the DPA 2018. In addition, a monitoring body under Article 41 or a certification provider can be given an enforcement notice if they fail to comply with their obligations under the UK GDPR. A penalty notice can be also given to a person who has not complied with an information notice, an assessment notice or an enforcement notice.

(94) The penalty notice requires the person to pay to the Information Commissioner an amount specified in the notice. In determining whether to give a penalty notice to a person and determining the amount of the penalty, the Information Commissioner must have regard to the matters listed in Article 83(1) and (2) of the UK GDPR, which are identical to the corresponding rules of Regulation (EU) 2016/679[103]. Under Article 83(4) and (5) the maximum amounts of the administrative fines in case

98 Section 142 of the DPA 2018 (subject to the restrictions in Section 143 of the DPA 2018).

99 Section 146 of the DPA 2018 (subject to the restrictions in Section 147of the DPA 2018).

100 Section 149 to 151 of the DPA 2018 (subject to the restrictions in Section 152 of the DPA 2018).

101 Section 155 of the DPA 2018 and Article 83 of the UK GDPR (subject to the restrictions in Section 156 of the DPA 2018).

102 Regulatory Action Policy, available at the following link: https://ico.org.uk/media/about-the-ico/documents/2259467/regulatory-action-policy.pdf

103 Including the nature and gravity of the infringement (taking into account the nature scope or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them), the intentional or negligent character of the infringement, any action taken by the controller to mitigate the damage suffered by data subjects, the degree of responsibility of the controller or processor (taking into account technical and organisational measures implemented by the controller or processor), any relevant previous infringement by the controller or processor; the degree of cooperation with the Commissioner, the categories of personal data affected by the failure, any other aggravating or mitigating factor applicable to the circumstances of the case, such as financial benefits gained, or losses avoided, directly or indirectly, from the infringement

of a failure to comply with the obligations referred to in those provisions are £8,700,000 or £17,500,000 respectively. In the case of an undertaking, the Information Commissioner can also impose fines as a percentage of worldwide annual turnover, if higher. As in the equivalent provisions of Regulation (EU) 2016/679, these amounts are set at 2% and 4% in Articles 83(4) and (5) respectively. In case of 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 the higher of £17,500,000 or, in the case of an undertaking, 4% worldwide annual turnover.

(95) The UK GDPR together with the DPA 2018 have also strengthened other powers of the Information Commissioner. For example, the Commissioner can now conduct compulsory audits in relation to all controllers and processors through the use of assessment notices, whereas under the previous legislation, the Data Protection Act 1998, the Commissioner only had this power in respect of central government and health organisations, others having to agree to an audit.

(96) Since the introduction of Regulation (EU) 2016/679, the ICO handles about 40,000 complaints from data subjects per year[104] and, in addition, carries out about 2,000 *ex officio* investigations[105]. A majority of complaints are related to the rights of access to and disclosure of data. Following her investigations, the Commissioner is taking enforcement measures across a broad range of sectors. More specifically, according to the Information Commissioner's latest annual report (2019-2020)[106], the Commissioner issued 54 information notices, 8 assessment notices, 7 enforcement notices, 4 cautions, 8 prosecutions and 15 fines during the reporting period[107].

(97) This includes several significant monetary penalties imposed under Regulation (EU) 2016/679 and the DPA 2018. In particular, the Information Commissioner in October 2020 fined a British airline company £20 million for a data breach affecting more than 400,000 customers. At the end of October 2020, an international hotel chain was

---

104 According to the information provided by the UK authorities, during the period covered by the Information Commissioner's Annual Report 2019-2020, no infringement was found in about 25% of the cases, in about 29% of the cases the data subject was asked to either raise the concern with the data controller for the first time, to wait for the controller's reply or to continue an ongoing dialogue with the data controller, in about 17% of the cases, no infringement was found but advice was provided to the data controller, in about 25% of the cases the Information Commissioner found an infringement and either provided advice to the data controller or the data controller was required to take certain actions, in about 3% of the cases it was determined that the complaint did not fall under Regulation (EU) 2016/679, and about 1% of the cases were referred to another data protection authority in the framework of the European Data Protection Board.

105 The ICO can initiate those investigations based on information received from a variety of sources, including personal data breach notifications, referrals from other UK public authorities or foreign data protection authorities, and complaints from individuals or civil society organisations.

106 Information Commissioner's Annual Report and Financial Statements 2019-2020 (see footnote 88).

107 According to the previous annual report covering the period 2018-2019, the Information Commissioner issued 22 penalty notices under the DPA 1998 during the reporting period, with fines totalling £3,010,610, including two fines of £500,000 (the maximum permitted under the DPA 1998). In 2018, the Information Commissioner notably conducted an investigation into the use of data analytics for political purposes following the Cambridge Analytica revelations. The investigation resulted in a policy report, a set of recommendations, a £500,000 fine against Facebook and an enforcement notice to Aggregate IQ, a Canadian data broker, ordering the company to delete personal data it held about United Kingdom citizens and residents (See the Information Commissioner's Annual Report and Financial Statement 2018-2019 available at the following link https://ico.org.uk/media/about-the-ico/documents/2615262/annual-report-201819.pdf)

fined £18.4 million for failing to keep millions of customers' personal data secure and in November 2020 a British service provider selling event tickets online was fined £1.25 million for failing to protect customers' payment details[108].

(98) In addition to the enforcement powers of the Information Commissioner described in recital (93), certain violations of the data protection legislation constitute offences and may therefore be subject to criminal sanctions (Section 196 of the DPA 2018). This applies, for example, to knowingly or recklessly obtaining or disclosing personal data without the consent of the controller, procuring the disclosure of personal data to another person without the consent of the controller[109], re-identifying information that is de-identified personal data without the consent of the controller responsible for de-identifying the personal data[110], intentionally obstructing the Commissioner's power to exercise her powers in relation to the inspection of personal data in accordance with international obligations[111], making false statements in response to an information notice, or destroying information in connection to information and assessment notices[112].

*2.6.3 Oversight over the judiciary*

(99) 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 ICO. Where the controller is operating in a judicial capacity, the ICO cannot exercise its oversight functions[113] and the oversight is carried out by special bodies. This reflects the approach taken in Regulation (EU) 2016/679 (Article 55(3)).

(100) 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[114]. Additionally, the Lord Chief Justice and Senior

---

108 For a summary of enforcement actions taken, see the ICO website, available at the following link: https://ico.org.uk/action-weve-taken/enforcement/

109 Section 170 of the DPA 2018.

110 Section 171 of the DPA 2018.

111 Section 119 of the DPA 2018.

112 Sections 144 and 148 of the DPA 2018.

113 Section 117 of the DPA 2018.

114 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.

President of Tribunals have issued a Privacy Notice[115] 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[116] and Scottish judiciaries[117].

(101) Moreover, in Northern Ireland, the Lord Chief Justice of Northern Ireland has appointed a High Court judge as Data Supervisory Judge (DSJ)[118]. 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[119].

(102) 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[120].

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

*2.6.4 Redress*

(104) 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.

(105) 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 the UK GDPR[121]. The UK GDPR retains the rules in Article 77 of Regulation (EU) 2016/679 on that right without material modifications. The same applies to Article 57(1)(f) and (2) that set out the tasks of the Commissioner in relation to the handling of complaints. As described in recitals (92) to (98) above, the Information Commissioner has the power to assess the compliance of the controller and processor with the UK GDPR and DPA 2018, require them to take or refrain from taking necessary steps in case of non-compliance and to impose fines.

---

115 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

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

117 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

118 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.

119 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

120 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)

121 Article 77 of the UK GDPR.

(106) Second, the UK GDPR and DPA 2018 provide the right to a remedy against the Information Commissioner. Pursuant to Article 78(1) of the UK GDPR, an individual has a right to an effective judicial remedy against a legally binding decision of the Commissioner concerning them. In the context of the judicial review, the judge examines the decision being challenged in the claim, and considers whether the Information Commissioner has acted lawfully. Moreover, pursuant to Article 78(2) of the UK GDPR, if the Commissioner fails to appropriately handle a complaint made by the data subject,[122] the complainant has access to judicial remedy. It can apply to a First Tier Tribunal to order the Commissioner to take appropriate steps to respond to the complaint, or to inform the complainant of progress on the complaint[123]. In addition, any person who is served one of the abovementioned notices (information, assessment, enforcement or penalty notice) by the Commissioner may appeal to a First Tier Tribunal[124]. If the Tribunal considers that the decision of the Commissioner is not in accordance with the law or the Information Commissioner should have exercised her discretion differently, the Tribunal must allow the appeal, or substitute another notice or decision which the Information Commissioner could have given or made.

(107) Third, individuals can obtain judicial redress against controllers and processors directly before the courts under Article 79 of the UK GDPR and 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.

(108) Moreover, under Article 82 of the UK GDPR and Section 168 of the DPA 2018, any person who has suffered material or non-material damage as a result of an infringement of the UK GDPR has the right to receive compensation from the controller or processor for the damage suffered. The rules on the compensation and liability in Article 82(1) – (5) of the UK GDPR are identical with the corresponding rules in Regulation (EU) 2016/679. Under Section 168 of the DPA 2018, non-material damage includes also distress. Under Article 80 of the UK GDPR the data subject has also a right to mandate a representative body or organisation to lodge the complaint with the Commissioner on his or her behalf (under Article 77 of the UK GDPR) and to exercise the rights referred to in Articles 78 (right to an effective judicial remedy against the Commissioner), 79 (right to an effective judicial remedy against a controller or processor) and 82 (right to compensation and liability) of the UK GDPR on his or her behalf.

(109) Fourth, and in addition to the avenues for redress, any person that considers that his or her rights, including rights to privacy and data protection, have been violated by public authorities, can obtain redress before the United Kingdom courts under the

---

122 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.

123 Article 78(2) of the UK GDPR and Section 166 of the DPA 2018.

124 Article 78(1) of the UK GDPR and Section 162 of the DPA 2018.

Human Rights Act 1998[125]. 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.

(110) 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[126]. The court can also declare a provision of primary legislation to be incompatible with a Convention right.

(111) 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 European Convention of Human Rights.

## 3. ACCESS AND USE OF PERSONAL DATA TRANSFERRED FROM THE EUROPEAN UNION BY PUBLIC AUTHORITIES IN THE UNITED KINGDOM

(112) The Commission also assessed the United Kingdom's legal framework for the collection and subsequent use of personal data transferred to business operators in the United Kingdom by United Kingdom public authorities in the public interest, in particular for criminal law enforcement and national security purposes (hereinafter referred to as "government access"). In assessing whether the conditions under which government access to data transferred to the UK under this Decision would fulfil the "essential equivalence" test pursuant to Article 45(1) of Regulation (EU) 2016/679, as interpreted by the Court of Justice of the European Union in light of the Charter of Fundamental Rights, the Commission took into account in particular the following criteria.

(113) First, any limitation to the right to the protection of personal data must be provided for by law and the legal basis which permits the interference with such a right must itself define the scope of the limitation on the exercise of the right concerned[127].

(114) Second, in order to satisfy the requirement of proportionality, according to which derogations from and limitations to the protection of personal data must apply only in so far as is strictly necessary in a democratic society to meet specific objectives of general interest equivalent to those recognized by the Union, the legislation of the third country in question which permits the interference must lay down clear and precise rules governing the scope and application of the measures in question and impose minimum safeguards so that the persons whose data has been transferred have sufficient guarantees to protect effectively their personal data against the risk of

---

125 Section 7(1) of the Human Rights Act 1998. According to Section 7(7) a person is a victim of an unlawful act only if he would be a victim for the purposes of Article 34 of the European Convention of Human Rights if proceedings were brought in the European Court of Human Rights in respect of that act.

126 Section 8(1) of the Human Rights Act 1998.

127 See *Schrems II*, paragraphs174-175 and the case-law cited. See also, as regards access by public authorities of Member States, Case C-623/17 *Privacy International* ECLI:EU:C:2020:790, paragraph 65; and Case Joined Cases C-511/18, C-512/18 and C-520/18 *La Quadrature du Net and Others* ECLI:EU:C:2020:791, paragraph 175.

abuse[128]. The legislation must, in particular, indicate in what circumstances and under which conditions a measure providing for the processing of such data may be adopted[129] as well as subject the fulfilment of such requirements to independent oversight[130].

(115) Third, that legislation must be legally binding under domestic law and these legal requirements must not only be binding on the authorities, but also enforceable before courts against the authorities of the third country in question[131]. In particular, data subjects must have the possibility of bringing legal action before an independent and impartial court in order to have access to their personal data, or to obtain the rectification or erasure of such data[132].

### 3.1 General legal framework

(116) As an exercise of power by a public authority, government access in the United Kingdom must be carried out in full respect of the law. The United Kingdom has ratified the European Convention of Human Rights (see recital (8)) and all public authorities in the United Kingdom are required to act in compliance with the Convention[133]. Article 8 of the Convention provides that any interference with privacy must be in accordance with the law, in the interests of one of the aims set out in Article 8(2), and proportionate in light of that aim. Article 8 also requires that the interference is "foreseeable", i.e. have a clear, accessible basis in law, and that the law contains appropriate safeguards to prevent abuse.

(117) In addition, in its case law, the European Court of Human Rights has specified that any interference with the right to privacy and data protection should be subject to an effective, independent and impartial oversight system that must be provided for either by a judge or by another independent body[134] (e.g. an administrative authority or a parliamentary body).

(118) Moreover, individuals must be provided with an effective remedy, and the European Court of Human Rights has clarified that the remedy must be offered by an independent and impartial body which has adopted its own rules of procedure, consisting of members that must hold or have held high judicial office or be experienced lawyers, and that there must be no evidential burden to be overcome in order to lodge an application with it. In undertaking its examination of complaints by individuals, the independent and impartial body should have access to all relevant

---

128 See *Schrems II*, paragraphs 176 and 181, as well as the case-law cited. See also, as regards access by public authorities of Member States, *Privacy International*, paragraph 68; and *La Quadrature du Net and Others*, paragraph 132.

129 See *Schrems II*, paragraph 176. See also, as regards access by public authorities of Member States, *Privacy International*, paragraph 68; and *La Quadrature du Net and Others*, paragraph 132.

130 See *Schrems II*, paragraph 179.

131 See *Schrems II*, paragraphs 181-182.

132 See *Schrems I*, paragraph 95 and Schrems *II*, paragraph 194. In that respect, the CJEU has notably stressed that compliance with Article 47 of the Charter of Fundamental Rights, guaranteeing the right to an effective remedy before an independent and impartial tribunal, "contributes to the required level of protection in the European Union [and] must be determined by the Commission before it adopts an adequacy decision pursuant to Article 45(1) of Regulation (EU) 2016/679" (*Schrems II*, paragraph 186).

133 Section 6 of the Human Rights Act 1998.

134 European Court of Human Rights, *Klass and others v. Germany*, Application no. 5029/71, paragraphs 17-51.

information, including closed materials. Finally, it should have the powers to remedy non-compliance[135].

(119) 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), and 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[136]. Article 9 of Convention 108 provides that derogations from the general data protection principles (Article 5 Quality of data), the rules governing special categories of data (Article 6 Special categories of data) and data subject rights (Article 8 Additional safeguards to the data subject) are only permissible when such derogation is provided for by the law of the Party and constitutes a necessary measure in a democratic society in the interests of protecting State security, public safety, the monetary interests of the State or the suppression of criminal offences, or for protecting the data subject or the rights and freedoms of others[137].

(120) Therefore, through membership of the Council of Europe, adherence to the European Convention of Human Rights and submission to the jurisdiction of the European Court of Human Rights, the UK is subject to a number of obligations, enshrined in international law, that frame its system of government access on the basis of principles, safeguards and individual rights similar to those guaranteed under EU law and applicable to the Member States. As stressed in recital (18), continued adherence to such instruments is therefore a particularly important element of the assessment on which this Decision is based.

(121) Further, specific data protection safeguards and rights are guaranteed by the DPA 2018 when data is processed by public authorities, including by law enforcement and national security bodies.

(122) In particular, the regime for the processing of personal data in the context of criminal law enforcement is set out in Part 3 of the DPA 2018, which was enacted to transpose Directive (EU) 2016/680. Part 3 of the DPA 2018 applies 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, including the safeguarding against and the prevention of threats to public security[138]. It applies to "competent authorities" listed in Schedule 7 to the DPA 2018 as well as to any other person that has statutory functions for any of the law enforcement purposes[139]. For example, competent authorities under Part 3 of the DPA 2018 include all UK Ministerial government departments, the police, other

---

135 European Court of Human Rights, *Kennedy v. the United Kingdom*, Application no. 26839/05, ("*Kennedy"*), paragraphs 167 and 190.

136 For more information on the European Convention of Human Rights and its incorporation into United Kingdom law through the Human Rights Act 1998 as well as on Convention 108, see recital (8) above.

137 Similarly, pursuant to Article 11 of Convention 108+, restrictions to certain specific rights and obligations of the Convention for purposes of national security or the prevention, investigation and prosecution of criminal offences and the execution of criminal penalties are only permissible when such a restriction is provided for by law, respects the essence of the fundamental rights and freedoms, and constitutes a necessary and proportionate measure in a democratic society. Processing activities for national security and defence purposes must also be subject to independent and effective review and supervision under the domestic legislation of the respective Party to the Convention

138 Section 31 of the DPA 2018.

139 Section 30 of the DPA 2018 and Schedule 7 to the DPA 2018.

authorities with investigatory functions[140], prosecutorial agencies, other criminal justice agencies and other holders or organisations that carry out law enforcement activities.

(123) Similarly to Directive (EU) 2016/680, Part 3 of the DPA 2018 sets out the principles of lawfulness and fairness[141], purpose limitation[142], data minimisation[143], accuracy[144], storage limitation[145] and security[146]. The legislation imposes specific transparency obligations[147] and provides individuals with a right of access[148], rectification and deletion[149] and the right not to be subject to automated decision-making[150]. The competent authorities are also required to implement data protection by design and default, to keep records of processing activities, and, for certain processing operations, to carry out data protection impact assessments and to pre-consult the Information Commissioner[151]. Pursuant to Section 56 of the DPA 2018, they are required to demonstrate compliance. Moreover, they are required to put in place appropriate measures to ensure security of processing[152] and are subject to specific obligations in case of a data breach, including notification of such breaches to the Information Commissioner and data subjects[153]. As is the case in Directive (EU) 2016/680, there is also a requirement for a controller (unless it is a court or other judicial authority acting in a judicial capacity) to designate a data protection officer (DPO)[154] which assists the controller in complying with its obligations as well as monitoring that compliance[155]. Furthermore, the legislation imposes specific requirements for international transfers of personal data for law enforcement purposes to third countries or international organisations to ensure continuity of protection[156]. At the same date as this Decision, the Commission [has adopted] an adequacy decision on the basis of Article 36(3) of Directive (EU) 2016/680, finding that the data protection regime applicable to processing by UK criminal law enforcement authorities ensures a level of protection essentially equivalent to the one guaranteed by Directive (EU) 2016/680.

(124) Part 4 of the DPA 2018 applies to all processing by or on behalf of the intelligence services. In particular, it sets out the main data protection principles (lawfulness, fairness and transparency[157]; purpose limitation[158]; data minimisation[159]; accuracy[160];

---

140 For example, the Commissioner for Her Majesty's Revenue and Customs, the Welsh Revenue Authority, the Competition and Markets Authority or Her Majesty's Land Register.

141 Section 35 of the DPA 2018.

142 Section 36 of the DPA 2018.

143 Section 37 of the DPA 2018.

144 Section 38 of the DPA 2018.

145 Section 39 of the DPA 2018.

146 Section 40 of the DPA 2018.

147 Section 44 of the DPA 2018.

148 Section 45 of the DPA 2018.

149 Section 46 and 47 of the DPA 2018.

150 Section 49 and 50 of the DPA 2018.

151 Sections 56-65 of the DPA 2018.

152 Section 66 of the DPA 2018.

153 Section 67-68 of the DPA 2018.

154 Sections 69–71 of the DPA 2018.

155 Section 67-68 of the DPA 2018.

156 Chapter 5 of Part 3 of the DPA 2018.

157 Under Section 86(6) of the DPA 2018, to determine fairness and transparency of the processing, the method by which it is obtained must be regarded. In this sense, the fairness and transparency

storage limitation[161] and security[162]), imposes conditions on the processing of special categories of data[163], provides for data subject rights[164], requires data protection by design[165] and regulates international transfers of personal data[166].

