Key	
Purple additions	Changes in No.1 Bill that remain
Green additions	New changes in No.2 Bill
Teal references	Reference to affected provision in No.2 Bill as first published

Note – some provisions of the Government Bill amend provisions that are later omitted. In these circumstances, we have not shown the amendments subsequently omitted.

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 (United Kingdom General Data Protection Regulation) (Text with EEA relevance) (Retained EU Legislation)
Preamble

[No Changes to The Recitals]

Chapter 1 General Provisions

Article 1 Subject-matter and objectives

1.

This Regulation lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data.

2.

This Regulation protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data.

Article 2 Material scope

1.

This Regulation applies to the automated or structured processing of personal data, including—

(a) processing in the course of an activity which, immediately before IP completion day, fell outside the scope of EU law, and

(b) processing in the course of an activity which, immediately before IP completion day, fell within the scope of Chapter 2 of Title 5 of the Treaty on European Union (common foreign and security policy activities).

1A.

This Regulation also applies to the manual unstructured processing of personal data held by an FOI public authority.

2.

This Regulation does not apply to—

(a) the processing of personal data by an individual in the course of a purely personal or household activity;

(b) the processing of personal data by a competent authority for any of the law enforcement purposes (see Part 3 of the 2018 Act);

(c) the processing of personal data to which Part 4 of the 2018 Act (intelligence services processing) applies.

4.

This Regulation shall be without prejudice to the application of the Electronic Commerce (EC Directive) Regulations 2002, in particular the provisions about mere conduits, caching and hosting (see regulations 17 to 19 of those Regulations).

5.

In this Article—

(a) *'the automated or structured processing of personal data'* means—

(i) the processing of personal data wholly or partly by automated means, and

(ii) the processing otherwise than by automated means of personal data which forms part of a filing system or is intended to form part of a filing system;

(b) *'the manual unstructured processing of personal data'* means the processing of personal data which is not the automated or structured processing of personal data;

(c) *'FOI public authority'* has the same meaning as in Chapter 3 of Part 2 of the 2018 Act (see section 21(5) of that Act);

(d) references to personal data *'held'* by an FOI public authority are to be interpreted in accordance with section 21(6) and (7) of the 2018 Act;

(e) *'competent authority'* and *'law enforcement purposes'* have the same meaning as in Part 3 of the 2018 Act (see sections 30 and 31 of that Act).

Article 3 Territorial scope

1.

This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the United Kingdom, regardless of whether the processing takes place in the United Kingdom or not.

2.

This Regulation applies to the relevant processing of personal data of data subjects who are in the United Kingdom by a controller or processor not established in the United Kingdom, where the processing activities are related to:

(a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the United Kingdom; or

(b) the monitoring of their behaviour as far as their behaviour takes place within the United Kingdom.

2A.

In paragraph 2, *"relevant processing of personal data"* means processing to which this Regulation applies, other than processing described in Article 2(1)(a) or (b) or (1A).

3.

This Regulation applies to the processing of personal data by a controller not established in the United Kingdom, but in a place where domestic law applies by virtue of public international law.

Article 4 Definitions

For the purposes of this Regulation:

1. [s. 1(3)(a)]

(A1) *'the 2018 Act'* means the Data Protection Act 2018;

(A2) *'domestic law'* means the law of the United Kingdom or of a part of the United Kingdom;

(A3) *'the Commissioner'* means the Information Commissioner (see section 114 of the 2018 Act);

(A4) "*the data protection legislation*" has the same meaning as in the 2018 Act (see section 3(9) of that Act); [sch 9. para 2(2)]

(1) *'personal data'* means any information relating to an identified or identifiable living individual ~~natural person~~ ('data subject'); an identifiable living individual ~~natural person~~ is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the individual ~~that natural person~~ (and see paragraph 2); [s. 1(3)(b)]

(1A) an individual is identifiable from information "directly" if the individual can be identified without the use of additional information;

(1B) an individual is identifiable from information "indirectly" if the individual can be identified only with the use of additional information; [s. 1(3)(c)]

(2) *'processing' means* any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

(3) *'restriction of processing' means* the marking of stored personal data with the aim of limiting their processing in the future;

(4) *'profiling' means* any form of automated processing of personal data consisting of the use of

personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;

(5) *'pseudonymisation' means* the processing of personal data in such a manner that it becomes information relating to a living individual who is only indirectly identifiable; but personal data is only pseudonymised if the additional information needed to identify the individual is kept separately and is subject to technical and organisational measures to ensure that the personal data is not information relating to an identified or directly identifiable living individual; ~~the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;~~ [s. 1(3)(d)]