(125) At the same time, Section 110 of the DPA 2018 provides for an exemption from specified provisions in Part 4 of the DPA 2018[167] when such exemption is required to safeguard national security. This exemption can be relied upon on the basis of a case-by-case analysis[168]. As explained by the UK authorities and confirmed by the case law, 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"[169]. Whether or not the exemption has been used appropriately is subject to the oversight of the ICO[170].

---

requirement is accomplished if data is obtained from a person who is lawfully authorised or required to supply it.

158 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 Section 87(3) of the DPA 2018, 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).

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

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

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

162 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.

163 Section 86(2)(b) and Schedule 10 to the DPA 2018.

164 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.

165 Section 103 of the DPA 2018.

166 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.

167 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.

168 See *Baker v Secretary of State*, see footnote 69.

169 UK Explanatory Framework for Adequacy Discussions, section H: National Security Data Protection and Investigatory Powers Framework, page 15-16 (see footnote 29). See also *Baker v Secretary of State* (see footnote 69), in which the court 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

(126) Moreover, in relation to the possibility to restrict for the protection of "national security" the application of these specified provisions of Part 4 of DPA 2016, a controller may apply for a certificate signed by a Cabinet Minister or the Attorney General certifying that a restriction of such rights is a necessary and proportionate measure to the protection of national security[171]. The UK government has issued guidance to assist controllers when considering whether to apply for a national security certificate under the DPA 2018, that notably highlight that any limitation to data subjects' rights for safeguarding national security must be proportionate and necessary[172].

(127) The certificate should be for a fixed duration of no more than five years, so to be regularly reviewed by the Executive[173]. 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[174]. The controller or processor can only rely on a certificate when it has concluded it is necessary to rely on the national security exemption which, as explained above, must be applied on a case-by-case basis[175]. 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[176].

(128) Any person directly affected by the issuing of the certificate may appeal to the Upper Tribunal[177] against the certificate[178] or, where the certificate identifies data by means of a general description, challenge the application of the certificate to specific data[179]. The tribunal will review the decision to issue a certificate and decide whether there

---

allowing such exception in all circumstances without a case-by-case analysis exceeded what was necessary and proportionate for the protection of national security.

170 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 Understandings between Information Commission's Office and the UK 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

171 Section 111 of the DPA 2018.

172 UK 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 According to the explanation provided by the UK authorities, while a certificate is conclusive proof that, in respect to data or processing described in the certificate, the exemption is applicable, it does not remove the requirement for the controller to consider whether there is a need to rely on the exemption on a case-by-case basis.

173 UK Government Guidance on National Security Certificates, paragraph 15, see footnote 172.

174 UK Government Guidance on National Security Certificates, paragraph 5, see footnote 172.

175 See footnote 169.

176 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/

177 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.

178 Section 111(3) of the DPA 2018.

179 Section 111(5) of the DPA 2018.

were reasonable grounds for issuing the certificate[180]. 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[181].

(129) 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[182] 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")[183]. 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.

(130) It follows from the above that limitation and conditions are in place under the applicable UK 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.

### 3.2 Access and use by United Kingdom public authorities for criminal law enforcement purposes

(131) The law of the United Kingdom imposes a number of limitations on the access and use of personal data for criminal law enforcement purposes, and provides oversight and redress mechanisms in this area which are in line with the requirements referred to in recitals (113) to (115) of the present decision. The conditions under which such

180 In *Baker v Secretary of State* (see footnote 69), 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.

181 UK Government Guidance on National Security Certificates, paragraph 25, see footnote 172.

182 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.

183 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 29.

access can take place and the safeguards applicable to the use of these powers are assessed in detail in the following sections.

*3.2.1 Legal bases and applicable limitations/safeguards*

(132) Pursuant to the principle of lawfulness guaranteed under Section 35 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[184] or the processing is necessary for the performance of a task carried out for that purpose by a competent authority.

3.2.1.1 Search warrants and production orders

(133) In the United Kingdom legal framework, the collection of personal data from business operators, including those that would be processing data transferred from the EU under the present adequacy decision, for purposes of criminal law enforcement is permissible on the basis of search warrants[185] and production orders[186].

(134) Search warrants are issued by a court, usually on the application of the investigating officer. They permit an officer to enter premises to search for material or individuals relevant to their investigation and retain anything for which a search has been authorised, including any relevant documents or material containing personal data[187]. A production order, which also needs to be issued by a court, requires the person specified in it to produce or give access to material they are in possession or control of. The applicant must justify to the court why the warrant or order is necessary, as well as why it is in the public interest. There are several statutory powers that permit the issuance of search warrants and production orders. Each provision has its own set

184 The use of consent does not appear relevant in an adequacy scenario as in a transfer situation the data will not have been directly collected from an EU data subject by a UK law enforcement authority on the basis of consent.

185 For the relevant legal basis, See Sections 8 et seq. of PACE 1984 (for England and Wales), Sections 10 et seq, of the Police and Criminal Evidence Order (Northern Ireland) 1989 and for Scotland it is obtained under common law (see Section 46 of the Criminal Justice (Scotland) Act 2016) and Section 23B of the Criminal Law (Consolidation) (Scotland). For search warrant issued after the arrest the legal basis is section 18 of PACE 1984 (for England and Wales), Sections 20 et seq., of the Police and Criminal Evidence Order (Northern Ireland) 1989 and for Scotland it is obtained under common law (see Section 46 of the Criminal Justice (Scotland) Act 2016). UK authorities clarified that search warrants are issued by a court, on the application of the investigating officer. They permit an officer to enter premises to search for material or individuals relevant to their investigation; the execution of the warrant will often require the assistance of a police constable.

186 When the investigation concerns money laundering (including confiscation and civil recovery proceedings), the relevant legal basis for applying for a production order are Sections 345 et seq. for England, Wales and Northern Ireland and sect 380 et seq. of Proceeds of Crime Act 2002 for Scotland. When the investigation concerns other issues than money laundering, an application for a production order can be made under Section 9 and Schedule 1 to the PACE 1984 for England and Wales, and Section 10 et seq. of the Police and Criminal Evidence Order (Northern Ireland) 1989 for Northern Ireland. For Scotland it is obtained under common law (see Section 46 of the Criminal Justice (Scotland) Act 2016) and Section 23B of the Criminal Law (Consolidation) (Scotland). UK authorities clarified that a production order requires the person specified in it to produce or to give access to the material they are in possession or control of (see para 4 of Schedule 1 to the PACE 1984).

187 For instance, the PACE 1984 contains powers in Sections 8 and 18 to seize and retain anything for which a search has been authorised.

of statutory conditions which must be satisfied for a warrant[188] or a production order[189] to be issued.

[188] For example, Section 8 and Section 18 of PACE regulate respectively the power of a justice of the peace to authorise a warrant and of a police officer to search a property. In the first case (Section 8), before issuing a warrant a justice of the peace must first be satisfied that there are reasonable grounds for believing that: (i) an indictable offence has been committed; (ii) there is material on the premises which is likely to be of substantial value (whether by itself or together with other material) to the investigation of the offence; (iii) the material is likely to be relevant evidence; (iv) it does not consist of or include items subject to legal privilege, excluded material or special procedure material; and (v) it wouldn't be possible to obtain entry without the use of a warrant. In the second case, Section 18 allows a police officer to search the premises of a person arrested for an indictable offence for material other than material subject to legal privilege if they have reasonable grounds for suspecting that there is evidence on the premises that relate to that offence or another similar or connected indictable offence. Such a search must be limited to uncovering that material and must be authorised, in writing, by a police officer of at least the rank of inspector unless it is necessary for the investigation of the offence. In which case, an officer of the rank of at least inspector must be informed as soon as practicable after it has been carried out. The grounds for the search and nature of the evidence sought must be recorded. Moreover, Sections 15 and 16 the PACE 1984 provide statutory safeguards that must be followed when applying for a search warrant. Section 15 specifies the requirements applicable for obtaining a search warrant (including the content of the application made by the constable and the fact that the warrant must specify, among the other things, the enactment under which it is issued and identify, as far as possible, the articles and persons to be sought and the premises to be searched). Section 16 governs how a search under a warrant must be carried out (for example: section 16(5) provides that the officer executing the warrant provides the occupier with a copy of the warrant; section 16(11) requires that the warrant, once executed, be retained for a period of 12 months; Section 16(12) provides the occupier with the right to inspect the warrant during that period if they so wish). These Sections help ensure compliance with Art. 8 ECHR (see for instance Kent Pharmaceuticals v Director of the Serious Fraud Office [2002] EWHC 3023 (QB) at [30] by Lord Woolf CJ). A failure to comply with these safeguards can result in the search being declared unlawful (examples include R (Brook) v Preston Crown Court [2018] EWHC 2024 (Admin), [2018] ACD 95; R (Superior Import / Export Ltd) v Revenue and Customs Commissioners [2017] EWHC 3172 (Admin), [2018] Lloyd's Rep FC 115; and R (F) v Blackfriars Crown Court [2014] EWHC 1541 (Admin)). Sections 15 and 16 of PACE 1984 are supplemented by Code B of PACE, a code of practice which governs the exercise of police powers to search premises.

[189] For instance, when issuing a production order under the Proceeds of Crime Act 2002, in addition to the need to have reasonable grounds to meet the conditions set in out in 346(2) Proceeds of Crime Act, there should be reasonable grounds that the person is in possession or control of the material so specified and that the material is likely to be of substantial value. Moreover, another requirement for issuing a production order is that there must be reasonable grounds for believing that it is in the public interest for the material to be produced or for access to it to be given, having regard to (a) the benefit likely to accrue to the investigation if the material is obtained; and (b) the circumstances under which the person the application specifies as appearing to be in possession or control of the material holding their information. Similarly, a court considering an application for a production order under Schedule 1 to the PACE 1984 must be satisfied that specific conditions are met. In particular, Schedule 1 of PACE sets out two separate alternative sets of conditions, one of which must be met before a judge can issue a production order. The first set requires that the judge has reasonable grounds for believing (i) that an indictable offence has been committed; (ii) the material sought on the premises consists of, or includes, special procedure but not excluded material; (iii) it is likely to be of substantial value, whether on its own or together with other material, to the investigation; (iv) and that it is likely to be relevant evidence; (v) other methods of obtaining the material have either been attempted or have not been attempted because they would be bound to fail; and (vi) having considered the benefit to the investigation and the circumstances under which the individual possesses it is in the public interest that the material be produced or that access to it be provided. The second set of conditions requires: (i) there is material on the premises which consists of special procedure or excluded material; (ii) were it not for the prohibition on searches carried out on the basis of legislation passed before PACE for special procedure, excluded or legal privilege material, a search warrant for the material could have been issued; and (iii) it would have been appropriate to do so.

(135) Production orders and search warrants may be challenged by way of judicial review[190]. In terms of safeguards, all competent authorities under Part 3 of the DPA 2018, including the police, may only access personal data – which is a form of processing – in line with the principles and requirements set out in the DPA 2018 (see recitals (122) and (123) above). Therefore, a request made by any law enforcement authority should be in compliance with the principle according to which the purposes of processing must be specified, explicit and legitimate[191] and that the personal data processed by a competent authority must be relevant to that purpose and not excessive[192].

(136) Moreover, for law enforcement authorities different from the police, in addition to the safeguards provided by the Part 3 of the DPA 2018, specific and additional safeguards may be provided by the statutes empowering them.

3.2.1.2 Investigatory powers for law enforcement purposes

(137) For the purpose of preventing or detecting serious crimes[193], certain law enforcement authorities[194] can use targeted investigatory powers, namely targeted interception (Part 2 of the IPA 2016), acquisition of communications data (Part 3 of the IPA 2016), retention of communications data (Part 4 of the IPA 2016) and targeted equipment interference (Part 5 of the IPA 2016). Interception covers the acquisition of the content of a communication[195] while acquisition and retention of communications data is not aimed at obtaining the content of the communication, but at the "who", "when", "where" and "how" of the communication. This covers for

190 Judicial review is the legal procedure by which the decisions of a public body can be challenged in the High Court. The Courts "review" the decision being challenged and decide if it is arguable that the decision is legally flawed, considering public law concepts/principles. The core grounds for judicial review are namely, illegality, irrationality, procedural impropriety, legitimate expectations and human rights. Following a successful judicial review a court is able to order a number of different remedies; the most common of which is a quashing order (which would set aside or cancel the original decision - i.e. the decision to issue a search warrant), in some circumstances this can also include the award of financial compensation. Additional detail on judicial review in the UK is available in the Government Legal Department's publication "Judge Over Your Shoulder – a guide to good decision-making", available at the following link: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/746170/JOYS-OCT-2018.pdf

191 Section 36(1) of the UK DPA 2018.

192 Section 37 of the UK DPA 2018.

193 Section 263(1) of the IPA 2016 provides that "serious crime" means an offence for which an adult, who had no previous conviction, could reasonably be expected to be sentenced to imprisonment for a term of 3 years or more or the conduct involves the use of violence, results in substantial financial gain or is conduct by a large number of persons. Moreover, for the purposes of the acquisition of communications data under Part 4 of the IPA 2016, Section 87(10B) provides that "serious crime" means a crime for which a sentence of imprisonment of 12 months or more can be imposed or an offence committed by a person who is not an individual or which involves, as an integral part of it, the sending of a communication or a breach of a person's privacy.

194 The following law enforcement authorities can apply for a targeted interception warrant: the Director General of the National Crime Agency, the Commissioner of Police of the Metropolis, the Chief Constable of the Police Service of Northern Ireland, the Chief Constable of the Police Service of Scotland, the Commissioner for Her Majesty's Revenue and Customs, the Chief of Defence Intelligence and a person who is a competent authority of a country or territory outside the United Kingdom for the purposes of an EU mutual assistance instrument or an international mutual assistance agreement (Section 18(1) of the IPA 2016).

195 See Section 4 of the IPA 2016.

instance the time and duration of a communication, the phone number or email address of the originator and recipient of the communication, and sometimes the location of the devices from which the communication was made, the subscriber to a telephone service or an itemised bill[196]. Equipment interference is a set of techniques used to obtain a variety of data from equipment, which includes computers, tablets and smart phones as well as cables, wires and storage devices[197].

(138) Targeted interception powers can also be used when "necessary for the purpose of giving effect to the provisions of an EU mutual assistance instrument or an international mutual assistance agreement" (so-called "mutual assistance warrant"[198]). Mutual assistance warrants are only provided in relation to interception, not acquisition of communications data or equipment interference. These targeted powers are regulated in the Investigatory Powers Act 2016 (IPA 2016)[199], which, together with the Regulation of Investigatory Powers Act 2000 (RIPA) for England, Wales and Northern Ireland and the Regulation of Investigatory Powers (Scotland) Act 2000 (RIPSA) for Scotland, provide for the legal basis and set out the applicable limitations and safeguards for the use of such powers. The IPA 2016 also provides the regime for the use of bulk investigatory powers, although those are not available to law enforcement authorities (only intelligence agencies can make use of them)[200].

(139) In order to exercise these powers, the authorities need to obtain a warrant[201] issued by a competent authority[202], and approved by an independent Judicial Commissioner[203] (so-called "double-lock" procedure). The obtaining of such a warrant is subject to a necessity and proportionality test[204]. Since these targeted

196 See Section 261(5) of the IPA 2016 and Code of Practice on Bulk Acquisition of Communications Data, available at the following link: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715477/Bulk_Communications_Data_Code_of_Practice.pdf, paragraph 2.9.

197 Code of Practice on Equipment Interference, available at the following link: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715479/Equipment_Interference_Code_of_Practice.pdf , paragraph 2.2.

198 A mutual assistance warrant authorises a UK authority to provide assistance to an authority outside the UK territory for the interception and the disclosure of the intercepted material to such authority, in accordance with an international mutual assistance instrument (Section 15(4) of the IPA 2016).

199 The Investigatory Powers Act 2016 (see: https://www.legislation.gov.uk/ukpga/2016/25/contents/enacted) replaced a different laws concerning the interception of communications, equipment interference and the acquisition of communication data, in particular Part I of the RIPA 2000 that provided the previous general legislative framework for the use of investigatory powers by law enforcement and national security authorities.

200 Sections 138(1), 158(1), 178(1), 199(1) of the IPA 2016.

201 Chapter 2 of Part 2 of the IPA 2016 provides for a limited number of cases where interceptions can be performed without a warrant. This includes: interception with the consent of the sender or the recipient, interception for administrative or enforcement purposes, interception taking place in certain institutions (prisons, psychiatric hospitals and immigration detention facilities) as well as interception carried out in accordance with a relevant international agreement.

202 In most of the cases, the Secretary of State is the authority that issues the warrants under the IPA 2016, while Scottish Ministers are empowered to issue targeted interception warrants, mutual assistance warrant and targeted equipment interference warrants when the persons or premises to be intercepted and the equipment to be interfered are located in Scotland (see Sections 22 and 103 of the IPA 2016). In case of targeted equipment interference, a law enforcement chief (described in Part 1 and Part 2 of Schedule 6 to the IPA 2016) can issue the warrant under the conditions of Section 106 of the IPA 2016.

203 Judicial Commissioners assist the Investigatory Powers Commissioner (IPC), an independent body which exercises oversight functions over the use of investigative powers by intelligence agencies (see for more details recital (160) et seq.).

204 See, in particular, Section 19 and 23 of IPA 2016.

investigatory powers provided by the IPA 2016 are the same as those available to national security agencies, the conditions, limitations and safeguards applicable to such powers are addressed in detail in the Section on access and use of personal data by UK public authorities for national security purposes (see recitals (174) and following).

### *3.2.2 Further use of the information collected*

(140) The sharing of data by a law enforcement authority with a different authority for purposes other than the ones for which it was originally collected (so-called "onward sharing") is subject to certain conditions.

(141) 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 to that purpose[205]. In this case, all the safeguards provided by Part 3 of the DPA 2018, referred to in recitals (122) and (123) apply to the processing carried out by the receiving authority.

(142) In the UK legal order, different laws explicitly allow such 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 public authorities[206] or in case of a debt owed to a public authority or to the Crown[207]; (ii) the Crime and Courts Act 2013 that permits the sharing of information with the National Crime Agency (NCA)[208] for combating, investigating and prosecuting serious and organised crime; (iii) the Serious Crime Act 2007 that allows public authorities to disclose information to anti-fraud organisations for the purposes of preventing fraud[209].

(143) These laws explicitly provide that the sharing of information should be in compliance with the principles set in the DPA 2018. Moreover, the College of Policing has issued an Authorised Professional Practice on Information Sharing[210] 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 is, of course, subject to judicial review[211].

---

205 Section 36(3) of the DPA 2018.

206 Section 56 of the Digital Economy Act 2017, available at the following link: https://www.legislation.gov.uk/ukpga/2017/30/section/56

207 Section 48 of the Digital Economy Act 2017.

208 Section 7 of the Crime and Courts Act 2013, available at the following link: https://www.legislation.gov.uk/ukpga/2013/22/section/7

209 Section 68 of the Serious Crime Act 2007, available at the following link: https://www.legislation.gov.uk/ukpga/2007/27/contents

210 Authorised Professional Practice on Information Sharing, available at the following link: https://www.app.college.police.uk/app-content/information-management/sharing-police-information

211 See for example case *M, R 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 schemes, 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 to some sensitive information shared between the police and BCRP. Another example is case

(144) 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[212].

(145) 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, etc.); and 2) when a criminal law 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. The Commission has assessed the safeguards provided by the UK GDPR and Part 2 of the DPA 2018 in recitals (11)-(111) and has come to the conclusion that the United Kingdom ensures an adequate level of protection for personal data transferred within the scope of Regulation (EU) 2016/679 from the European Union to the United Kingdom.

(146) 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 Section 19 of the Counter Terrorism Act 2008 (CTA 2008)[213]. Under this Act, 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".

(147) As regards the conditions under which data can be shared for national security purposes, the Intelligence Services Act[214] and the Security Services Act[215] limit the ability of the intelligence services to obtain data to what is necessary to discharge their statutory functions. Law enforcement agencies 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[216]. Section 20 of the CTA 2008 makes

---

*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.

212 Section 36(4) of the DPA 2018.

213 Counter Terrorism Act 2008, available at the following link: https://www.legislation.gov.uk/ukpga/2008/28/section/19

214 Intelligence Services Act 1994, available at the following link: https://www.legislation.gov.uk/ukpga/1994/13/contents

215 Security Services Act 1989, available at the following link: https://www.legislation.gov.uk/ukpga/1989/5/contents

216 Section 2(2) of the Intelligence Service Act 1994 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 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

clear that any data sharing pursuant to Section 19 must still comply with the data protection legislation; which means that all of the limitations and requirements in Part 3 of the DPA 2018 apply. Furthermore, as competent authorities are public authorities for the purpose of the Human Rights Act 1998, they must ensure that they act in compliance with Convention rights, including Article 8 of the ECHR. These limits ensure that all data sharing between the law enforcement agencies and the intelligence services complies with data protection legislation and the ECHR.

(148) When a competent authority intends to share personal data processed under Part 3 of the DPA 2018 with law enforcement authorities of a third country, specific requirements apply[217]. In particular, such transfers may take place when they are based on adequacy regulations made by the Secretary of State or, in the absence of such regulations, appropriate safeguards must be ensured. Section 75 of the DPA 2018 provides that appropriate safeguards are in place where established by a legal instrument binding the intended recipient, or where the controller, having assessed all the circumstances surrounding transfers of that type of personal data to the third country or international organization, concludes that appropriate safeguards exist to protect the data.

(149) If a transfer is not based on an adequacy regulation or appropriate safeguards, it can take place only in certain, specified circumstances, referred to as "special circumstances"[218]. 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 member state or third country; (d) in individual cases for any of the law enforcement purposes; or (e) in individual cases for a legal purpose (such as in relation to legal proceedings or to obtain legal advice). It may be noted that (d) and (e) do not apply if the rights and freedoms of the data subject override the public interest in the transfer. This set of circumstances corresponds to the specific situations and conditions qualifying as "derogations" under Article 38 of Directive (EU) 2016/680.

(150) Moreover, when the material acquired by law enforcement authorities under a warrant authorising the use of interception or equipment interference is handed over to a third country, the IPA 2016 imposes additional safeguards. In particular, such disclosure, defined as "overseas disclosure", is allowed only if the issuing authority considers that specific appropriate arrangements are in place which limit the number of persons to whom the data is disclosed, the extent to which any material is disclosed or made available as well as the extent to which any of the material is copied and the number of copies made. Moreover, the issuing authority may consider that appropriate arrangements are necessary to ensure that every copy made of any part of that material is destroyed as soon as there are no longer any relevant grounds for retaining it (if not destroyed earlier)[219].

---

party; and (c) that there are arrangements, agreed with Director General of the National Crime Agency, for co-ordinating 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".

217 See Chapter 5 of Part 3 of the DPA 2018.

218 Section 76 of the DPA 2018.

219 Section 54 and section 130 of the IPA 2016. The issuing authorities must consider the need to impose specific safeguards to the material handed over to foreign authorities, as to make sure that the data is

(151) Finally, specific forms of onward transfers from the United Kingdom to the United States could in the future take place based on the "Agreement between the Government of the United Kingdom of Great Britain and Northern Ireland and the Government of the United States of America on Access to Electronic Data for the Purpose of Countering Serious Crime (the "UK-US Agreement" or "the Agreement")[220], concluded in October 2019[221]. While the UK-US Agreement has not yet entered into force [at the time of adoption of this Decision], its foreseeable entry into force may affect onward transfers to the US of data first transferred to the UK on the basis of the Decision. More specifically, data transferred from the EU to service providers in the UK could be subject to orders for the production of electronic evidence issued by competent US law enforcement authorities and made applicable in the UK under this Agreement once in force. For these reasons, the assessment of the conditions and safeguards under which such orders can be issued and executed is relevant to this Decision.

(152) In this respect, it should be noted that, first, as regards its material scope, the Agreement is only applicable to crimes that are punishable with a maximum term of imprisonment of at least three years (defined as "serious crime")[222], including "terrorist activity". Second, data processed in the other jurisdiction may be obtained under this Agreement only following an "Order […] subject to review or oversight under the domestic law of the Issuing Party by a court, judge, magistrate, or other independent authority prior to or in proceedings regarding, enforcement of the Order"[223]. Third, any order must "be based on requirements for a reasonable justification based on articulable and credible facts, particularity, legality, and severity regarding the conduct under investigation"[224] and "be targeted at specific accounts as well as identify a specific person, account, address, or personal device, or any other specific identifier"[225]. Fourth, data obtained under this agreement benefits from equivalent protections to the specific safeguards provided by the so-called "EU-

---

subject to safeguards in terms of retention, destruction and disclosure of the data similar to the ones that are imposed in Section 53 and section 129 of the IPA 2016.

220 Agreement between the Government of the United Kingdom of Great Britain and Northern Ireland and the Government of the United States of America on Access to Electronic Data for the Purpose of Countering Serious Crime, available at the following link: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/836969/CS_USA_6.2019_Agreement_between_the_United_Kingdom_and_the_USA_on_Access_to_Electronic_Data_for_the_Purpose_of_Countering_Serious_Crime.pdf

221 This is he first agreement reached under the US Clarifying Lawful Overseas Use of Data (CLOUD) Act The United States CLOUD Act is a US federal law that was adopted on 23 March 2018 and that clarifies, through an amendment of the Stored Communications Act of 1986, that U.S. service providers are obliged to comply with U.S. orders to disclose content and non-content data, regardless of where such data is stored. The CLOUD Act also allows the conclusion of executive agreements with foreign governments, on the basis of which U.S. service providers would be able to deliver content data directly to these foreign governments (the text of the CLOUD Act is available at the following link: https://www.congress.gov/115/bills/s2383/BILLS-115s2383is.pdf)

222 Article 1 (14) of the Agreement.

223 Article 5(2) of the Agreement.

224 Article 5(1) of the Agreement.

225 Article 4(5) of the Agreement. An additional and stricter standard applies with respect to real-time interception: orders need to be for a limited duration, which shall not be longer than what is reasonably necessary to accomplish the purposes of the order, and shall only be issued if the same information could not be reasonably obtained by a less intrusive method (Article 5(3) of the Agreement).

US Umbrella Agreement"[226] – a comprehensive data protection agreement concluded in December 2016 by the EU and the US and that sets out the safeguards and rights applicable to data transfers in the area of law enforcement cooperation – which are all incorporated into this Agreement by reference on a *mutatis mutandis* basis to notably take into account the specific nature of the transfers (i.e. transfers from private operators to a law enforcement, rather than transfers between law enforcement authorities)[227]. The UK-US Agreement specifically provides that equivalent protections to those provided by the EU-US Umbrella Agreement will be applied "to all personal information produced in the execution of Orders subject to the Agreement to produce equivalent protections"[228].

(153) Data transferred to US authorities under the UK-US Agreement should therefore benefit from protections provided by an EU law instrument, with the necessary adaptations to reflect the nature of the transfers at issue. The UK authorities have further confirmed that the protections of the Umbrella Agreement will apply to all personal information produced or preserved under the Agreement, irrespective of the nature or type of body making the request (e.g. both federal and State law enforcement authorities in the US), so that equivalent protection must be provided in all cases. However, the UK authorities have also explained that the details of the concrete implementation of the data protection safeguards are still subject to discussions between the UK and the US. In the context of the talks with the European Commission's services on this decision, the UK authorities confirmed that they will only let the Agreement enter into force once they are satisfied that its implementation complies with the legal obligations provided therein, including clarity with respect to compliance with the data protection standards for any data requested under this Agreement. As a possible entry into force of the Agreement may impact the level of protection assessed in this Decision, any future clarification regarding the way the US will comply with its obligations under the Agreement should be communicated by the UK to the European Commission, as soon as it becomes available, to ensure proper monitoring of this decision in line with Article 45 (4) of Regulation (EU) 2016/679. Particular attention will be given to the application and adaptation of the Umbrella Agreement's protections to the specific type of transfers covered by the UK-US Agreement.

(154) More generally, any relevant development as regards the entry into force and application of the Agreement will be duly taken into account in the context of the continuous monitoring of this decision, including with respect to the necessary consequences to be drawn in case of any indication that an essentially equivalent level of protection is no longer ensured.

### *3.2.3 Oversight*

(155) Depending on the powers used by the competent authorities when processing personal data for a law enforcement purpose (whether under the DPA 2018 or the IPA 2016), different bodies ensure the oversight over the use of these powers. In particular, the Information Commissioner oversees the processing of personal data

---

226 Agreement between the United States of America and the European Union on the protection of personal information relating to the prevention, investigation, detection, and prosecution of criminal offences OJ L 336, 10.12.2016, p. 3–13, available at the following link: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:22016A1210(01)&from=EN

227 Article 9(1) of the Agreement.

228 Article 9(1) of the Agreement.

when it falls under the scope of Part 3 of the DPA 2018[229]. Independent and judicial oversight on the use of investigatory powers under the IPA 2016 is ensured by the Investigatory Powers Commissioner's Office (IPCO)[230] (this part is addressed in recitals (244) to (249)). Moreover, additional oversight is guaranteed by the Parliament a well as by other bodies.

3.2.3.1 Oversight over Part 3 of the DPA 2018

(156) The general functions of the Information Commissioner – whose independence and organisation are explained in recital (87) – 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 ICO's main task is to monitor and enforce Part 3 of the DPA 2018 as well as to promote public awareness, advise Parliament, the government and other institutions and bodies. To maintain the independence of the judiciary, the Information Commissioner is not authorised to exercise its 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. In these circumstances, other bodies would exercise the oversight functions, as explained in recitals (99) to (103).

(157) The Commissioner has general investigative, corrective, authorisation and advisory powers in relation to processing of personal data to which Part 3 applies. In particular, the Commissioner has the powers to notify the controller or the processor of an alleged infringement of Part 3 of the DPA 2018, to issue warnings or reprimand to a controller or processor that has infringed provisions of Part 3 of the Act, as well as to issue on its own initiative or on request, opinions to Parliament, government or other institutions and bodies as well as to the public on any issue related to the protection of personal data[231].

(158) Moreover, the Commissioner has powers to issue information notices[232], assessment notices[233] and enforcement notices[234] as well as the power to access documents of controllers and processors, access their premises[235] and issue administrative fines in the form of penalty notices[236]. The ICO's Regulatory Action Policy sets out the circumstances under which it issues respectively information, assessment, enforcement and penalty notices[237] (see also recital (93) and Directive (EU) 2016/680 adequacy decision recitals 101-102).

(159) According to its latest annual reports (2018–2019[238], 2019-2020[239]), the Information Commissioner has conducted a number of investigations and taken enforcement measures with respect to processing of data by law enforcement authorities. For

229 Section 116 of the DPA 2018.
230 See IPA 2016 and in particular Chapter 1 Part 8.
231 Paragraph 2 of the Schedule 13 to the DPA 2018.
232 Ordering the controller and the processor (and in certain circumstances any other person) to provide necessary information (Section 142 of the DPA 2018).
233 Allowing the carrying out investigations and audit, 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 (Section 146 of the DPA 2018).
234 Permitting the exercise of corrective powers, which requires controllers/processors to take or refrain from taking specified steps (Section 149 of the DPA 2018).
235 Section 154 of the DPA 2018.
236 Section 155 of the DPA 2018.
237 Regulatory Action Policy, see footnote 102.
238 Information Commissioner's Annual Report and Financial Statements 2018-19, see footnote 101.
239 Information Commissioner's Annual Report and Financial Statements 2019-20, see footnote 82.

example, the Commissioner conducted an investigation and published an Opinion in October 2019 concerning law enforcement's use of facial recognition technology in public places. The investigation focused, in particular, on the use of live facial recognition capabilities by South Wales Police and the Metropolitan Police Service (MPS). The Information Commissioner also investigated the MPS "Gangs matrix"[240] and found a range of serious infringements of data protection law that were likely to undermine public confidence in the matrix and how the data was being used. 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. Another example of a enforcement action in this area is the £325,000 fine issued by the Commissioner in May 2018 against the Crown Prosecution Service, for losing unencrypted DVDs containing recordings of police interviews. The Information Commissioner also 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. Moreover, the Commissioner is currently investigating a case that involves the access of law enforcement authorities to data held by a private sector entity, Clearview AI Inc.[241]

(160) Besides the enforcement powers of the Information Commissioner mentioned in recitals (158 and (159), certain violations of the data protection legislation constitute offences and may therefore be subject to criminal sanctions (section 196 of the DPA 2018). This applies, for example, to obtaining, disclosing or retaining personal data without the consent of the controller and procuring the disclosure of personal data to another person without the consent of the controller[242]'; re-identifying information that is de-identified personal data without the consent of the controller responsible for de-identifying the personal data[243]; intentionally obstructing the Commissioner to exercise its powers in relation to inspection of personal data in accordance with international obligations[244], making false statements in response to an information notice, or destroying information in connection to information and assessment notices[245].

3.2.3.3 Other oversight bodies in the area of criminal law enforcement

(161) In addition to the Information Commissioner, there are several oversight bodies in the area of criminal law enforcement with specific mandates relevant for data protection issues. This includes for instance the Commissioner for the Retention and

240 A database which recorded intelligence related to alleged gang members and victims of gang related crimes.

241 See ICO statement, available at the following link: https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/07/oaic-and-ico-open-joint-investigation-into-clearview-ai-inc/

242 Section 170 of the DPA 2018.

243 Section 171 of the DPA 2018.

244 Section 119(6) of the DPA 2018

245 During the financial year covering the period from 1 April 2019 to 31 March 2020, the ICO's investigations have resulted in four cautions and eight prosecutions. These cases were prosecuted under Section 55 of the Data Protection Act 1998, Section 77 of the Freedom of Information Act 2000 and Section 170 of the Data Protection Act 2018. In 75% of cases, the defendants submitted guilty pleas negating the necessity for protracted trials with the associated costs. (Information Commissioner's Annual Report and Financial Statements 2019/2020, see footnote 87, page 40).

Use of Biometric Material ('the Biometrics Commissioner')[246] and the Surveillance Camera Commissioner[247].

3.2.3.4 Parliamentary oversight in the area of criminal law enforcement

(162) The Home Affairs Select Committee (HASC) ensures parliamentary oversight in the area of law enforcement. This Committee consists of 11 Members of Parliament, drawn from the three largest political parties. The Committee has the task to examine the expenditure, administration, and policy of the Home Office and associated public bodies, i.e. including the police and the NCA – whose work the Committee can scrutinise specifically[248].

(163) The Committee can, within the limits of their remit, choose its own subject of inquiry, including specific cases, as long as the issue is not *sub judice*. The Committee may also seek written and oral evidence from a wide range of relevant groups and individuals. It produces reports on its findings and issues recommendations to the Government[249]. The Government is expected to respond to each of the report's recommendations and must respond within 60 days[250].

(164) In the area of surveillance, the Committee also produced a report concerning the Regulation of Investigatory Powers Act 2000 (RIPA 2000)[251], which found that the RIPA 2000 was not fit for purpose. Their report was taken into account during the replacement of significant parts of the RIPA 2000 with the IPA 2016. A full list of inquiries can be found on the Committee's website[252].



246 The Biometrics Commissioner was established by the Protection of Freedoms Act 2012 (see: https://www.legislation.gov.uk/ukpga/2012/9/contents) and focuses on the retention and use of biometrics data (DNA samples and profiles and fingerprints) by police. This includes reviewing decisions by the police to retain DNA data, reviewing national security determinations in connection with the retention of DNA profiles and fingerprints and reporting to the Home Secretary about the carrying out of their functions.

247 The Surveillance Camera Commissioner was established by the Protection of Freedoms Act 2012 and has the role of encouraging compliance with the Surveillance Camera Code of Practice; reviewing the operation of this Code ; and providing advice to ministers on whether this Code needs amending.

248 See https://committees.parliament.uk/committee/83/home-affairs-committee/news/100537/work-of-the-national-crime-agency-scrutinised/

249 Select Committees, including the Home Affairs Select Committee, are subject to the Standing Orders of the House of Commons. Standing Orders are the rules, agreed by the House of Commons, governing the way parliament does business. The remit of select committees is broad, with Standing Order 152(1) providing that the "Select committees shall be appointed to examine the expenditure, administration and policy of the principal government departments as set out in paragraph (2) of this order and associated public bodies." This enables the Home Affairs Select Committee to look at any policy owned by the Home Office, which includes policies (and the related legislation) on investigatory powers. Moreover, standing Order 152(4) makes clear that Committees have various powers, including the ability to request persons to give evidence or documents on a particular issue, and to produce reports. The Committee's current and previous enquiries are available at the following link https://committees.parliament.uk/committee/83/home-affairs-committee/.

250 The powers of the Home Affairs Select Committee in England and Wales are set out in the Standing Orders of the House of Commons, available at the following link: https://www.parliament.uk/business/publications/commons/standing-orders-public11/.

251 Available at the following link: https://publications.parliament.uk/pa/cm201415/cmselect/cmhaff/711/71103.htm

252 https://committees.parliament.uk/committee/83/home-affairs-committee

(165) The tasks of the HASC are performed in Scotland by the Justice Subcommittee on Policing and in Northern Ireland by the Committee for Justice[253].

*3.2.4 Redress*

(166) As regards processing of data by law enforcement authorities, redress mechanisms are available under Part 3 of the DPA 2018 and under the IPA 2016, as well as under the Human Rights Act 1998.

(167) This series of mechanisms provide data subjects with effective administrative and judicial means of redress, enabling them in particular to ensure their rights, including the right to have access to their personal data, or to obtain the rectification or erasure of such data.

First, under Section 165 the DPA 2018, 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[254]. The Information Commissioner has the power to assess the compliance of the controller and processor with the DPA 2018, require them to take necessary steps in case of non-compliance and impose fines.

(168) Second, the DPA 2018 provides the right to a remedy against the Information Commissioner if it fails to appropriately handle a complaint made by the data subject. More specifically, if the Commissioner fails to "progress"[255] a complaint made by the data subject, the complainant has access to judicial remedy, as they can apply to a First Tier Tribunal[256] to order the Commissioner to take appropriate steps to respond to the complaint, or to inform the complainant of progress on the complaint[257]. In addition, any person who is given any of the mentioned notices

253 The rules of the Justice Subcommittee on Policing in Scotland are provided at the following link https://www.parliament.scot/parliamentarybusiness/CurrentCommittees/justice-committee.aspx and the rules of Committee of Justice in Northern Ireland are set out at the following link: http://www.niassembly.gov.uk/assembly-business/standing-orders/ ]

254 The last ICO annual report provides a breakdown of the nature of complaints received and closed. In particular, the number of complaints received for "policing and criminal records" amount to 6% of the total number of complaints received (with an increase of 1% compared to the previous financial year). The annual report also shows that complaints concerning subjects' access requests represent the highest number (46% over total number of complaints, with an increase of 8% compared to the previous financial year) (ICO' s Annual report 2019-2020, page 55; see footnote 88).

255 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.

256 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.

257 Section 166 of the DPA 2018. Example of successful actions against the ICO before the Tribunal include a case where the ICO acknowledged receipt of a complaint from a data subject but did not indicate what course of action it intended to take, and was therefore ordered to confirm, within 21 calendar days, whether it was going to investigate the complaints and, if so, to inform the complainant of the progress of the investigation no less frequently than every 21 calendar days thereafter (the judgment has not yet been published), and a case where the First Tier Tribunal considered that it was unclear whether the ICO's response to a complainant properly constituted the 'outcome' of the complaint (see *Susan Milne v The Information Commissioner* [2020], judgement available at the following link:

(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[258].