(6) *'filing system' means* any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis;

(7) *'controller'* means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data (but see section 6 of the 2018 Act);

(8) *'processor'* means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;

(9) *'recipient'* means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with domestic law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing;

(10) *'third party'* means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data;

(10A) *'public authority'* and *'public body'* are to be interpreted in accordance with section 7 of the 2018 Act and provision made under that section;

(11) *'consent'* of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her (and see paragraphs 7 and 8 of this Article); [s. 3(2)]

(11A) "senior responsible individual" means an individual designated as the senior responsible individual of a controller or processor under Article 27A; [sch. 4 para 2]

(12) *'personal data breach'* means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;

(13) *'genetic data'* means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question;

(14) *'biometric data' means* personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data;

(15) *'data concerning health' means* personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status;

(15A) "direct marketing" means the communication (by whatever means) of advertising and marketing material which is directed to particular individuals; [sch 9. para 2(3)]

~~(17) *'representative'* means a natural or legal person established in the United Kingdom who, designated by the controller or processor in writing pursuant to Article 27, represents the controller or processor with regard to their respective obligations under this Regulation;~~ [s. 13(2)(a)]

(18) *'enterprise' means* a natural or legal person engaged in an economic activity, irrespective of its legal form, including partnerships or associations regularly engaged in an economic activity;

(19) *'group of undertakings' means* a controlling undertaking and its controlled undertakings;

(20) *'binding corporate rules'* means personal data protection policies which are adhered to by a controller or processor established in the United Kingdom for transfers or a set of transfers of personal data to a controller or processor in one or more third countries within a group of undertakings, or group of enterprises engaged in a joint economic activity;

(21A) *'foreign designated authority'* means an authority designated for the purposes of Article 13 of the Data Protection Convention (as defined in section 3 of the 2018 Act) by a party, other than the United Kingdom, which is bound by that Convention;

(25) *'information society service' means* a service as defined in point (b) of Article 1(1) of Directive (EU) 2015/1535 of the European Parliament and of the Council as it has effect immediately before IP completion day;

(26) *'international organisation' means* an organisation and its subordinate bodies governed by public international law, or any other body which is set up by, or on the basis of, an agreement between two or more countries;

(27) *'third country' means* a country or territory outside the United Kingdom;

(28) references to a *fundamental right* or *fundamental freedom* (however expressed) are to a fundamental right or fundamental freedom which continues to form part of domestic law on and after IP completion day by virtue of section 4 of the European Union (Withdrawal) Act 2018 , as the right or freedom is amended or otherwise modified by domestic law from time to time on or after IP completion day.

(29) "enactment" has the same meaning as in the 2018 Act (see section 205 of that Act);

(30) "tribunal" means any tribunal in which legal proceedings may be brought. [sch 9. para 2(4)]

2.

Section 3A of the 2018 Act (information relating to an identifiable living individual) applies for the purposes of

this Regulation as it applies for the purposes of that Act (and, as so applied, the references in that section to section 3(3) of that Act are to be read as references to Article 4(1)(1) of this Regulation). [s. 1(3)(e)]

3.

References in this Regulation to the processing of personal data for the purposes of scientific research (including references to processing for "scientific research purposes") are references to processing for the purposes of any research that can reasonably be described as scientific, whether publicly or privately funded, and whether carried out as a commercial or non-commercial activity.

4.

Such references

(a) include processing for the purposes of technological development or demonstration, fundamental research or applied research, so far as those activities can reasonably be described as scientific, but
(b) only include processing for the purposes of a study in the area of public health that can reasonably be described as scientific where the study is conducted in the public interest.

5.

References in this Regulation to the processing of personal data for the purposes of historical research (including references to processing for "historical research purposes") include processing for the purposes of genealogical research.

6.

References in this Regulation to the processing of personal data for statistical purposes are references to processing for statistical surveys or for the production of statistical results where—

(a) the information that results from the processing is aggregate data that is not personal data, and
(b) the controller does not use the personal data processed, or the information that results from the processing, in support of measures or decisions with respect to a particular data subject to whom the personal data relates.

[s. 2]

7.