(169) Third, individuals can obtain judicial redress against controllers and processors directly before the courts. In particular, under Section 167 of the DPA 2018, a data subject may submit an application before the court for an infringement of his/her right under the data protection legislation and the court may by means of an order request the controller to take (or to refrain from taking) any step with respect to the processing to comply with the DPA 2018. Moreover, under Section 169 of the DPA 2018, any person who has suffered damage due to 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.

(170) Finally, any person, as far as he/she considers that his/her rights, including rights to privacy and data protection, have been violated by any public authorities, can obtain redress before the courts of the United Kingdom under the Human Rights Act 1998[259], and, after exhausting national remedies, a person, non-governmental organisation and groups of individuals can obtain redress before the European Court of Human Rights for violations of the rights guaranteed under the European Convention of Human Rights[260] (see in recital (111)).

3.2.4.1 Redress mechanisms available under the IPA 2016

(171) Individuals can obtain redress for violations of the IPA 2016 before the Investigatory Powers Tribunal. The redress avenues available under the IPA 2016 are described in recitals (257)-(263) below.



https://informationrights.decisions.tribunals.gov.uk/DBFiles/Decision/i2730/Milne,%20S%20-%20QJ2020-0296-GDPR-V,%20051220%20Section%20166%20DPA%20-DECISION.pdf)

258 Sections 162 and 163 of the DPA 2018.

259 See for example *Brown v Commissioner of Police of the Metropolis & Anor* [2019] EWCA Civ 1724 where damages of £9,000 were awarded under the DPA 1998 and the Human Rights Act 1998 for unlawful obtaining and misuse of personal information, and *R (on the application of Bridges) v Chief Constable of South Wales* [2020] EWCA Civ 1058 where the Court of Appeal declared unlawful the deployment of a facial recognition system by the Wales police, as it was in breach of Article 8 of the ECHR and the data protection impact assessment produced by the controller did not comply with the DPA 2018.

260 Article 34 of the European Convention of Human Rights provides that "The Court may receive applications from any person, non-governmental organisation or group of individuals claiming to be the victim of a violation by one of the High Contracting Parties of the rights set forth in the Convention or the Protocols thereto. The High Contracting Parties undertake not to hinder in any way the effective exercise of this right".

### 3.3 Access and use by United Kingdom public authorities for national security purposes

(172) In the United Kingdom legal order, the intelligence services empowered to collect electronic information held by controllers or processors on national security grounds, in situations that are relevant to an adequacy scenario, are the Security Service[261] (MI5), the Secret Intelligence Service[262] (SIS) and the Government Communications Headquarters[263] (GCHQ)[264].

*3.3.1 Legal bases, limitations and safeguards*

(173) In the UK, the powers of the intelligence agencies are set out in the IPA 2016 and the RIPA 2000, which, together with the DPA 2018, provide limitations and safeguards for the exercise of these powers. Those powers as well as the limitations and safeguards applicable to them are assessed in detail in the following sections.

3.3.1.1 Investigatory powers exercised in the context of national security

(174) The IPA 2016 provides the legal framework for the use of investigatory powers, i.e. the power to intercept, access communication data and perform equipment interference. The IPA 2016 introduces a general prohibition and makes it a criminal offence to use techniques that allow access to the content of communications, access to communication data or equipment interference without lawful authority[265]. This is

261 The MI5 is under the authority of the Home Secretary. The Security Services Act 1989 sets out MI5's functions: protecting national security (including protection against threats from espionage, terrorism and sabotage, from activities of agents of foreign powers and from actions intended to overthrow or undermine parliamentary democracy by political, industrial or violent means), safeguarding the economic well-being of the UK against outside threats and supporting activities of the police forces and other law enforcement agencies in the prevention and detection of serious crime.

262 The SIS is under authority of the Foreign Secretary and its functions are set out in the Intelligence Services Act 1994. Its functions are to obtain and provide information relating to the actions or intentions of persons outside the British Islands and to perform other tasks relating to the actions or intentions of such persons. These functions can be exercised only in the interest of national security, in the interests of the economic well-being of the UK or in support of the prevention or detection of serious crime.

263 The GCHQ is under authority of the Foreign Secretary and its functions are set out in the Intelligence Services Act 1994. These are (a) to monitor, make use of or interfere with electromagnetic and other emissions and equipment producing such emissions, obtain and provide information derived from or related to such emissions or equipment and from encrypted material; (b) to provide advice and assistance about languages, including terminology used for technical matters and cryptography and other matters relating to the protection of information to the armed forces, to the government or other organisations or persons considered appropriate. These functions can be exercised only in the interest of national security, in the interests of the economic well-being of the UK in the relation to the actions or intentions of persons outside the British Islands or in support of the prevention or detection of serious crime.

264 Other public bodies exercising functions relevant to national security are the Defence Intelligence (DI), the National Security Council and Secretariat, the Joint Intelligence Organisation and the Joint Intelligence Committee. However, neither the JIC nor the JIO are able to make use of investigatory powers under the IPA 2016 while the DI has limited scope to use its powers.

265 The prohibition applies to both public and private communication networks, as well as the public postal service when the interception is carried out in the United Kingdom. The prohibition does not apply to the controller of the private network if the controller has given express or implied consent to carry out the interception (Section 3 of the IPA 2016).

reflected in the fact that the use of these investigatory powers is lawful only when carried out on the basis of a warrant or an authorization[266].

(175) The limitations and safeguards applicable to each of the powers are specified in the IPA 2016. Different rules apply depending on the type of investigatory power (interception of communications, acquisition and retention of communication data and equipment interference), as well as on whether the power is exercised on a specific target[267] or in bulk[268].

(176) The IPA 2016 is supplemented with a number of statutory Codes of Practice, issued by the Secretary of State, approved by both Houses of the Parliament[269] and applicable throughout the country, providing guidance on the use of these powers[270]. The effects of the Codes of Practice are detailed in Schedule 7 paragraph 5 to the IPA 2016, which specifies that they are admissible as evidence in civil and criminal proceedings, and the court, tribunal or supervisory authority may take into account any non-compliance with the Codes when determining a relevant issue in judicial proceedings[271]. In this respect the European Court of Human Rights has recognised the relevance of the UK Codes of Practice on the IPA 2016's investigatory powers, in the context of the assessment of the "quality of the law" of the legislation permitting the surveillance[272].

---

266 In specific limited cases lawful interception without a warrant is possible, i.e. when intercepting with the consent of the sender or recipient (Section 44 of the IPA 2016), in case of limited administrative or enforcement purposes (Section 45 to 48 of the IPA), in certain special institutions (Sections 49-51 of the IPA 2016) and in accordance with overseas requests (Section 52 of the IPA 2016).

267 Sections 15 and following of the IPA 2016 govern targeted interception of communication, Section 60A and following of the IPA 2016 for acquisition and retention of communication data and Section 99 of the IPA 2016 for equipment interference.

268 Sections 136 and following of the IPA 2016 govern bulk interception, Sections 158 and following of the IPA 2016 for bulk acquisition of communication data, Sections 176 and following of the IPA 2016 for bulk equipment interference and Sections 199 and following of the IPA 2016 for bulk personal dataset.

269 Schedule 7 to the IPA 2016 determines the scope of the Codes, the procedure to be followed when issuing them, the rules for the revision of them and the effect of the codes.

270 The codes of practice under the IPA 2016 are available at the following link: https://www.gov.uk/government/publications/investigatory-powers-act-2016-codes-of-practice

271 The Courts and Tribunals use the Codes of practice to assess the lawfulness of the conduct of the authorities. See for example: *Dias v Cleveland Police*, [2017] UKIPTrib15_586-CH , where the Investigatory Powers Tribunal made reference to specific passages of the Code of Practice on Communication Data to understand the definition of the ground of "preventing or detecting crime or of preventing disorder" used to apply for the acquisition of communication data. The Code was included in the reasoning to find whether that ground was used incorrectly. The Court went on to conclude that the conducts contested were unlawful. Courts have also made evaluation on the level of safeguards available in the Codes, see for example *Just for Law Kids v Secretary of State for the Home Department* [2019] EWHC 1772 (Admin) where the High Court found that primary and secondary legislation together with the internal guidance provided sufficient safeguards; or *R (National Council for Civil Liberties) v Secretary of State for the Home Department & Others* [2019] EWHC 2057 (Admin), where it found that both the IPA 2016 and Code of Practice on Equipment Interference contained sufficient provisions as to the need for specificity of warrants.

272 In the *Big Brother Watch* case, paragraph 325 (see footnote **Error! Bookmark not defined.**) the European Court of Human Rights recognised that "As the IC Code is a public document, subject to the approval of both Houses of Parliament, and has to be taken into account both by those exercising interception duties and by courts and tribunals, the Court has expressly accepted that its provisions could be taken into consideration in assessing the foreseeability of the RIPA 2000 regime (see Kennedy, cited above, § 157)".

(177) It should also be noted that targeted powers (targeted interception[273], acquisition of communication data[274], retention of communication data[275] and targeted equipment interference[276]) are available to national security agencies and certain law enforcement authorities[277] while only intelligence services may make use of bulk powers (i.e. bulk interception[278], bulk acquisition of communications data[279], bulk equipment interference[280] and bulk personal datasets[281]).

(178) In deciding which investigation power should be used, the intelligence agency has to comply with the "general duties in relation to privacy" listed in Section 2(2)(a) of the IPA 2016, which include a necessity and proportionality test. More specifically, pursuant to this provision, a public authority having the intention to use an investigatory power must consider (i) whether what is sought to be achieved by the warrant, authorisation or notice could reasonably be achieved by other less intrusive means; (ii) whether the level of protection to be applied in relation to any obtaining of information by virtue of the warrant, authorisation or notice is higher because of the particular sensitivity of that information; (iii) the public interest in the integrity and security of telecommunication systems and postal services, and (iv) any other aspects of the public interest in the protection of privacy[282].

(179) The way these criteria should be applied – and the way their compliance is assessed as part of the authorisation of the use of such powers by the Secretary of State and the independent Judicial Commissioners – is further specified in the relevant Codes of Practice. In particular, the use of any one of these investigative powers must always be "proportionate to what is sought to be achieved [which] involves balancing the seriousness of the intrusion into the privacy (and other considerations set out in section 2(2)) against the need for the activity in investigative, operational or capability terms". This means notably that it "should offer a realistic prospect of bringing the expected benefit and should not be disproportionate or arbitrary" and "[n]o interference with privacy should be considered proportionate if the information which is sought could reasonably be obtained by other less intrusive means" [283].

---

273 Part 2 of the IPA 2016.

274 Part 3 of the IPA 2016.

275 Part 4 of the IPA 2016.

276 Part 5 of the IPA 2016.

277 For the list of relevant law enforcement authorities that can apply targeted investigative powers under the IPA 2016, see above footnote (137).

278 Section 136 of the IPA 2016.

279 Section 158 of the IPA 2016.

280 Section 176 of the IPA 2016.

281 Section 199 of the IPA 2016.

282 The Code of Practice on Interception of Communications specifies that other elements of the proportionality test are: "(i) the extent of the proposed interference with privacy against what is sought to be achieved; (ii) how and why the methods to be adopted will cause the least possible interference to the person and others; (iii) whether the activity is an appropriate use of the Act and a reasonable way, having considered all reasonable alternatives, of achieving what is sought to be achieved; (iv) what other methods, as appropriate, were either not implemented or have been employed but which are assessed as insufficient to fulfil operational objectives without the use of the proposed investigatory power". Code of Practice on Interception of Communications paragraph 4.16, available at the following link: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715480/Interception_of_Communications_Code_of_Practice.pdf

283 See Code of Practice on Interception of Communications, paragraphs 4.12 and 4.15, available at the following link:

More specifically, compliance with the principle of proportionality must be assessed having regard to the following criteria: "(i) the extent of the proposed interference with privacy against what is sought to be achieved; (ii) how and why the methods to be adopted will cause the least possible interference to the person and others; (iii) whether the activity is an appropriate use of the Act and a reasonable way, having considered all reasonable alternatives, of achieving what is sought to be achieved; (iv) what other methods, as appropriate, were either not implemented or have been employed but which are assessed as insufficient to fulfil operational objectives without the use of the proposed investigatory power"[284].

(180) In practice, as explained by the UK authorities, this ensures that an intelligence agency, first, sets the operational objective (thus delimitating the collection, e.g. an international counterterrorism purpose in a specific geographic area) and, second, on the basis of that operational objective, will have to consider which technical option (e.g. targeted or bulk interception, equipment interference, acquisition of communication data) is the most proportionate (i.e. the least intrusive to privacy cf. Section 2(2) of the IPA) to what is sought to be achieved and therefore can be authorised under one of the available statutory bases.

(181) It is worth noting that this reliance on standards of necessity and proportionality has also been noted and welcomed by the UN Special Rapporteur on the Right to Privacy, Joseph Cannataci, who stated, regarding the system established by the IPA 2016, that "[t]he procedures in place both within the intelligence services as within the law enforcement agencies appear to systematically require consideration of the necessity and proportionality of a surveillance measure or operation before it is recommended for authorization as well as its review on the same grounds"[285]. He also observed that in his meeting with representatives of law enforcement and national security agencies "[he] received a consensus view that the right to privacy needs to be a primary consideration for any decision regarding surveillance measures. All of them understood and appreciated necessity and proportionality as the cardinal principles to be taken into account".

(182) The specific criteria for issuing the different warrants, as well as the limitations and safeguards established by the IPA 2016 regarding each investigatory power are detailed in recitals (186) to (237).

3.3.1.1.1 Targeted interception and examination

(183) There are two types of warrant that allow the targeted interception and examination of communications that are relevant to the activities of national security bodies: the targeted interception warrant[286] and the targeted examination warrant. The conditions to obtain them and the relevant safeguards are set out in Chapter 1 of Part 2 of the IPA 2016.



---

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715480/Interception_of_Communications_Code_of_Practice.pdf

284 See Code of Practice on Interception of Communications, paragraph 4.16.

285 End of Mission Statement of the Special Rapporteur on the Right to Privacy at the Conclusion Of his Mission to the United Kingdom of Great Britain and Northern Ireland, available at the following link: https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=23296&LangID=E, para 1.a..

286 Section 15(2) of the IPA 2016.

(184) A targeted interception warrant authorizes the interception of the communications described in the warrant in the course of their transmission and obtaining other data relevant for those communications[287], including secondary data[288]. A targeted examination warrant authorises a person to carry out the selection for examination of intercepted content obtained under a bulk interception warrant[289].

(185) Any warrant pursuant to Part 2 of the IPA 2016 may be issued by the Secretary of State[290] and approved by a Judicial Commissioner[291]**.** In all cases the duration of any type of targeted warrant is limited to 6 months[292] and specific rules apply concerning its modification[293] and renewal[294].

(186) Before issuing the warrant, the Secretary of State must carry out a necessity and proportionality assessment[295]. Specifically, for a targeted interception warrant and a targeted examination warrant, the Secretary of State should verify whether the measure is necessary for one of the following grounds: the interest of national security; the prevention or detection of a serious crime; or the interests of the economic well-being of the United Kingdom[296] in so far as those interests are also relevant to the interests of national security[297]. On the other hand, a mutual assistance warrant (see recital (137) above(137)) can be issued only if the Secretary of State considers that circumstances exist equivalent to those in which he/she would issue a warrant for the purpose of preventing and or detecting serious crime[298].

(187) Moreover, the Secretary of State should assess whether the measure is proportionate to what is sought to be achieved[299]. The assessment on the proportionality of the

287 Section 15(2) of the IPA 2016.

288 Secondary data are data attached or logically associated with the intercepted communication, can be logically separated from it and if it were so separated, would not reveal anything of what might reasonably be considered to be the meaning (if any) of the communication. Some examples of secondary data include router configurations or firewalls or the period of time a router has been active on a network when they are part of, attached to or logically associated with intercepted communication. For more details see the definition in Section 16 of the IPA 2016 and Code of Practice on Interception of Communications, paragraph 2.19, see footnote 282.

289 This examination is carried out as an exception of section 152(4) of the IPA 2016 which provides for the prohibition of seeking to identify communication of individuals which are in the British Islands. See recital (223).

290 The Scottish Minister authorises the warrant when it relates to serious criminal activity in Scotland (see Section 21 and Section 22 of the IPA 2016) while a senior officer can be designated by the Secretary of State to issue a mutual assistance warrant when it appears that the interception will concern a person or premises located outside the United Kingdom (Section 40 of the IPA 2016).

291 Sections 19 and 23 of the IPA 2016.

292 Section 32 of the IPA 2016.

293 Section 39 of the IPA 2016. Limited modifications can be made to the warrants by prescribed persons under the conditions set out in the IPA 2016. The person who issued the warrant can cancel a warrant at any time. They must do so if the warrant is no longer necessary on any relevant grounds or the conduct authorised by the warrant is no longer proportionate to what is sought to be achieved.

294 Section 33 of the IPA 2016. The decision to renew the warrant must be approved by a Judicial Commissioner.

295 Section 19 of the IPA 2016.

296 On the notion of "interests of the economic well-being", when those interests are also relevant for national security, see the European Court of Human Rights *Big Brother Watch* case, where the Court considered such notion to be "sufficiently clear", also in light of the clarifications provided by the Code of Practice on Interception of Communications (See *Big Brother Watch*, paras 334-335).

297 Section 20(2) of the IPA 2016.

298 Section 20(3) of the IPA 2016.

299 Sections 19(1)(b), 19(2)(b) and 19(3)(b) of the IPA 2016.

measures requested must take into account the general duties in relation to privacy set out in Section 2(2) of the IPA 2016, notably the need to assess whether what is sought to be achieved by the warrant, authorisation or notice could reasonably be achieved by other less intrusive means and whether the level of protection to be applied in relation to any obtaining of information by virtue of the warrant, is higher because of the particular sensitivity of that information (see recital (178) above).

(188) To this end, the Secretary of State will have to take into account all the elements of the application provided by the authority submitting the request, in particular those related to the persons to be intercepted and the relevance of the measure for the investigation. Such elements are spelled out in the Code of Practice on Interception of Communications and must be described at a certain level of specificity[300]. Moreover, Section 17 of the IPA 2016 requires that any warrant issued under its Chapter 2 must name or describe the specific person or a group of persons, organization or premises to be intercepted (the "target"). In case of a targeted interception warrant or a targeted examination warrant, these may also relate to a group of persons, more than one person or organisation, or more than one set of premises (also so called "thematic warrant")[301]. In these cases, the warrant should describe the common purpose or activity shared by the group of persons or the operation/investigations and name or describe as many of those persons/organisations or set of premises where it is reasonably practicable[302]. Finally, all the warrants issued under Part 2 of the IPA 2016 must specify the addresses, numbers, apparatus, factors, or combination of factors that are to be used for identifying the communications[303]. In this respect, the Code of Practice on Interception of Communications specifies that, in case of a targeted interception warrant and targeted examination warrant "the warrant must specify (or describe) the factors or combination of factors that are to be used for identifying the communications. Where the communications are to be identified by reference to a telephone number (for example) the number must be specified by being rendered in its entirety. But where very complex or continually-changing internet selectors are to be used for identifying the communications, those selectors should be described as far as possible"[304].

(189) An important safeguard in this context is that he assessment carried out by the Secretary of State to issue a warrant must be approved by an independent Judicial Commissioner[305] that will notably check whether the decision to issue the warrant

300 The information requested includes the details about the background (description of the persons/organisations/set of premises, the communication to be intercepted) and how obtaining those information will benefit the investigation as well as a description of the conduct to be authorised. In case is not possible to describe the persons/organisation/premises an explanation must be included on why it was not possible or on why only a general description was done (Code of Practice on Interception of Communications, paragraphs 5.32 and 5.34, see footnote 282).

301 Section 17(2) of the IPA 2016. See also Code of Practice of Interception of Communications, paragraphs 5.11 and following, see footnote 282.