A data subject's consent is to be treated as falling within the definition of "consent" in point (11) of paragraph 1 if—

(a) it does not fall within that definition because (and only because) the consent is given to the processing of personal data for the purposes of an area of scientific research,
(b) at the time the consent is sought, it is not possible to identify fully the purposes for which personal data is to be processed,
(c) seeking consent in relation to the area of scientific research is consistent with generally recognised ethical standards relevant to the area of research, and
(d) so far as the intended purposes of the processing allow, the data subject is given the opportunity to consent only to processing for part of the research.

8.

References in this Regulation to consent given for a specific purpose (however expressed) include consent described in paragraph 7. [s. 3(3)]

Chapter 2 Principles

Article 5 Principles relating to processing of personal data

1.

Personal data shall be:

(a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');

(b) collected (whether from the data subject or otherwise) for specified, explicit and legitimate purposes and not further processed by or on behalf of a controller in a manner that is incompatible with the purposes for which the controller collected the data ~~those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes~~ ('purpose limitation'); [s. 6(2)]

(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');

(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 84B ~~Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject~~ ('storage limitation'); [s. 23(1)(a)]

(f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

2.

The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability').

3.

For the avoidance of doubt, processing is not lawful by virtue only of being processing in a manner that is compatible with the purposes for which the personal data was collected. [s. 6(3)]

Article 6 Lawfulness of processing

1.

Processing shall be lawful only if and to the extent that at least one of the following applies:

(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 of the controller carried out in the public interest or a task carried out in the exercise of official authority vested in the controller; [s. 5(2)(a)]

(ea) processing is necessary for the purposes of a recognised legitimate interest; [s. 5(2)(b)]

(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.

Points (ea) and (f) of the first subparagraph shall not apply to processing carried out by public authorities in the performance of their tasks. [s. 5(2)(a)]

3.

The basis for the processing referred to in point (c) and (e) of paragraph 1 shall be laid down by domestic law.

The purpose of the processing shall be determined in that legal basis or, as regards the processing referred to in point (e) of paragraph 1, shall be necessary for the performance of a task of the controller carried out in the public interest or a task carried out in the exercise of official authority vested in the controller. That legal basis may contain specific provisions to adapt the application of rules of this Regulation, inter alia: the general conditions governing the lawfulness of processing by the controller; the types of data which are subject to the processing; the data subjects concerned; the entities to, and the purposes for which, the personal data may be disclosed; the purpose limitation; storage periods; and processing operations and processing procedures, including measures to ensure lawful and fair processing such as those for other specific processing situations as provided for in Chapter IX. The domestic law shall meet an objective of public interest and be proportionate to the legitimate aim pursued. [s. 5(3)]

~~4.~~

~~Where the processing for a purpose other than that for which the personal data have been collected is not based on the data subject's consent or on domestic law which constitutes a necessary and proportionate measure in a democratic society to safeguard national security, defence or any of the objectives referred to in Article 23(1), the controller shall, in order to ascertain whether processing for another purpose is compatible with the purpose for which the personal data are initially collected, take into account, inter alia:~~

~~(a) any link between the purposes for which the personal data have been collected and the purposes of the intended further processing;~~

~~(b) the context in which the personal data have been collected, in particular regarding the relationship between data subjects and the controller;~~

~~(c) the nature of the personal data, in particular whether special categories of personal data are processed, pursuant to Article 9, or whether personal data related to criminal convictions and offences are processed, pursuant to Article 10;~~

~~(d) the possible consequences of the intended further processing for data subjects;~~

~~(e) the existence of appropriate safeguards, which may include encryption or pseudonymisation.~~ [s. 6(4)]

5.

For the purposes of paragraph 1(ea), processing is necessary for the purposes of a recognised legitimate interest only if it meets a condition in Annex 1.

6.

The Secretary of State may by regulations amend Annex 1 by—

(a) adding or varying provisions, or

(b) omitting provisions added by regulations made under this paragraph.

7.

The Secretary of State may only make regulations under paragraph 6 where the Secretary of State considers it appropriate to do so having regard to, among other things—

(a) the interests and fundamental rights and freedoms of data subjects which require protection of personal data, and

(b) where relevant, the need to provide children with special protection with regard to their personal data.

8.

Regulations under paragraph 6 are subject to the affirmative resolution procedure.

9.

For the purposes of paragraph 1(f), examples of types of processing that may be processing that is necessary for the purposes of a legitimate interest include

(a) processing that is necessary for the purposes of direct marketing,
(b) intra-group transmission of personal data (whether relating to clients, employees or other individuals) where that is necessary for internal administrative purposes, and
(c) processing that is necessary for the purposes of ensuring the security of network and information systems.