302 Section 31(4) and (5) of the IPA 2016.

303 Section 31(8) of the IPA 2016.

304 Code of Practice on Interception of Communications, paragraphs 5.37 and 5.38, see footnote 282.

305 The approval by a Judicial Commissioner is not required when the Secretary of State considers that there is an urgent need to issue the warrant (Section 19(1) of the IPA). However, the Judicial Commissioner needs to be informed in a short period of time and must decide whether to approve or not the warrant. If it does not, the warrant ceases to have effect (Sections 24 and 25 of the IPA 2016).

complies with the necessity and proportionality principles[306] (on the status and role of Judicial Commissioners see recitals (245) to (250) below). The IPA 2016 also clarifies that, when carrying out such check, the Judicial Commissioner must apply the same principles as would be applied by a court on an application for judicial review[307]. This ensure that in each case, and before access to data takes place, compliance with the principle of necessity and proportionality is systematically check by an independent body.

(190) The IPA 2016 provides for additional limitations and safeguards relating to the specific status of the person(s) intercepted[308]. In particular the Prime Minister needs to be involved when the communications of Members of Parliament are intercepted[309]. The interception of items subject to legal privilege is authorised only in presence of exceptional and compelling circumstances, the person issuing the warrant must give regard to the public interest in the confidentiality of items subject to legal privilege and that specific requirements are in place for the handling, retention and disclosure of such material[310]. Confidential journalistic material and information on journalistic sources can be intercepted if specific arrangements are in place for the handling, retention and disclosure of this material[311].

(191) Furthermore, the IPA 2016 provides for specific safeguards related to security, retention and disclosure that the Secretary of State should take into account before issuing a targeted warrant[312]. In particular, Section 53(5) of the IPA 2016 requires that every copy made of any of that material collected under the warrant must be stored in a secure manner and is destroyed as soon as there are no longer any relevant grounds for retaining it, while Section 53(2) of the IPA 2016 requires that the number of persons to whom the material is disclosed and the extent to which any material is disclosed, made available or copied must be limited to the minimum that is necessary for the statutory purposes.

(192) Finally, when the material that has been intercepted either by a targeted interception warrant or by a mutual assistance warrant is to be handed over to a third country ("overseas disclosures"), the IPA 2016 provides that the Secretary of State must ensure that appropriate arrangements are in place to ensure that similar safeguards on security, retention and disclosure exist in that third country[313].

3.3.1.1.2 Targeted acquisition and retention of communications data

306 Section 23(1) of the IPA 2016.

307 Section 23 (2) of the IPA 2016.

308 Sections 26-29 of the IPA 2016 introduce limitations to obtain targeted interception and examination warrants in relation to the interception of communications sent by, or intended for, a person who is a Member of Parliament (any Parliament of the United Kingdom), the interception of items subject to legal privilege, the interception of communications which the intercepting authority believes will be communications containing confidential journalistic material, and when the purpose of the warrant is to identify or confirm a source of journalistic information.

309 Section 26 of the IPA 2016.

310 Section 26 of the IPA 2016.

311 Section 28-29 of the IPA 2016 specify that when journalistic material or information on journalistic sources are to be intercepted the issuing authorities must make sure that the warrant includes specific arrangements for the handling, retention, use and destruction of communications containing confidential journalistic material or communication that identify sources of journalistic information and that, under section 53(7) of the IPA 2016, the Investigatory Power Commissioner is informed of them as soon as reasonably possible.

312 Section 19(1) of the IPA 2016.

313 Section 54 of the IPA 2016.

(193) The IPA 2016 permits the Secretary of State to require telecommunications operators to retain communications data for the purpose of targeted access by a range of public authorities, including law enforcement and intelligence agencies. Part 4 of the IPA 2016 provides for the retention of communications data, while Part 3 provides for targeted acquisition of communications data (TCD). Part 3 and Part 4 of the IPA 2016 also set out specific limitations on the use of these powers and provide for specific safeguards.

(194) The term "communications data" covers the "who", "when", "where" and "how" of a communication, but not the content, i.e. what was said or written. Different from interception, the acquisition and retention of communications data is not aimed at obtaining the content of the communication, but aimed at obtaining information such as the subscriber to a telephone service or an itemised bill. This could include the time and duration of communication, the number or email address of the originator and recipient and sometimes the location of the devices from which the telecommunication was made[314].

(195) The regime for the retention and acquisition of communication data has been amended and strengthened by the IPA 2016 following notably the *Tele2/Watson* judgment of the European Court of Justice[315]. In particular, as explained in recitals (200) to (206), this new regime has introduced additional conditions and safeguards that apply when communication data is retained for law enforcement or national security purposes, ensuring that such retention is not general and indiscriminate. This includes an *ex ante* authorisation by an independent Judicial Commissioner aimed notably at accessing the necessity and proportionality of the proposed measure.

(196) It should be noted that the retention and acquisition of communications data normally does not concern personal data of EU data subjects transferred under this Decision to the UK. The obligation to retain or disclose communications data pursuant to Part 3 and 4 of the IPA 2016 covers data that is collected by telecommunication operators in the UK directly from the users of a telecommunication service[316]. This type of "customer facing" processing typically

---

314 Communications data is defined in Section 261(5) to the IPA 2016. Communications data is divided into "events data" (any data which identifies or describes an event, whether or not by reference to its location, in or by means of a telecommunication system where the event consists of one or more entities engaging in a specific activity at a specific time) and "entity data" (any data which (a) is about (i) an entity, (ii) an association between a telecommunications service and an entity, or (iii) an association between any part of a telecommunication system and an entity, (b) consists of, or includes, data which identifies or describes the entity (whether or not by reference to the entity's location), and (c) is not events data).

315 Joined Cases C-203/15 and C-698/15, Tele2/Watson, ECLI:EU:C:2016:970).

316 This follows from the definition of communications data provided in Section 261(5) of the IPA 2016, according to which communications data is held or obtained by a telecommunications operator and is either about the user of a telecommunications service and relating to the provision of this service, or is comprised in, included as part of, attached to or logically associated with a communication (see also Code of Practice on Communications Data, available at the following link https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/757850/Communications_Data_Code_of_Practice.pdf, paragraphs 2.22 to 2.33). Moreover, the definition of telecommunications operator provided in Section 261(10) of the IPA 2016 requires that a telecommunications operator is a person who offers or provides a telecommunications service to persons in the UK or who controls or provides a telecommunication system which is (wholly or partly) in or controlled from the UK. These definitions make clear that obligations under the IPA 2016 cannot be imposed on telecommunications operators whose equipment is not in or controlled from the UK and who do not offer or provide services to persons in the UK (see also Code of Practice on

does not involve a transfer on the basis of this Decision, i.e. a transfer from a controller/processor in the EU to a controller/processor in the UK.

(197) However, for the sake of completeness, the conditions and safeguards governing these acquisition and retention regimes are described below.

*(i) Authorisation for obtaining communications data*

(198) According to Part 3 of the IPA 2016, relevant public authorities[317] are authorised to obtain communications data from a telecommunication operator or any person capable of obtaining and disclosing such data. The authorisation may not allow the interception of the content of the communications[318] and ceases to have effect after a period of one month[319] with the possibility to be renewed subject to an additional authorisation[320]. The acquisition of communications data requires an authorisation by the independent Investigatory Powers Commissioner (IPC)[321] (on the status and powers of the IPC see recitals (244) to (245) below) in all cases where the acquisition of communication data is requested by a relevant law enforcement authority[322]. However, Section 61 of the IPA 2016 provides that when data is acquired in case of urgency[323], for the interests of national security or economic well-being of the UK as long as it is relevant for national security, or where an application is made by a member of an intelligence agency under Section 61(7)(b)[324], the acquisition may be alternatively[325] authorised by the IPC or by a designated senior officer[326]. The

---

Communications Data, paragraph 2.1). If EU subscribers (whether located in the EU or in the UK) made use of services in the UK, any communications in relation to the provision of this service would be collected directly by the service provider in the UK rather than subject to a transfer from the EU.

317 The relevant authorities are listed in the Schedule 4 to the IPA 2016 and they include the police forces, intelligence services, some ministries and government departments, National Crime Agency, Her Majesty's Revenue and Customs, Competition and Markets Authority, Information Commissioner, ambulance, fire and rescue services and authorities for example in the area of health and food safety.

318 Section 60A(6) of the IPA 2016.

319 This period is reduced to three days when the authorization is given for reasons of urgency (Section 65(3)A of the IPA 2016).

320 According to Section 65 of the IPA 2016, the renewed authorisation will last for a period of one month from the date the current authorisation expires. The person who has granted the authorisation can cancel the authorisation at any time if it considers that the requirements are not anymore satisfied.

321 Section 60A (1) of the IPA 2016.

322 See footnote 317.

323 Section 61A of the IPA 2016.

324 The application under Section 61(7)(b) of the IPA 2016 is made for "an applicable crime purpose" meaning, according to Section 61(7)A of the IPA 2016: "where the communications data is wholly or partly events data, the purpose of preventing or detecting serious crime; in any other case, the purpose of preventing or detecting crime or of preventing disorder".

325 The Code of Practice on Communication Data specifies that "Where an application relating to national security could be made under either section 60A or section 61, the decision on which authorisation route is most appropriate in any given case is a matter for individual public authorities. Public authorities who wish to use the designated senior officer route should have clear guidelines in place on when this authorisation route is appropriate" (Code of Practice on Communication Data, paragraph 5. 19, available at the following link: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/822817/Communications_Data_Code_of_Practice.pdf ).

326 Section 70(3) of the IPA 2016 provides the definition of a "designated officer" which vary depending on the relevant public authority (as set out in Schedule 4 of the IPA 2016). The Code of Practice on Communications Data further specifies that the designated officer must be independent from the investigation concerned and have working knowledge of human rights principles and legislation, specifically those of necessity and proportionality. If, in case of exceptional circumstances, such as an immediate threat to life or another emergency, the public authority may not be able to call upon the

decision taken by the designated officer will be subject to the *ex-post* oversight carried out by the IPC (see recital (248) below for more details on *ex-post* oversight functions of the IPC).

(199) The authorisation to acquire communication data is based on an assessment of necessity and proportionality of the measure. More specifically, the necessity of the measure is assessed in light of the grounds listed in the legislation[327]. Considering the targeted nature of this measure, it must also be necessary for a specific investigation or operation[328]. Further requirements on the assessment of the necessity of the measures are laid out in the Code of Practice on Communication Data[329]. In particular, this Code provides that the application submitted by the requesting authority should identify three minimum elements to justify the necessity of such request: (i) the event under investigation such as a crime or location of vulnerable missing person; (ii) the person whose data is sought, such as a suspect, witness or missing person, and how they are linked to the event; and (iii) the communications data sought, such as a telephone number or IP address, and how this data is related to the person and the event[330].

(200) Moreover the acquisition of communication data has to be proportionate to what is sought to be achieved[331]. The Code of Practice on Communication Data clarifies that, in conducting such assessment, the authorising individual should carry out a balancing exercise between "the extent of the interference with an individual's rights and freedoms against a specific benefit to the investigation or operation being undertaken by a relevant public authority in the public interest" and that taking into account all the considerations of a particular case, "an interference with the rights of an individual may still not be justified because the adverse impact on the rights of another individual or group of individuals is too severe". Moreover, in order to specifically assess the proportionality of the measure, the Code lists a number of elements that should be included in the application submitted by the requesting authority[332]. Furthermore, particular consideration must be given to the type of

---

services of a designated senior officer who is independent from the investigation or operation, the senior responsible officer must notify the IPC of the circumstances and reasons (noting which designated senior officer granted the authorisation) at the next inspection or as otherwise required by the IPC. The details of the public authorities and the reasons for such measures are being undertaken may be published and included in the IPC's report (Code of Practice on Communications Data, paragraphs 4.12-4.17, see footnote 325).

327 The grounds are: (i) national security; (ii) preventing or detecting crime or of preventing disorder (in case of "events data" only serious crime); (iii) in the interests of the economic well-being of the United Kingdom so far as those interests are also relevant to the interests of national security; (iv) in the interests of public safety; (v) for the purpose of preventing death or injury or any damage to a person's physical or mental health, or of mitigating any injury or damage to a person's physical or mental health; (vi) to assist investigations into alleged miscarriages of justice or (vii) to identify a dead person or person unable to identify themselves because of a certain condition (Section 61(7) of the IPA 2016).

328 Section 60A(1)(b) of the IPA 2016.

329 The Code of Practice on Communications Data, paragraphs 3.3 and following, see footnote 325.

330 The Code of Practice on Communications Data, paragraph 3.13, see footnote 325.

331 Section 60(1)(c) of the IPA 2016.

332 This information to be included must contain: (i) an outline of how obtaining the data will benefit the investigation or operation; (ii) an explanation of the relevance of time periods requested, including how these periods are proportionate to the event under investigation; (iii) an explanation of how the level of intrusion is justified when taking into consideration the benefit the data will give to the investigation (this justification should include consideration of whether less intrusive investigations could be undertaken to achieve the objective); (iv) a consideration of the rights (particularly to privacy and, in relevant cases, freedom of expression) of the individual and a balancing of these rights against the

communication data ("entity" or "events" data[333]) to be acquired, and preference must be given to the use of less intrusive category of data[334]. The Code of Practice on Communication Data also contains specific instructions for authorisations involving the communications data of people in particular professions (such as medical doctors, lawyers, journalists, parliamentarians, or ministers of religion)[335] which are subject to additional safeguards[336].

*(ii) Notice requiring the retention of communication data*

(201) Part 4 of the IPA 2016 sets out the rules on retention of communications data, and in particular the criteria allowing the Secretary of State to issue a retention notice[337]. The safeguards introduced by the IPA apply both when the data is retained for a law enforcement purpose and in the interest of national security.

(202) The issuance of such retention notices aims at securing that telecommunication operators retain, for a maximum period of 12 months, relevant communications data that would otherwise be deleted once no longer required for business purpose[338]. The data retained are to remain available for the period required should it subsequently be necessary for a public authority to acquire it under an authorisation for a targeted acquisition of communication data provided by Part 3 of the IPA 2016 and described in recitals (198) to (200).

(203) The exercise of this power is subject to a number of limitations and safeguards. More specifically, the Secretary of State can issue a retention notice only when he/she considers that the requirement to retain the data is necessary for one of the statutory grounds[339] and it is proportionate to what is sought to be achieved[340]. To that end,

---

benefit to the investigation; (v) details of what collateral intrusion may occur and how the time periods requested impact on the collateral intrusion (Code of Practice on Communications Data, paragraph 3.22-3.26, see footnote 325).

333 See footnote 314.

334 When more intrusive communication data are sought (i.e. events data) the Code specifies that it is more appropriate to acquire first entity data or to acquire directly events data in limited cases of specific urgency (Code of Practice on Communications Data, paragraph 6.10-6.14, see footnote 325).

335 Code of Practice on Communications Data, paragraph 8.8-8.44, see footnote 325.

336 The Code of Practice specifies that "particular care must be taken by an authorising individual when considering such applications, including additional consideration of whether there might be unintended consequences of such applications and whether the public interest is best served by the application" (Code of Practice on communications data, paragraph 8.8). Furthermore, records must be kept for this type of applications and at the next inspection, such applications should be marked for the IPC's attention (Code of Practice on Communications Data, paragraph 8.10, see footnote 325).

337 Section 87 of the IPA 2016.

338 Under Section 90 of the IPA 2016, a telecommunication operator to whom a retention notice is given may ask for a review from the Secretary of State that has issued it.

339 The grounds are (i) the interests of national security; (ii) the applicable crime purpose (as defined in section 87.10A of the IPA 2016); (iii) the interests of the economic well-being of the United Kingdom in so far as those interests are also relevant to the interests of national security; (iv) the interests of public safety; (v) the purpose of preventing death or injury or any damage to a person's physical or mental health, or of mitigating any injury or damage to a person's physical or mental health; or (vi) to assist investigations into alleged miscarriages of justice (Section 87 of the IPA).

340 Section 87 of the IPA 2016. Moreover, according to the relevant code of practice, in order to assess the proportionality of the retention notice, the criteria provided by Section 2(2) of the IPA 2016 apply, notably the requirement to assess whether what is sought to be achieved by the notice, could reasonably be achieved by less intrusive means. Similarly to the assessment of proportionality on the acquisition of communication data, the Code of Practice on Communications Data clarifies that such assessment involves the "balancing between the extent of the interference with an individual's right to respect for

and as clarified by the IPA 2016 itself[341], before issuing a retention notice, the Secretary of State must take into account: the likely benefits of the notice[342]; a description of the telecommunications services; the appropriateness of limiting the data to be retained by reference to location, or descriptions of persons to whom telecommunications services are provided[343]; the likely number of users (if known) of any telecommunications service to which the notice relates[344]; the technical feasibility of complying with the notice; the likely cost of complying with the notice, and any other effect of the notice on the telecommunications operator (or description of operators) to whom it relates[345]. As further detailed in Chapter 17 of the Code of Practice on Communications Data, all retention notices need to specify each data type that needs to be retained and how that data type meets the necessary tests for retention.

(204) An additional safeguard is that the decision of the Secretary of State to issue the retention notice must be approved by an independent Judicial Commissioner[346] under the so-called "double-lock procedure".

3.3.1.1.3 Equipment interference

(205) Equipment interference is a set of techniques used to obtain a variety of data from equipment[347], which includes computers, tablets and smart phones as well as cables, wires and storage devices[348]. Equipment interference allows to obtain both the content of communications and equipment data[349].

(206) In accordance with Section 13(1) of the IPA 2016, the use of equipment interference by an intelligence service requires an authorisation by means of a warrant under the "double lock" procedure established by the IPA 2016, provided that there is "a

---

their private life against a specific benefit to the investigation (Code of Practice on Communications Data, paragraph 16.3, see footnote 325).

341 See section 88 of the IPA 2016.

342 The benefits may be existing or projected and must be in respect of the statutory purposes for which the data can be retained (Code of Practice on Communications Data, paragraph 17.17, see footnote 325).

343 These considerations will include determining whether the full geographical reach of the retention notice is necessary and proportionate and whether it is necessary and proportionate to include or exclude any particular descriptions of persons (Code of Practice on Communications Data, paragraph 17.17, see footnote 325).

344 This will help the Secretary of State to consider both the level of intrusion on customers but also the likely benefits of the data to be retained (Code of Practice on Communications Data, paragraph 17.17, see footnote 325).

345 Section 88 of the IPA 2016.

346 Section 89 of the IPA 2016.

347 Pursuant to Sections 135(1) and 198(1) of the IPA 2016, "equipment" comprises equipment producing electromagnetic, acoustic or other emissions and any device capable of being used in connection with such equipment.

348 Code of Practice on Equipment Interference, available at the following link: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715479/Equipment_Interference_Code_of_Practice.pdf , paragraph 2.2.

349 Equipment data is defined in Section 100 of the IPA 2016 as system data and data which is (a) comprised in, included as part of, attached to or logically associated with a communication (whether by the sender or otherwise) or any other item of information; (b) is capable of being logically separated from the remainder of the communication or the item of information, and (c) if it were so separated, would not reveal anything of what might reasonably be considered to be the meaning (if any) of the communication or the item of information.

British Islands connection"[350]. According to the explanations provided by the UK authorities, in situations where data is transferred from the European Union to the UK within the scope of this Decision, there would always be a "British Islands connection" and any equipment interference covering such data would therefore be subject to the mandatory warrant requirement of Section 13(1) of the IPA 2016[351].

(207) The rules on targeted equipment interference warrants are set out in Part 5 of the IPA 2016. Similarly to targeted interception, targeted equipment interference has to relate to a specific "target", which has to be set out in the warrant[352]. The details on how a "target" must be identified depend on the matter and the type of equipment to be interfered. In particular Section 115(3) of the IPA specifies the elements that should be included in the warrant (e.g. name of the person or organisation, description of the location), depending for example on whether the interference concerns an equipment that belongs, is used to or is in possession of a particular person or an organisation or a group of person, is in a specific location etc.[353]. The purposes for which targeted equipment interference warrants can be issued depends on the public authority applying for it[354].