10.

In paragraph 9—

"intra-group transmission" means transmission between members of a group of undertakings or between members of a group of institutions affiliated to a central body;

"security of network and information systems" has the same meaning as in the Network and Information

Systems Regulations 2018 (S.I. 2018/506) (see regulation 1(3)(g)). [s. 5(4)]

Article 7 Conditions for consent

1.

Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data.

2.

If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. Any part of such a declaration which constitutes an infringement of this Regulation shall not be binding.

3.

The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent.

4.

When assessing whether consent is freely given, utmost account shall be taken of whether, *inter alia* , the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.

Article 8 Conditions applicable to child's consent in relation to information society services

1.

Where point (a) of Article 6(1) applies, in relation to the offer of information society services directly to a child, the processing of the personal data of a child shall be lawful where the child is at least 13 years old. Where the child is below the age of 13 years, such processing shall be lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility over the child.

2.

The controller shall make reasonable efforts to verify in such cases that consent is given or authorised by the holder of parental responsibility over the child, taking into consideration available technology.

3.

Paragraph 1 shall not affect the general contract law as it operates in domestic law such as the rules on the validity, formation or effect of a contract in relation to a child.

4.

In paragraph 1, the reference to information society services does not include preventive or counselling services.

Article 8A Purpose limitation: further processing

1.

This Article is about the determination, for the purposes of Article 5(1)(b) (purpose limitation), of whether processing of personal data by or on behalf of a controller for a purpose (a "new purpose") other than the purpose for which the controller collected the data ("the original purpose") is processing in a manner compatible

with the original purpose.

2.

In making the determination, a person must take into account, among other things—

(a) any link between the original purpose and the new purpose;

(b) the context in which the personal data was collected, including the relationship between the data subject and the controller;

(c) the nature of the personal data, including whether it is a special category of personal data (see Article 9) or personal data related to criminal convictions and offences (see Article 10);

(d) the possible consequences of the intended processing for data subjects;

(e) the existence of appropriate safeguards (for example, encryption or pseudonymisation).

3.

Processing of personal data for a new purpose is to be treated as processing in a manner compatible with the original purpose where—

(a) the data subject consents to the processing of personal data for the new purpose and the new purpose is specified, explicit and legitimate,

(b) the processing is carried out in accordance with Article 84B—

(i) for the purposes of scientific research or historical research,

(ii) for the purposes of archiving in the public interest, or

(iii) for statistical purposes,

(c) the processing is carried out for the purposes of ensuring that processing of personal data complies with Article 5(1) or demonstrating that it does so,

(d) the processing meets a condition in Annex 2, or

(e) the processing is necessary to safeguard an objective listed in Article 23(1)(c) to (j) and is authorised by an enactment or rule of law.

4.

Where the controller collected the personal data based on Article 6(1)(a) (data subject's consent), processing for a new purpose is only processing in a manner compatible with the original purpose if—

(a) it falls within paragraph 3(a) or (c), or

(b) it falls within paragraph 3(d) or (e) and the controller cannot reasonably be expected to obtain the data subject's consent.

5.

The Secretary of State may by regulations amend Annex 2 by—

(a) adding or varying provisions, or

(b) omitting provisions added by regulations made under this paragraph.

6.

The Secretary of State may only make regulations under paragraph 5 adding a case to Annex 2 where the Secretary of State considers that processing in that case is necessary to safeguard an objective listed in Article 23(1)(c) to (j).

7.

Regulations under paragraph 5 may make provision identifying processing by any means, including by reference to the controller, the data subject, the personal data or the provision of Article 6(1) relied on for the purposes of the processing.

8.

Regulations under paragraph 5 are subject to the affirmative resolution procedure. [s. 6(5)]

Article 9 Processing of special categories of personal data

1.

Processing of personal data 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 shall be prohibited.

2.

Paragraph 1 shall not apply if the processing is based on Article 6(1) and one of the following applies: [sch 9. para 3(a)]

(a) the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where domestic law provides that the prohibition referred to in paragraph 1 may not be lifted by the data subject;

(b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by domestic law or a collective agreement pursuant to domestic law providing for

appropriate safeguards for the fundamental rights and the interests of the data subject;

(c) processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;

(d) processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that 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 that the personal data are not disclosed outside that body without the consent of the data subjects;

(e) processing relates to personal data which are manifestly made public by the data subject;

(f) processing is necessary for the establishment, exercise or defence of legal claims or whenever courts or tribunals are acting in their judicial capacity; [sch 9. para 3(b)]

(g) processing is necessary for reasons of substantial public interest, on the basis of domestic law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;

(h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of domestic law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3;

(i) processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of domestic law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;

(j) processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, is carried out in accordance with Article 84B and is ~~in accordance with Article 89(1) (as supplemented by section 19 of the 2018 Act)~~ based on domestic law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

[s. 23(1)(b)]

3.