---

350 For the warrant requirement to be mandatory, Section 13(1) of the IPA 2016 also requires that the conduct of the intelligence service would constitute one or more offences under Sections 1 to 3A of the Computer Misuse Act 1990, which would be the case in the vast majority of circumstances, see Code of Practice on Equipment Interference, paragraphs 3.32 and 3.6 to 3.9). Pursuant to Section 13(2) of the IPA 2016, there is a "British Islands connection" if (a) any of the conduct would take place in the British Islands (regardless of the location of the equipment which would, or may, be interfered with), (b) the intelligence service believes that any of the equipment which would, or may, be interfered with would, or may, be in the British Islands at some time while the interference is taking place, or (c) a purpose of the interference is to obtain (i) communications sent by, or to, a person who is, or whom the intelligence service believes to be, for the time being in the British Islands, (ii) private information relating to an individual who is, or whom the intelligence service believes to be, for the time being in the British Islands, or (iii) equipment data which forms part of, or is connected with, communications or private information falling within subparagraph (i) or (ii).

351 For reasons of completeness it should be noted that even in situations where there is no "British Islands connection" and the use of equipment interference is therefore not subject to the mandatory warrant requirement of Section 13(1) of the IPA 2016, an intelligence service that plans to engage in activity for which it is able to obtain a bulk equipment interference warrant should obtain such warrant as a matter of policy (see Code of Practice on Equipment Interference, paragraph 3.24) . Even where an equipment interference warrant under the IPA 2016 is neither legally required nor obtained as a matter of policy, actions of the intelligence services are subject to a number of conditions and limitations under to Section 7 of the Intelligence Services Act 1994. This includes notably the requirement of an authorisation by the Secretary of State, who must be satisfied that any action does not go beyond what is necessary for the proper discharge of the functions of the Intelligence Service.

352 Section 115 of the IPA 2016 regulates the content of the warrant, specifying that it needs to include the name or description of persons, organisations, location or group of persons that constitute the "target", a description of the nature of the investigation and a description of the activities for which the equipment is used. It must also describe the type of equipment and the conduct which the person to whom the warrant is addressed is authorised to take.

353 See also the Code of Practice on Equipment Interference, paragraph 5.7, see footnote 348.

354 National security agencies can apply for an equipment interference warrant when necessary for national security purposes, for the purpose of detecting serious crime and/or in the interests of the economic well-being of the United Kingdom in so far as those interests are also relevant for the interests of national security (Section 102-103 of the IPA 2016). Depending on the agency, an equipment interference warrant may be requested for a law enforcement purpose when it is necessary for detecting or preventing a serious crime or for the purpose of preventing death or any injury or damage to a person's physical or mental health or of mitigating any injury or damage to a person's physical or mental health (see Section 106(1) and 106(3) of the IPA 2016).

(208) Similarly to targeted interception, the issuing authority needs to consider whether the measure is necessary to achieve a specific purpose and whether it is proportionate to what is sought to be achieved[355]. Moreover, it should also consider whether safeguards exist in relation to security, retention and disclosure as well as in relation to "overseas disclosure"[356] (see recitals (186) above and (195)).

(209) The warrant has to be approved by a Judicial Commissioner, except in cases of urgency[357]. In the latter case, a Judicial Commissioner has to be informed that a warrant has been issued and must approve it within three working days. In case the Judicial Commissioner refuses to approve it, the warrant ceases to have affect and may not be renewed[358]. In all cases, the test applied by the Commissioner is the necessity and proportionality test as applicable to requests for targeted interception[359] (see recital (189) above).

(210) Finally, specific safeguards applicable to targeted interception apply also to equipment interference as regards the duration, renewal, and modification of the warrant as well as the interception of Members of Parliament, of items subject to legal privilege and of journalistic material (see further details in recital (193)).

3.3.1.1.4 Exercise of bulk powers

(211) Bulk powers are regulated in Part 6 of the IPA 2016. Moreover, the Codes of practice provide for more details on the use of bulk powers. While there is no definition in UK law of 'bulk power', in the context of the IPA 2016 it has been described as the collection and retention of large quantities of data acquired by the Government through various means (i.e. the powers of bulk interception, bulk acquisition, bulk equipment interference and bulk personal datasets) and which can subsequently be accessed by the authorities. This description is clarified by contrasting it to what 'bulk power' is not: it does not equate to so-called "mass surveillance" without limitations or safeguards. On the contrary, as explained below, it incorporates limitations and safeguards designed to ensure that access to data is not given on an indiscriminate or unjustified basis[360]. In particular, bulk powers can only be used if a link is established between the technical measure that a national intelligence agency intends to use and the operational objective for which such measure is requested.

(212) Moreover, bulk powers are available to intelligence agencies only and are always subject to a warrant issued by the Secretary of State and approved by a Judicial Commissioner. In choosing the means to collect intelligence, regards must be given

355 Section 102(1) of the IPA 2016.

356 Sections 129 - 131 of the IPA 2016.

357 Section 109 of the IPA 2016.

358 Section 109(4) of the IPA 2016.

359 Section 108 of the IPA 2016.

360 According to the Report on bulk powers presented by Lord David Anderson, independent reviewer of terrorism legislation ahead of the approval of the IPA 2016, "*it should be plain that the collection and retention of data in bulk does not equate to so-called "mass surveillance". Any legal system worth the name will incorporate limitations and safeguards designed precisely to ensure that access to stores of sensitive data (...) is not given on an indiscriminate or unjustified basis. Such limitations and safeguards certainly exist in the Bill*. Lord David Anderson, Report of the bulk power review, August 2016, paragraph 1.9 (emphasis added), available at the following link: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/546925/56730_Cm9326_WEB.PDF

to whether the objective in question can be sought by "less intrusive means"[361]. This approach follows from the framework of the legislation which is built on the principle of proportionality and therefore prioritises targeted over bulk collection.

3.3.1.1.4.1 Bulk interception and bulk equipment interference

(213) The regime for bulk interception is provided in Chapter 1 of Part 6 of the IPA 2016 while Chapter 3 of the same Part regulates bulk equipment interference. These regimes are substantially the same, so the conditions and additional safeguards applicable to those warrants are analysed together.

*(i) Conditions and criteria for the issuance of the warrant*

(214) A bulk interception warrant is limited to the interception of communications in the course of their transmission sent or received by individuals who are outside the British Islands[362], so-called "overseas-related communications"[363], as well as other relevant data and the subsequent selection for examination of the intercepted material[364]. A bulk equipment interference warrant[365] authorises the addressee to secure interference with any equipment for the purpose of obtaining overseas-related communications (including anything comprising speech, music, sounds, visual images or data of any description), equipment data (data that enables or facilitates a functioning of a postal service; a telecommunication system; telecommunications service) or any other information[366].

(215) The Secretary of State can issue a bulk warrant only on an application made by a head of an intelligence service[367]. A warrant authorising a bulk interception or a bulk equipment interference must be issued only if necessary for the interest of national security and for a further purpose of preventing or detecting serious crime, or the

---

361 Section 2.2. of the IPA 2016. See for example the Code of Practice on Bulk Acquisition of Communications Data, paragraph 4.11, available at the following link: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715477/Bulk_Communications_Data_Code_of_Practice.pdf

362 The "British Islands" constitute the United Kingdom, the Channel Islands and the Isle of Man and are defined in Schedule 1 to the Interpretation Act 1978, available at the following link https://www.legislation.gov.uk/ukpga/1978/30/schedule/1.

363 According to Section 136 of the IPA 2016, "overseas-related communications" means: (i) communications sent by individuals who are outside the British Islands, or (ii) communications received by individuals who are outside the British Islands. This regime, as confirmed by the UK authorities, also covers communications between two persons that are both outside the British Islands.

364 Section 136(4) of the IPA 2016. According to the explanations received from the UK government, bulk interception can be used, for example, to identify previously unknown threats to the national security of the UK, by filtering and analysing intercepted material in order to identify communications of intelligence value (Explanatory Framework section H: National security, p. 27 – 28, see footnote29). As explained by the UK authorities, such instruments can be used to establish links between known subjects of interest as well as to search for traces of activity by individuals who may not yet be known but who surface in the course of an investigation, and to identify patterns of activity that may indicate a threat to the United Kingdom.

365 In accordance with Section 13(1) of the IPA 2016, the use of equipment interference by an intelligence service requires an authorisation by means of a warrant under the IPA 2016, provided that there is "a British Islands connection", see recital (206).

366 Section 176 of the IPA 2016. A bulk equipment interference warrant may not authorise a conduct, which would (unless done with lawful authority) constitute unlawful interception (except in relation to a stored communication). According to the Explanatory Framework, the information obtained could be necessary for the identification of subjects of interest and would be usually appropriate large-scale operations (Explanatory Framework, section H: National security p. 28, see footnote 29).

367 Section 138(1) and 178(1) of the IPA 2016.

interest of the economic well-being of the United Kingdom when relevant for national security[368]. Moreover, Section 142(7) of the IPA 2016 requires that a bulk interception warrant must be specified in a greater detailed than the simple reference to the "interests of national security", the "economic wellbeing of the UK" and of "preventing and combating serious crime" but a link must be established between the measure to be sought and one or more operational purpose/s that must be included in the warrant.

(216) The choice of the operational purpose is a result of a multi-layer process. Section 142(4) provides that the operational purposes specified in the warrant must be specified in a list maintained by the heads of the intelligence services, as purposes which they consider are operational purposes for which intercepted content or secondary data obtained under bulk interception warrants may be selected for examination. The list of operational purposes must be approved by the Secretary of State. The Secretary of State may give such approval only if satisfied that the operational purpose is specified in a greater level of detail than the general grounds for authorising the warrant (national security or national security and economic well-being or preventing serious crime)[369]. At the end of each relevant three-month period, the Secretary of State must give a copy of the list of operational purposes to the Parliamentary ISC. Finally, the Prime Minister must review the list of operational purposes at least once a year[370]. As noted by the High Court, "[t]hese are not to be belittled as insignificant safeguards, as they build together an intricate set of modes of accountability, which involve Parliament as well as members of the government at the highest level"[371].

(217) Such operational purposes also limit the scope of the selection of the interception material for the examination stage. The selection for examination of the material collected under the bulk warrant must be justified in light of the operational purpose/s. As explained by the UK authorities, this means that practical arrangements on examination must be assessed by the Secretary of State already at the stage of the warrant, providing sufficient details to fulfil the statutory duties under section 152 and 193 of the IPA 2016[372]. The details given to the Secretary of State in relation to those arrangements would need to include for example, information (if applicable) on how filtering arrangements might vary during the time that a warrant will have effect[373]. For more details on the process and the safeguards applied to the filtering and examination phases, see recital (223) below.

(218) A bulk power can be authorised only if its proportionate to what is sought to be achieved[374]. As specified in the Code of Practice on Interception, any assessment of proportionality involves "balancing the seriousness of the intrusion into the privacy

368 Section 138 (2) and 178(2) of the IPA 2016.

369 According to the explanations provided by the UK authorities, for example, an operational purpose may limit the scope of the measure to the existence of a threat in a specific geographical area.

370 Section 142(4)-(10) of the IPA 2016.

371 High Court of Justice, *Liberty*, [2019] EWHC 2057 (Admin), paragraph 167.

372 Sections 152 and 193 of the IPA 2016 require that: (a) the selection for examination is carried out only for the operational purposes specified in the warrant, (b) the selection for examination is necessary and proportionate in all the circumstances, and (c) the selection for examination does not breach the prohibition of selecting material and identify communications that have been sent by or are intended for individuals known to be in the British Islands at that time.

373 See Code of Practice on Interception of Communications, paragraph 6.6, see footnote 282.

374 Sections 138(1)(b) and (c) and Sections 178(b) and (c) of the IPA 2016.

(and other considerations set out in section 2(2)) against the need for the activity in investigative, operational or capability terms. The conduct authorised should offer a realistic prospect of bringing the expected benefit and should not be disproportionate or arbitrary"[375]. As already mentioned, this means in practice that the proportionality test is based on a balance test between what is sought to be achieved ("operational purpose/s") and the technical options available (e.g. targeted or bulk interception, equipment interference, acquisition of communication data), giving preference to the least intrusive means (see recitals (178) and (179) above). When more than one measure is appropriate to the objective, the less intrusive means must be preferred.

(219) An additional safeguard on the assessment of the proportionality of the measure requested is ensured by the fact that the Secretary of State must receive the relevant information needed to properly carry out his/her assessment. In particular, the Code of Practice on Interception and the Code of Practice on Equipment Interference require that the application submitted by the relevant authority should mention the background of the application, the description of communications to be intercepted and the telecommunications operators required to assist, the description of the conduct to be authorised, the operational purposes, and an explanation on why the conduct is necessary and proportionate[376].

(220) Finally and importantly, the Secretary of State's decision to issue the warrant must be approved by an independent Judicial Commissioner that assesses the evaluation of the necessity and proportionality of the proposed measure, using the same principles that would be used by a court in an application for judicial review[377]. The Judicial Commissioner will review the Secretary of State's conclusions as to whether the warrant is necessary and whether the conduct is proportionate in the light of the principles set in Section 2(2) of the IPA 2016 (general duties in relation to privacy). The Judicial Commissioner will also review the Secretary of State's conclusions as to whether each of the operational purposes specified on the warrant is a purpose for which selection is, or may be, necessary. If the Judicial Commissioner refuses to approve the decision to issue a warrant the Secretary of State may either: (i) accept the decision and therefore not issue the warrant; or (ii) refer the matter to the Investigatory Powers Commissioner for a decision (unless the Investigatory Powers Commissioner has made the original decision)[378].

*(ii) Additional safeguards*

(221) The IPA 2016 has introduced further limits on the duration, renewal and modification of a bulk warrant. The warrant must have a duration of a maximum of six months and any decision to renew or modify (except minor modifications) the warrant must be also approved by a Judicial Commissioner[379]. The Code of Practice

375 Code of Practice on Interception of Communications, paragraph 4.10, see footnote 282.

376 Code of Practice on Interception of Communications, paragraph 6.20, see footnote 282, and Code of Practice on Equipment Interference, paragraph 6.13, see footnote 348.

377 Section 138(1)(g) and 178(1)(f) of the IPA 2016.

378 Section 159 (3) and (4) of the IPA 2016.

379 Sections 143 – 146, and 184 - 188 of the IPA 2016. In case of an urgent modification the Secretary of State can make the modification without an approval, but must notify the Commissioner and the Commissioner must then decide whether to approve or refuse the modification (Section 147 of the IPA 2016). The warrants must be cancelled, where the warrant is no longer necessary or proportionate, or that the examination of intercepted content, metadata or other data obtained under the warrant is no longer necessary for any of the operational purposes specified on the warrant (Section 148, and 189 of the IPA 2016).

on Interception and the Code of Practice on Equipment Interference specified that a change in the operational purposes of the warrant is considered as a major modification of the warrant[380].

(222) Similar to what is provided for targeted interception, Part 6 of the IPA 2016 provides that the Secretary of State must ensure that arrangements are in force to provide safeguards on the retention and disclosure of material obtained under the warrant[381], as well as for overseas disclosure[382]. In particular, Sections 150(5) and 191(5) of the IPA 2016 require that every copy made of any of that material collected under the warrant must be stored in a secure manner and is destroyed as soon as there are no longer any relevant grounds for retaining it, while Sections 150(2) and 191(2) require that the number of persons to whom the material is disclosed and the extent to which any material is disclosed, made available or copied must be limited to the minimum that is necessary for the statutory purposes. Finally, when the material that has been intercepted either through a bulk interception or a bulk equipment interference is to be handed over to a third country ("overseas disclosures"), the IPA 2016 provides that the Secretary of State must ensure that appropriate arrangements are in place to ensure that similar safeguards on security, retention and disclosure exist in that third country[383].

(223) Once the warrant has been approved and the data has been collected in bulk, the data will be subject to a selection before being examined. The selection and examination phase is subject to a further proportionality test carried out by the analyst that defines, on the basis of the operational purposes included in the warrant (and potentially existing filtering arrangements) the criteria for selection. As provided by sections 152 and 193 of the IPA, when issuing the warrant the Secretary of State must ensure that arrangements are in place to guarantee that the selection of the material is carried out only for the specified operational purposes and that it is necessary and proportionate in all circumstances. In this respect, the UK authorities clarified that the material intercepted in bulk is selected, first of all, via automated filtering with the aim to discard data that is unlikely to be of national security interest. The filters will vary from time to time (as internet traffic patterns, types and protocols change) and will depend on the technology and operational context. After this phase, the data can be selected for examination only if relevant for the operational purposes specified in the warrant[384]. Section 152 and 193 of the IPA

380 Code of Practice on Interception of Communications, paragraph 6.44-6.47, see footnote 282, and Code of Practice on Equipment Interference, paragraph 6.48, see footnote 348.

381 Section 156 of the IPA 2016.

382 Sections 150 and 191 of the IPA 2016.

383 Sections 151 and 192 of the IPA 2016.

384 The Codes on interception of communications specifies, in this respect that "These processing systems process data from the communications links or signals that the intercepting authority has chosen to intercept. A degree of filtering is then applied to the traffic on those links and signals, designed to select types of communications of potential intelligence value whilst discarding those least likely to be of intelligence value. As a result of this filtering, which will vary between processing systems, a significant proportion of the communications on these links and signals will be automatically discarded. Further complex searches may then take place to draw out further communications most likely to be of greatest intelligence value, which relate to the agency's statutory functions. These communications may then be selected for examination for one or more of the operational purposes specified in the warrant where the conditions of necessity and proportionality are met. Only items which have not been filtered out can potentially be selected for examination by authorised persons" (Codes of practice on interception of communications, paragraph 6.6, see footnote 282).

2016 also provide for a general prohibition to select for examination material referring to conversations sent by or intended to individuals who are in the British Islands. If the authorities wish to examine such material, they would submit a request for a targeted examination warrant under Part 2 and Part 4 of the IPA 2016, issued by the Secretary of State and approved by a Judicial Commissioner. If a person deliberately selects intercepted content for examination in breach of the requirements set in the legislations[385] he or she commits a criminal offence[386].

(224) The assessment carried out by the analyst over the selection of the material is subject to an *ex post* oversight by the IPC who evaluates the compliance with the specific safeguards set in the IPA 2016 for the examination phase[387] (see also recital (223)). The IPC must keep under review (including by way of audit, inspection and investigation) the exercise by public authorities of the investigatory powers mentioned in the IPA 2016[388]. In this respect, the Code of Practice on Interception and the Code of Practice on Equipment Interference clarify that records must be kept by the agency for purposes of subsequent examination and audits, and these records must outline why access to the material by authorised persons is necessary and proportionate and the applicable operational purposes[389]. For example, in its 2018 Annual report the Investigatory Powers Commissioner Office (IPCO)[390] concluded that the justifications recorded by the analysts for the examination of certain material collected in bulk met the required standard of proportionality, by providing sufficient details of the reasons of their "queries" in relation to the purpose to be achieved[391]. In its 2019 report, the IPCO was satisfied with the use of bulk powers by the GCHQ, especially in light of compliance with the requirement s of necessity and proportionality. Moreover the IPCO was satisfied that "GCHQ continue to consider carefully on a case-by-case basis whether it is most appropriate to authorise EI [equipment interference] activity under bulk or targeted warrants and we will continue to pay close attention to this both during our consideration of warrant applications under the double lock and at inspections"[392].

3.3.1.1.4.2 Bulk acquisition of communications data

(225) Chapter 2 of Part 6 of the IPA 2016 regulates bulk acquisition warrants that authorise the addressee to require a telecommunications operator to disclose or obtain any communications data in the possession of the operator. These warrants also authorize the requesting authority to select the data for the further phase of the examination. As it is the case for targeted retention and acquisition of communications data (see recital (196)), also the bulk acquisition of communications data does normally not concern personal data of EU data subjects transferred under this Decision to the UK.

385 Section 152 and 193 of the IPA 2016.

386 Section 155 and 196 of the IPA 2016.

387 Section 152 and 193 of the IPA 2016.

388 Section 229 of the IPA 2016.

389 Code of Practice on Interception of Communications, paragraph 6.74, see footnote 282 and Code of Practice on Equipment Interference, paragraph 6.78, see footnote 348.

390 The IPCO is constituted under Section 238 of the IPA 2016 to provide the IPC with necessary staff, accommodation, equipment and other facilities and services necessary for the carrying out of his/her functions (see recital (245))

391 The IPCO Annual Report of 2018 specified that the justifications recorded by the analysts of the GCHQ "were meeting the required standard and analysts were accounting for the proportionality of their queries of bulk data in sufficient detail". Annual Report of the Investigatory Powers Commissioner 2018, paragraph 6.22, see footnote 456.

392 Annual Report of the Investigatory Powers Commissioner 2019, paragraph 10.22, see footnote 455.

The obligation to disclose communications data pursuant to Chapter 2 of Part 6 of the IPA 2016 covers data that is collected by telecommunication operators in the UK directly from the users of a telecommunication service[393]. This type of "customer facing" processing typically does not involve a transfer on the basis of this Decision, i.e. a transfer from a controller/processor in the EU to a controller/processor in the UK.

(226) However, for the sake of completeness the conditions and safeguards governing the acquisition of bulk communications data are described below.

(227) The IPA 2016 replaces the legislation concerning the acquisition of bulk communications data which was the subject of the CJEU judgment in the *Privacy International* case. The legislation at issue in that case was repealed and the new regime provides for specific conditions and safeguards under which such measure can be authorised.

(228) In particular, differently from the previous regime under which the Secretary of State had full discretion in authorising the measure[394], the IPA 2016 requires the Secretary of State to issue a warrant only if the measure is necessary and proportionate. This means in practice that there should be a link between the access to the data and the aim pursued[395]. More specifically, the Secretary of State will have to assess the existence of a link between the measure requested and one or more "operational purpose/s" indicated in the warrant (see recital (219)) respect to the assessment of the proportionality, the relevant code of practice specifies that "the Secretary of State must take into account whether what is sought to be achieved by the warrant could reasonably be achieved by other less intrusive means (Section 2(2)(a) of the Act). For example, obtaining the required information through a less intrusive power such as the targeted acquisition of communications data"[396].



393 This follows from the definition of communications data provided in Section 261(5) of the IPA 2016, according to which communications data is held or obtained by a telecommunications operator and is either about the user of a telecommunications service and relating to the provision of this service, or is comprised in, included as part of, attached to or logically associated with a communication (see also Code of Practice on Bulk Acquisition of Communications Data, available at the following link: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715477/Bulk_Communications_Data_Code_of_Practice.pdf paragraphs 2.15 to 2.22). Moreover, the definition of telecommunications operator provided in Section 261(10) of the IPA 2016 requires that a telecommunications operator is a person who offers or provides a telecommunications service to persons in the UK or who controls or provides a telecommunication system which is (wholly or partly) in or controlled from the UK. These definitions make clear that obligations under the IPA 2016 cannot be imposed on telecommunications operators whose equipment is not in or controlled from the UK and who do not offer or provide services to persons in the UK (see also Code of Practice on Bulk Acquisition of Communications Data, paragraph 2.2). If EU subscribers (whether located in the EU or in the UK) made use of services in the UK, any communications in relation to the provision of this service would be collected directly by the service provider in the UK rather than subject to a transfer from the EU.

394 Section 94(1) of the Telecommunication Act 1984 provided that the Secretary of State could issue "directions of a general character as appear to the Secretary of State to be requisite or expedient in the interests of national security (…)" (see footnote 451).

395 See *Privacy International*, paragraph 78

396 See Code of Practice on Bulk Acquisition of Communications Data, paragraph 4.11, (see footnote 393414).

(229) To conduct such assessment, the Secretary of State will rely on information that the heads of intelligence[397] are required to submit in their application, such as the reasons why the measure is considered to be necessary for one of the statutory grounds and the reasons why what is sought to be achieved could not reasonably be achieved by other less intrusive means[398]. Moreover, the operational purposes limit the scope for which data obtained under the warrant can be selected for examination[399]. As specified in the relevant code of practice, the operational purposes must describe a clear requirement and contain sufficient detail to satisfy the Secretary of State that acquired data may only be selected for examination for specific reasons[400]. In fact, the Secretary of State will have to ensure, before authorising the warrant, that specific arrangements are in place for securing that only that material which has been considered necessary for examination for an operational purpose and a statutory purpose is selected for the examination and should be proportionate and necessary in all circumstances. This specific requirement, reflected in sections 158 and 172[401] of the IPA 2016, regarding the prior assessment of the necessity and proportionality of the criteria used for the purposes of selection represents another important novelty of the regime introduced by the IPA 2016 compared to the regime previously in place.

(230) The IPA 2016 also introduced the obligation on the Secretary of State, to ensure that, before issuing the warrant for the bulk acquisition of communications data specific limitations are in place on the security, the retention and the disclosure of the personal data collected[402]. In case of overseas disclosure, the safeguards, described in recital (222), for bulk interception and bulk equipment interference apply also in this context[403]. Further limits are set out in the legislation on the duration[404], renewal[405] and modification of the bulk warrants[406].

(231) Importantly, as for the other bulk powers, before issuing the warrant, the Secretary of State needs get the approval by a Judicial Commissioner[407]. This is key feature of the regime put in place by the IPA 2016.

(232) The IPC carries out an *ex post* oversight on the examination procedure over the material (communication data) acquired in bulk (see recital (248) below. In that respect, the IPA 2016 introduced the requirement that the intelligence analysist carrying out the examination, has to record, prior to selecting the data for

397 A bulk acquisition warrant may be requested only by the heads of the intelligences services which are: (i) the Director General of the Security Service; (ii) the Chief of the Secret Intelligence Service; or (iii) the Director of the GCHQ (see section 158 and 263 of the IPA 2016).

398 Code of practice on bulk acquisition of communications data, paragraph 4.5 (see footnote 393).

399 According to section 161 of the IPA 2016, the operational purposes specified in the warrant must be ones specified, in a list maintained by the heads of the intelligence services ("the list of operational purposes"), as purposes which they consider are operational purposes for which communications data obtained under bulk acquisition warrants may be selected for examination.

400 Code of Practice on Bulk Acquisition of Communications Data, paragraph 6.6 (see footnote 393).

401 Section 172 of the IPA 2016 requires that specific safeguards must be put in place for the phase of filtering and selection for the examination of communication acquired in bulk. Moreover, a deliberate examination in breach of these safeguards is also a criminal offense (see section 173 of the IPA 2016).

402 Section 171 of the IPA 2016.

403 Section 171 (9) of the IPA 2016.

404 Section 162 of the IPA 2016.

405 Section 163 of the IPA 2016.

406 Section, 164 – 166 of the IPA 2016.

407 Section 159 of the IPA 2016.

examination, the reason why the proposed examination is necessary and proportionate for a specified operational purpose[408]. In the IPCO Annual Report 2019 it was found with respect to GCHQ's and MI5's practice that "the critical role of bulk communications data (BCD) to the range of activities conducted at GCHQ was well articulated in the casework we inspected. We considered the nature of the requested data and the stated intelligence requirements and were satisfied that the documentation demonstrated that their approach was necessary and proportionate"[409]. MI5's recorded justifications were of a good standard and satisfied the principles of necessity and proportionality"[410].

3.3.1.1.4.3 Retention and examination of bulk personal datasets

(233) Bulk Personal Dataset (BPD) warrants[411] authorise intelligence agencies to retain and examine sets of data that contain personal data relating to a number of individuals. According to the explanations provided by the UK authorities, the analysis of such datasets can be "the only way for UKIC to progress investigations and identify terrorists from very limited lead intelligence, or when their communications have been deliberately concealed"[412]. There are two types of warrants: "class BPD warrants"[413] which concern a certain category of datasets, i.e. datasets which are similar in their content and proposed use and raise similar considerations as to, for instance, the degree of intrusion and sensitivity and the proportionality of using the data, therefore allowing the Secretary of State to consider the necessity and proportionality of acquiring all data within the relevant class all at once. For example, a class BPD warrant may cover travel datasets that relate to similar routes[414]. "Specific BPD warrants"[415] instead concern one specific dataset, such as a dataset of a novel or unusual type of information which does not fall within an existing class BPD warrant, or a dataset that concerns specific types of personal data[416] and therefore requires additional safeguards[417]. The provisions of the IPA 2016 relating to BPDs allow such datasets to be examined and retained only where it



408 IPCO Annual Report 2019, paragraph 8.6, see footnote 455.

409 IPCO Annual Report 2019, paragraph 10.4, see footnote 455.

410 IPCO Annual Report 2019, paragraph 8.37, see footnote 455.

411 Section 200 of the IPA 2016.

412 UK Explanatory Framework for Adequacy Discussions, section H: National Security, page 34, see footnote 29.

413 Section 204 of the IPA 2016.

414 Code of Practice on Intelligence Services' Retention and Use of Bulk Personal Datasets, paragraph 4.7, available at the following link: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715478/Bulk_Personal_Datasets_Code_of_Practice.pdf

415 Section 205 of the IPA 2016.

416 Such as, for example, sensitive personal data, see Section 202 of the IPA 2016 and Code of Practice on Intelligence Services' Retention and Use of Bulk Personal Datasets, paragraphs 4.21 and 4.12, see footnote 469.

417 An application for a specific BPD warrant must be considered individually by the Secretary of State, i.e. with respect to one specific dataset. The intelligence service is required by Section 205 of the IPA to include in its application for a specific BPD warrant a detailed explanation of the nature and extent of the material in question and a list of the "operational purposes" for which the relevant intelligence service wishes to examine the BPD (where the intelligence service seeks a warrant for retention and examination, rather than retention only). When issuing a class BPD warrant, the Secretary instead considers the whole category of datasets at once.

is necessary and proportionate to do so[418], and in line with the general obligations relating to privacy[419].

(234) The power to issue a BPD warrant is subject to the "double lock" procedure: the assessment of the necessity and proportionality of the measure is first carried out by the Secretary of State and then by the Judicial Commissioner[420]. The Secretary of State is required to consider the nature and scope of the type of warrant being sought, the category of data concerned and the number of individual bulk personal datasets likely to fall within the specific type of warrant[421]. Also, as specified in the Code of Practice on Intelligence Services' Retention and Use of Bulk Personal Datasets, detailed records are to be kept and are subject to IPC audit[422]. Retaining and examining BPD outside the limits of the IPA 2016 is a criminal offense[423].

*3.3.2 Further use of the information collected*

(235) Personal data processed under Part 4 of the DPA 2018 must not be processed in a manner that is incompatible with the purpose for which it was collected[424]. The DPA 2018 provides that the controller can process the data for another purpose, different from that for which the data was collected, when it is compatible with the original one and provided that the controller is authorised by law to process the data and that processing is necessary and proportionate[425]. Moreover, the Security Services Act 1989 and the Intelligence Services Act 1994 specify that the heads of the intelligence agencies have the duty to ensure that no information is obtained or disclosed except so far as necessary for the proper discharge of the agency functions or for the other limited and specific purposes listed in the relevant provisions[426].

(236) In addition, Section 109 of the DPA 2018 sets out specific requirements for international transfers of personal data by intelligence services to third countries or international organisations. According to this provision, personal data is not allowed to be transferred to a country or territory outside the United Kingdom or to an international organization, unless the transfer is necessary and proportionate for the purpose of the controller's statutory functions or for other purposes provided for in

418 Section 204 and Section 205 of the IPA 2016.

419 Section 2 of the IPA 2016.

420 Sections 204 and 205 of the IPA 2016.

421 Code of Practice on Intelligence Services' Retention and Use of Bulk Personal Datasets, paragraph 5.2, see footnote 414.

422 Code of Practice on Intelligence Services' Retention and Use of Bulk Personal Datasets, paragraphs 8.1-8.15, see footnote 414.

423 UK Explanatory Framework for Adequacy Discussions, section H: National Security, page 34, see footnote29.

424 Section 87(1) of DPA 2018.

425 Section 87(3) of the DPA 2018. While controllers can be exempt from this principle pursuant to Section 110 of the DPA 2018 to the extent that such exemption is required to safeguard national security, such exemption must be assessed case-by-case and can be invoked only as far as the application of a particular provision would have negative consequences for national security (see recital (129)). The national security certificates for the UK intelligence services (available at the following link: https://ico.org.uk/about-the-ico/our-information/national-security-certificates/) do not cover Section 87(3) of the DPA 2018. Moreover, as any processing for a different purpose must be authorised by law, intelligence services must have a clear legal basis for the further processing.

426 These purposes are: for the Security Service the prevention or detection of serious crime or any criminal proceedings (Section 2(2)(a) of the Security Services Act 1989), for the Intelligence Service the interests of national security, the prevention or detection of serious crime, or any criminal proceedings (Section 2(2)(a) of the Intelligence Services Act 1994), and for the GCHQ any criminal proceedings (Section 4(2)(a)of the Intelligence Services Act 1994).

Section 2(2)(a) of the Security Services Act 1989 or Sections 2(2)(a) and 4(2)(a)of the Intelligence Services Act 1994[427].

(237) Finally, the IPA 2016 sets out further safeguards in relation to transfers to a third country of material collected through targeted interception[428], targeted equipment interference[429], bulk interception[430], bulk acquisition of communications data[431] and bulk equipment interference[432] (so-called "overseas disclosures"). In particular, the authority issuing the warrant must ensure that arrangements are in force for securing that the third country receiving the data limits the number of persons who see the material, the extent of disclosure and the number of copies made of any material to the minimum necessary for the authorised purposes set out in the IPA 2016[433].

*3.3.3 Oversight*

(238) Government access for national security purposes is overseen by a number of different bodies. The Information Commissioner oversees the processing of personal data in light of the DPA 2018 (for more information on the independence, appointment role and powers of the Commissioner see recitals (85) to (98)), while independent and judicial oversight on the use of investigatory powers under the IPA 2016 is provided by the IPC. The IPC oversees the use of IPA 2016 investigatory powers by both law enforcement and national security authorities. Political oversight is guaranteed by the Intelligence Service Committee of the Parliament.

3.3.3.1 Oversight under Part 4 of the DPA

(239) The processing of personal data carried out by the intelligence services under Part 4 of the DPA 2018, is overseen by the Information Commissioner[434].

(240) 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, 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, promote the awareness of controllers and processors of their obligations, provide information to a data subject concerning the exercise of the data subject's rights, conduct investigations etc.

(241) The Commissioner, as for Part 3 of the DPA 2018, has the powers 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

427 See footnote 426.
428 Section 54 of the IPA 2016.
429 Section 130 of the IPA 2016.
430 Section 151 of the IPA 2016.
431 Section 171 (9) of the IPA 2016.
432 Section 192 of the IPA 2016.
433 The arrangements must include measures for securing that every copy made of any of that material is stored, for as long as it is retained, in a secure manner. The material obtained under a warrant and every copy made of any of that material must be destroyed as soon as there are no longer any relevant grounds for retaining it.
434 Section 116 of the DPA 2018.

provision of the act[435]. However, differently than for other parts of the DPA 2018, the Commissioner cannot give an assessment notice to a national security body[436].

(242) 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 do inspections in accordance with international obligations, the powers of entry and inspection, and the rules on offences[437]. As explained in recital (125), these exceptions apply only if necessary and proportionate and on case-by-case basis.

(243) The ICO and UK intelligence services have signed a Memorandum of Understanding[438] that establishes a framework for co-operation 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 that the application of any national security exemption has been used 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 intelligence agency, 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[439].

3.3.3.2 Oversight of the use of investigatory powers under the IPA 2016

(244) Pursuant to Part 8 of the IPA 2016, oversight over the use of investigatory powers is exercised by the Investigatory Powers Commissioner (IPC). The IPC is assisted by other Judicial Commissioners, which are collectively referred to as Judicial

435 Pursuant to Schedule 13 paragraph 2 to 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 recital (92) above).

436 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).

437 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.

438 Memorandum of Understandings between Information Commission's Office and the UK Intelligence Community, see footnote 170.

439 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).

Commissioners[440]. Pursuant to Section 227 of the IPA 2016, the Prime Minister must appoint the IPC and as many Judicial Commissioners as he considers necessary, subject to the agreement of the senior judicial officers for England & Wales, Scotland and Northern Ireland[441]. The Judicial Commissioners are required to hold, or have held, a high judicial office[442]and, as any member of the judiciary, they enjoy an independent status from the government[443]. The Secretary of State must provide the IPC with staff, accommodation, equipment and other facilities and services[444]. The term of the Commissioners is three years and they can be reappointed[445]. Judicial Commissioners can be removed from office only subject to strict conditions imposing a high threshold: either by the Prime Minister in the specific circumstances listed in an exhaustive manner in Section 228(5) of the IPA 2016 (such as bankruptcy or imprisonment), or if a resolution approving the removal has been passed by each House of Parliament[446].

(245) The IPC and Judicial Commissioners are supported in their roles by the Investigatory Powers Commissioner's Office (IPCO). The IPCO's staff includes a team of inspectors, in-house legal and technical expertise, and a Technology Advisory Panel to provide expert advice. The IPCO is an "arm's-length body" of the Home Office, i.e. it receives funding from the Home Office, but carries out its functions independently[447].

(246) The main functions of the Judicial Commissioners are set out in Section 229 of the IPA 2016. In particular, the Judicial Commissioners have an extensive power of prior approval, which is part of the safeguards introduced in the United Kingdom legal framework with the IPA 2016. Warrants in relation to targeted interception, equipment interference, bulk personal datasets, bulk acquisition of communication data as well as retention notices for communication data all have to be approved by

---

440 In accordance with Section 227(7) and (8) of the IPA 2016, the Investigatory Powers Commissioner is a Judicial Commissioner, and the Investigatory Powers Commissioner and the other Judicial Commissioners are to be known, collectively, as the Judicial Commissioners. There are currently 15 Judicial Commissioners.

441 Section 227(3) of the IPA 2016. Judicial Commissioners must be recommended also by the Investigatory Powers Commissioner, Section 227(4)(e) of the IPA 2016.

442 According to Section 60(2) of Part 3 of the Constitutional Reform Act 2005, a "high judicial office" means office as a judge of any of the following courts: (i)the Supreme Court; (ii )the Court of Appeal in England and Wales; (iii) the High Court in England and Wales; (iv) the Court of Session; (v) the Court of Appeal in Northern Ireland; (vi) the High Court in Northern Ireland; or as a Lord of Appeal in Ordinary.

443 The independence of the judiciary is based on convention and has been broadly recognized since the 1701 Act of Settlement.

444 Section 238 of the IPA 2016.

445 Section 227(2) of the IPA 2016.

446 The removal process is identical to the removal process for other judges in the UK (see for example Section 11(3) of the Senior Courts Act 1981 and Section 33 of the Constitutional Reform Act 2005, which also require a resolution following an approval by both House of the Parliament). To date, no Judicial Commissioner has been removed from office.

447 An arm's-length body is an organization or agency that receives funding from a government, but is able to act independently (for a definition and more information on an arm's length body see the Handbook of the Cabinet Office on the classification of Public Bodies, available at the following link: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/519571/Classification-of-Public_Bodies-Guidance-for-Departments.pdf and the First Report of session 2014-2015 of the Public Administration Select Committee of the House of Commons, available at the following link: https://publications.parliament.uk/pa/cm201415/cmselect/cmpubadm/110/110.pdf )

Judicial Commissioners[448]. The IPC must also always pre-authorise the acquisition of communication data for law enforcement purposes[449]. If a Commissioner refuses to approve a warrant, the Secretary of State can appeal to the Investigatory Powers Commissioner, whose decision is final.

(247) The UN Special Rapporteur on the Right to Privacy strongly welcomed the establishment of the Judicial Commissioners with the IPA 2016, as "all the more sensitive or intrusive requests to conduct surveillance need to be authorized by both a cabinet minister and the Investigatory Powers Commissioner's Office". In particular, he stressed that "this element of judicial review [through the role of the IPC] assisted by a better-resourced team of experienced inspectors and technology experts is one of the most significant new safeguards introduced by the IPA", that replaced a previously fragmented system of oversight authorities and complements the role of the Intelligence and Security Committee of Parliament and the Investigatory Powers Tribunal"[450].

(248) In addition, the IPC has the powers to carry out *ex post* oversight[451] of the use of investigatory powers under the IPA 2016 and some other powers and functions provided in relevant legislation[452]. The results of such *ex post* oversight are included in the report that the IPC must prepare annually and present to the Prime Minister[453] and that must be published and laid before Parliament[454]. The report contains relevant statistics and information about the use of the investigatory powers by intelligence agencies and law enforcement authorities as well as the deployment of the safeguards in relation to items subject to legal privilege, confidential journalistic material and sources of journalistic information, information on the arrangements taken and the operational purposes used in the context of bulk warrants. Finally, in the IPCO Annual Report, it is specified in which area recommendations were given to public authorities and how they have been addressed[455].

---

448 Decisions on whether to approve a decision by the Secretary of State to issue a warrant are a matter for the Judicial Commissioners themselves. If a Commissioner refuses to approve a warrant, the Secretary of State can appeal to the Investigatory Powers Commissioner, whose decision is final.

449 The IPC authorization is always requested where communication data is acquired for purposes of law enforcement (Section 60A of the IPA 2016). Where communication data is acquired for purposes of national security, the authorisation can be granted by the IPC or, alternatively, by a designated senior officer of the relevant public authority (See Sections 61 and 61A of the IPA 2016 and recital (198) above).

450 End of Mission Statement of the Special Rapporteur on the Right to Privacy at the Conclusion Of his Mission to the United Kingdom of Great Britain and Northern Ireland (see footnote 285).

451 Section 229 of the IPA 2016.

452 This includes surveillance measures under the RIPA 2016, the exercise of functions under Part 3 of the Police Act 1997 (authorisation of action in respect of property), and the exercise by the Secretary of State of functions under Sections 5 to 7 of the Intelligence Services Act 1994 (warrants for interference with wireless telegraphy, entry and interference with property (Section 229 of the IPA 2016).

453 Section 230 of the IPA 2016. The IPC can also report to the Prime Minister on his own initiative on any matter relating to his functions. The IPC must also report to the Prime Minister on his request and the Prime Minister can direct the IPC to review any functions of the Intelligence Services.

454 Some parts may be excluded if publishing them would be contrary to national security.

455 For example, in the IPCO annual report 2019 (paragraph 6.38) it is mentioned that MI5 was recommended to modify their policy of retention for bulk personal datasets (BPD) since it should have taken an approach where consideration was given to the proportionality of the retention for all fields in BPD holdings and for each BPD held. At the end of 2018, the IPCO was not satisfied that this recommendation was followed and the 2019 report explained that the MI5 is now introducing a new process to discharge this requirement. The 2019 annual report (paragraph 8.22) mentions also that GHCQ was given a series of recommendations concerning the record accounting for the proportionality

(249) In accordance with Section 231 of the IPA 2016, if the IPC becomes aware of any relevant error committed by public authorities in the use of their investigatory powers, it must inform the person concerned where they consider that the error is serious and it is in the public interest for the person to be informed[456]. In particular, Section 231 of the IPA 2016 specifies that, when informing a person of an error, the IPC must provide information on any right he/she has to apply to the Investigatory Powers Tribunal, and provide such details as the Commissioner considers necessary for the exercise of those rights and there is a public interest for the disclosure[457].

3.3.3.3 Parliamentary oversight of Intelligence services

(250) The parliamentary oversight by the Intelligence and Security Committee (ISC) has its statutory footing in the Justice and Security Act 2013 (JSA 2013)[458]. The Act establishes the ISC as a committee of the UK Parliament. 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 investigations on operational matters when they do not relate to ongoing operations[459]. The Memorandum of Understanding agreed between the Prime Minister and the ISC[460] specifies in details the elements to be taken into account when considering whether an activity is not part of any ongoing operation[461]. The ISC can also be asked to investigate ongoing operations by the Prime Minister and can review information voluntarily provided by the agencies.

(251) Under Schedule 1 to 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[462]. According to the

---

of their queries on bulk data. The report confirms that improvements have been made in this area at the end of 2018. Annual Report of the Investigatory Powers Commissioner Office 2019, available at the following link: https://www.ipco.org.uk/docs/IPC%20Annual%20Report%202019_Web%20Accessible%20version_final.pdf

456 An error is considered "serious" when the Commissioner considers that it has caused significant prejudice or harm to the person concerned (Section 231(2) of the IPA 2016). In 2018, 22 errors were reported of which eight were deemed serious and resulted in information to the person concerned. See Annual Report of the Investigatory Powers Commissioner Office 2018, Annex C (see https://www.ipco.org.uk/docs/IPCO%20Annual%20Report%202018%20final.pdf). In 2019, 14 errors were considered to amount to serious. See Annual Report of the Investigatory Powers Commissioner Office 2019, Annex C, see footnote 455.

457 Section 231 of the IPA 2016 specifies that when informing a person of an error, the IPC must such details as the Commissioner considers necessary for the exercise of those rights, having regard in particular to the extent to which disclosing the details would be contrary to the public interest or prejudicial to the prevention or detection of serious crime, the economic well-being of the United Kingdom, or the continued discharge of the functions of any of the intelligence services.

458 As explained by UK 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.

459 Section 2 of the JSA 2013.

460 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

461 Memorandum of Understanding between the Prime minister and the ISC, para 14, see footnote 460.

462 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

explanations provided by the United Kingdom authorities, in practice very little information is withheld from the ISC[463].

(252) 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[464]. The ISC is required to make an annual report to Parliament on the discharge of its functions and other reports that it considers appropriate[465]. Moreover, the ISC is entitled to receive every three months the list of operational purposes that is used to examine material obtained in bulk[466]. Copies of the investigations, inspections or audits of the Investigatory Power Commissioner are shared with the ISC by the Prime Minister when the matter of the reports is relevant for the Committee statutory competences[467]. Finally the Committee can ask the IPC to perform an investigation and the Commissioner must inform the ISC of the decision as to whether to carry out such investigation[468].

(253) The ISC also provided input on the draft IPA 2016, which resulted in a number of amendments that are now reflected in the IPA 2016[469]. In particular, the ISC recommended the strengthening of privacy protections by introducing a set of privacy protections which apply across the full range of investigatory powers[470]. It

---

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) to the JSA 2013).

463 UK Explanatory Framework for Adequacy Discussions, section H: National Security, page 43, see footnote 29.

464 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.

465 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://isc.independent.gov.uk/wp-content/uploads/2021/01/20150312_ISC_PSRptweb.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

466 Section 142, 161 and 183 of the IPA 2016.

467 Section 234 of the IPA 2016.

468 Section 236 of the IPA 2016.

469 Intelligence and Security Committee of Parliament, Report on the draft Investigatory Powers Bill, available at the following link: https://b1cba9b3-a-5e6631fd-s-sites.googlegroups.com/a/independent.gov.uk/isc/files/20160209_ISC_Rpt_IPBill%28web%29.pdf?attachauth=ANoY7cq4ZF2T1LVap6nKWsK7tegidCSUBJUw4GtGobxeP0tXmmoVsSDfYOlUIcPirsLDT_d69YiMBDKW8hZp2N5zEHnE2qt6eRiZF-Hai2Ax-EnljLI547akzgQ6x_J0kdI7qAhvrXGdmftSv42qZXx_TG2n5_rviU4vBey9xkhwm2hjJpbAXkZf_RgAuUkto2gxONghU1v64vBwL-FqlLXywsy0rSR2KLdMeWxbiE_4xCZIdTjOHg8r7cryb5dMajK0ayu-bIF_&attredirects=2

470 These general duties in relation to privacy are now set out in Section 2(2) of the IPA 2016, which provides that a public authority acting under the IPA 2016 must have regard to whether what is sought to be achieved by the warrant, authorisation or notice could reasonably be achieved by other less intrusive means, whether the level of protection to be applied in relation to any obtaining of information by virtue of the warrant, authorisation or notice is higher because of the particular sensitivity of that

also suggested changes to the proposed capabilities concerning Equipment Interference, BPD and Communications Data, and requested other specific amendments to strengthen the limitations and safeguards for the use of investigatory powers[471].

*3.3.4 Redress*

(254) In the field of government access for national security purposes, data subjects must have the possibility of bringing legal action before an independent and impartial court in order to have access to their personal data, or to obtain the rectification or erasure of such data[472]. Such a judicial body must notably have the power to adopt binding decisions on the intelligence service[473]. In the United Kingdom, as explained in recitals (257) to , a number of judicial redress avenues provide data subjects with the possibility to pursue and obtain such legal remedies. .

3.3.4.1 Redress mechanisms available under Part 4 of the DPA

(255) Under Section 165 of the DPA 2018, 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 4 of the DPA 2018. The Information Commissioner has the power to assess the compliance of the controller and processor with the DPA 2018, require them to take necessary steps. 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[474], to object to processing[475] and to rectification or erasure[476].

(256) 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[477]. Damage includes both financial loss and damage not involving financial loss, such as distress[478].

3.3.4.2 Redress mechanisms available under the IPA 2016

(257) Individuals can obtain redress for violations of the IPA 2016 before the Investigatory Powers Tribunal.



information, the public interest in the integrity and security of telecommunication systems and postal services, and any other aspects of the public interest in the protection of privacy.

471 For example, further to the request of the ISC, the number of days an "urgent" warrant can be in place before the Judicial Commissioner has to approve it has been reduced from five to three working days, and the ISC was given the power to refer matters to the Investigatory Powers Commissioner for investigation.

472 *Schrems II*, paragraph 194.

473 *Schrems II*, paragraph 197.

474 Section 94(11) of the DPA 2018.

475 Section 99(4) of the DPA 2018.

476 Section 100(1) of the DPA 2018.

477 Section 169 of the DPA 2018 allows claims from "A person who suffers damage by reason of a contravention of a requirement of the data protection legislation". According to the information provided by the UK authorities, in practice, a claim or complaint against the intelligence services is likely to be made to the Investigatory Powers Tribunal, who has a broad jurisdiction, is capable of awarding compensation/damages and where bringing a claim does not involve any costs.

478 Section 169(5) of the DPA 2018.

(258) The Investigatory Powers Tribunal is established by the RIPA 2000 and is independent from the executive[479]. In accordance with Section 65 of the RIPA 2000, the members of that Tribunal are appointed by Her Majesty for a period of five years. A member of that Tribunal may be removed from office by Her Majesty on an Address[480] by both Houses of Parliament[481].

(259) Under Section 65 of the RIPA 2000 the Tribunal is the appropriate judicial body for any complaint by a person aggrieved by conduct under the IPA 2016, RIPA 2000 or any conduct of the intelligence services[482].

(260) To bring an action before the Investigatory Powers Tribunal ("standing requirement"), according to Section 65 of the RIPA 2000 an individual has to believe[483] 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"[484]. In addition, the complainant is required to believe that the conduct has taken place in "challengeable circumstances"[485] or "to have been carried out by or on behalf of the intelligence services[486]. As in particular this "belief" standard has been

479 Under Schedule 3 to the RIPA 2000, the members must have specified judicial experience and are eligible for reappointment.

480 An "Address" is a motion laid before Parliament which seeks to make the Monarch aware of Parliament's opinions on a particular issue.

481 Schedule 3 paragraph 1(5) to the RIPA 2000.

482 Section 65(5) to the RIPA 2000.

483 On the standard of the "belief" test see case *Human Rights Watch v Secretary of State* [2016] UKIPTrib15_165-CH, paragraph 41. In this case, the Investigatory Powers Tribunal, by referring to the European Court of Human Rights case law, held that the appropriate test is whether in respect of the asserted 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, there is any basis for such belief, such that the 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.

484 Section 65(4)(a) of the RIPA 2000.

485 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).

486 According to the information provided by UK 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 Investigatory Powers Tribunal specifies that in 2016 the Tribunal received 209 complaints, 52% of those were considered frivolous or vexatious and 25% received a "no determination" outcome. UK 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

interpreted quite broadly[487], bringing a case before that Tribunal is subject to low standing requirements.

(261) Where the Investigatory Powers 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[488]. Where that 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[489]. In addition, the addressees of the warrants or notices under the IPA 2016, and every other person holding office under the Crown, employed by the police force or the Police Investigations and Review Commissioner have the duty to disclose or provide to that Tribunal all such documents and information as the Tribunal may require for the purpose of enabling them to exercise their jurisdiction[490].

(262) The Investigatory Powers Tribunal must give notice to the complainant whether there has been determination in his or her favour or not[491]. 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. This may include an order quashing or cancelling any warrant or authorisation and an order requiring the destruction of any records of information obtained in exercise of any power conferred by a warrant, authorization or a notice, or otherwise held by any public authority in relation to any person[492]. 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.

(263) Finally, it is worth noting that the role of the Investigatory Powers Tribunal has been discussed in the context of legal actions before the European Court for Human Rights in several occasions, notably in the case of *Kennedy v. the United Kingdom*[493] and more recently in the case *Big Brother Watch and others v. United Kingdom*[494] where the Court declared that "as a general rule the IPT has shown itself to be a remedy,

---

487 See case *Human Rights Watch v Secretary of State* [2016] UKIPTrib15_165-CH. In this case, the Investigatory Powers Tribunal, by referring to the European Court of Human Rights 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).

488 Section 67(3) of the RIPA 2000.

489 Section 67(2) of the RIPA 2000.

490 Section 68(6) – (7) of the RIPA 2000.

491 Section 68(4) of the RIPA 2000.

492 An example of the application of those powers is the case in *Liberty & Others vs. the Security Service, SIS, GCHQ*, [2015] UKIP Trib 13_77-H_2. The Tribunal made determination in favour of two complainants because their communication, in one case, was retained beyond the limits established and, in the other, because the procedure on examination was not followed as laid down in GCHQ internal rules. In the first case the Court ordered the intelligence services to destroy the communications that were retained for longer than the relevant time limit. In the second case, a destruction order was not issued because the communication was not retained.

493 *Kennedy*, see footnote 135.

494 European Court of Human Rights, *Big Brother Watch and others v United Kingdom,* Applications nos. 58170/13, 62322/14 and 24960/15 (*"Big Brother Watch and others"*).

available in theory and practice, which is capable of offering redress to applicants complaining of both specific incidences of surveillance and the general Convention compliance of surveillance regimes"[495].

3.3.4.3 Other available redress mechanisms

(264) As explained in see recitals (109) to (111), means of redress under the Human Rights Act 1998 and European Court of Human Rights are also available in the area of national security. Section 65(2) of RIPA 2000 provides the Investigatory Powers Tribunal with exclusive jurisdiction for all Human Rights Act's claims in relation to the intelligence agencies[496]. 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 Tribunal 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 Tribunal is in principle amenable to judicial review: see R (Privacy International) v Investigatory Powers Tribunal [2019] UKSC 22; [2019] 2 WLR 1219"[497].

(265) It follows from the above that when UK law enforcement or national security authorities access personal data falling within the scope of this Decision, such access is governed by laws that set the conditions under which access can take place and ensures that access and further use of the data is limited to what is necessary and proportionate to the law enforcement or national security objective pursued. Moreover, such access is subject in most instances to prior authorisation by a judicial body, through the approval of a warrant or a production order, and in any case to independent oversight. Once data has been accessed by public authorities, its processing, including further sharing and onward transfer, is subject to specific data protection safeguards under Part 3 the DPA 2018, reflecting those provided by Directive (EU) 2016/680, for processing by law enforcement authorities and Part 4 of the DPA 2018 for processing by intelligence agencies. Finally, data subjects enjoy in this area effective administrative and judicial redress rights, including to obtain access to their data or rectification or erasure of such data.

## 4. CONCLUSION

(266) The Commission considers that the UK GDPR and the DPA 2018 ensure a level of protection for personal data transferred from the European Union that is essentially equivalent to the one guaranteed by Regulation (EU) 2016/679.

(267) 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 punished 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.

(268) 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

---

495 European Court of Human Rights, *Big Brother Watch*, paragraph 265.

496 In Belhaj & others [2017] UKSC 3 the determination of unlawfulness of the interception of legally privileged material was based directly on Article 8 of the ECHR (see determination 11).

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

the individuals whose personal data are transferred from the European Union to the United Kingdom by United Kingdom public authorities for public interest purposes, in particular law enforcement and national security purposes, will be limited to what is strictly necessary to achieve the legitimate objective in question, and that effective legal protection against such interference exists.

(269) Therefore, in the light of the findings of this Decision, it should be decided that the UK ensures an adequate level of protection within the meaning of Article 45 of Regulation (EU) 2016/679, interpreted in light of the Charter of Fundamental Rights of the European Union.

(270) This conclusion is based on both the relevant UK 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**.**

## 5. EFFECTS OF THIS DECISION AND ACTION OF DATA PROTECTION AUTHORITIES

(271) 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.

(272) Consequently, a Commission adequacy decision adopted pursuant to Article 45(3) of Regulation (EU) 2016/679 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 European Union to controllers or processors in the United Kingdom may take place without the need to obtain any further authorisation.

(273) It should be recalled that, pursuant to Article 58(5) of Regulation (EU) 2016/679 and as explained by the Court of Justice in the *Schrems* judgment[498], 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[499].

## 6. MONITORING, SUSPENSION, REPEAL OR AMENDMENT OF THIS DECISION

(274) Pursuant to Article 45(4) of Regulation (EU) 2016/679, 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 particularly important in this case,

498 *Schrems*, paragraph 65.

499 *Schrems*, paragraph 65: "It is incumbent upon the national legislature to provide for legal remedies enabling the national supervisory authority concerned to put forward the objections which it considers well founded before the national courts in order for them, if they share its doubts as to the validity of the Commission decision, to make a reference for a preliminary ruling for the purpose of examination of the decision's validity".

as the United Kingdom will administer, apply and enforce a new data protection regime no longer subject to European Union law and which may be liable to evolve.

(275) To this end, the United Kingdom authorities are invited to inform the Commission of any material change to the UK 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.

(276) 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 controllers or processors in the UK. 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, or for national security including any oversight bodies, do not ensure the required level of protection.

(277) Where available information, in particular information resulting from the monitoring of this Decision or provided by UK or Member States' authorities, reveals that the level of protection afforded by the UK may no longer be adequate, the Commission should inform the competent UK authorities thereof and request that appropriate measures be taken within a specified, reasonable timeframe.

(278) If, at the expiry of that specified timeframe, the competent United Kingdom authorities fail to take those measure 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 93(2) of Regulation (EU) 2016/679 with a view to partially or completely suspend or repeal this Decision.

(279) 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.

(280) 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 93(3) of Regulation (EU) 2016/679, immediately applicable implementing acts suspending, repealing or amending the Decision

## 7. DURATION AND RENEWAL OF THIS DECISION

(281) The Commission must take into account that, with the end of the transition period provided by the Withdrawal Agreement and as soon as the interim provision under Article FINPROV.10A 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 EU law. This may notably involve amendments or changes to the data protection framework assessed in this Decision, as well as other relevant developments.

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

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 UK 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 93(2) of Regulation (EU) 2016/679.

## 8. FINAL CONSIDERATIONS

(283) The European Data Protection Board published its opinion[500], which has been taken into consideration in the preparation of this Decision.

(284) The European Parliament has adopted […]

(285) The measures provided for in this Decision are in accordance with the opinion of the Committee established under Article 93 of Regulation (EU) 2016/679,

HAS ADOPTED THIS DECISION:

*Article 1*

For the purposes of Article 45 of Regulation (EU) 2016/679, the United Kingdom ensures an adequate level of protection for personal data transferred within the scope of Regulation (EU) 2016/679 from the European Union to the United Kingdom.

*Article 2*

Whenever the competent authorities in Member States, in order to protect individuals with regard to the processing of their personal data, exercise their powers pursuant to Article 58 of Regulation (EU) 2016/679 with respect to data transfers falling 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, 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.

[500] [add reference when opinion will be issued].

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

*Article 4*

This Decision shall expire on XXX [set date - *four years after the date of entry into force*], unless extended in accordance with the procedure referred to in Article 93(2) of Regulation (EU) 2016/679.

*Article 5*

This Decision is addressed to the Member States.

Done at Brussels,

*For the Commission*
*[…]*
*Member of the Commission*