~~Personal data referred to in paragraph 1 may be processed for the purposes referred to in point (h) of paragraph 2 when those data are~~ Paragraph 1 is only disapplied by point (h) of paragraph 2 is the personal data is processed by or under the responsibility of a professional subject to the obligation of professional secrecy under domestic law or rules established by national competent bodies or by another person also subject to an obligation of secrecy under domestic law or rules established by national competent bodies.

[sch 9. para 3(c)]

3A.

In paragraph 3, *'national competent bodies'* means competent bodies of the United Kingdom or a part of the United Kingdom.

5.—

In the 2018 Act—

(a) section 10 makes provision about when the requirement in paragraph 2(b), (g), (h), (i) or (j) of this Article for authorisation by, or a basis in, domestic law is met;

(b) section 11(1) makes provision about when the processing of personal data is carried out in circumstances described in paragraph 3 of this Article.

Article 10 Processing of personal data relating to criminal convictions and offences

1.

Processing of personal data relating to criminal convictions and offences or related security measures based on Article 6(1) shall be carried out 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. Any comprehensive register of criminal convictions shall be kept only under the control of official authority.

2.

In the 2018 Act—

(a) section 10 makes provision about when the requirement in paragraph 1 of this Article for authorisation by domestic law is met;

(b) section 11(2) makes provision about the meaning of *"personal data relating to criminal convictions and offences or related security measures"*.

Article 11 Processing which does not require identification

1.

If the purposes for which a controller processes personal data do not or do no longer require the identification of a data subject by the controller, the controller shall not be obliged to maintain, acquire or process additional information in order to identify the data subject for the sole purpose of complying with this Regulation.

2.

Where, in cases referred to in paragraph 1 of this Article, the controller is able to demonstrate that it is not in a position to identify the data subject, the controller shall inform the data subject accordingly, if possible. In such cases, Articles 15 to 20 shall not apply except where the data subject, for the purpose of exercising his or her rights under those articles, provides additional information enabling his or her identification.

Chapter 3 Rights of the Data Subject

S1 Transparency and Modalities

Article 12 Transparent information, communication and modalities for the exercise of the rights of the data subject

1.

The controller shall take appropriate measures to provide any information referred to in Articles 13 and 14 and any communication made under or by virtue of Articles 15 to 22D and 34 relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child. The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. When requested by the data subject, the

information may be provided orally, provided that the identity of the data subject is proven by other means. [sch. 3 para 2(2)]

2.

The controller shall facilitate the exercise of data subject rights under Articles 15 to 22D. In the cases referred to in Article 11(2), the controller shall not refuse to act on the request of the data subject for exercising his or her rights under Articles 15 to 22D unless the controller demonstrates that it is not in a position to identify the data subject (or refusal is allowed under Article 12A). [sch. 3 para 2(3) and s. 7(2)(a)]

3.

The controller shall provide information on action taken on a request made under or by virtue of Articles 15 to 22D to the data subject without undue delay and in any event before the end of the applicable time period (see Article 12B) ~~within one month of receipt of the request~~. That period may be extended by two further months where necessary, taking into account the complexity and number of the requests. The controller shall inform the data subject of any such extension within one month of receipt of the request, together with the reasons for the delay. Where the data subject makes the request by electronic form means, the information shall be provided by electronic means where possible, unless otherwise requested by the data subject.
[sch. 3 para 2(4) and s. 8(2)(a)]

4.

If the controller does not take action on the request of the data subject, the controller shall inform the data subject without undue delay and in any event before the end of the applicable time period (see Article 12B) ~~at the latest within one month of receipt of the request~~ of the reasons for not taking action and on the possibility of making a complaint to the controller under section 164A of the 2018 Act, making a complaint to the Commissioner under section 165 of that Act ~~lodging a complaint with the Commissioner~~ and seeking a judicial remedy. [s. 8(2)(b) and sch. 8 para 2]

5.

Subject to Article 15(3), information provided under Articles 13 and 14 and any communication and any actions taken or by virtue of Articles 15 to 22D and 34 shall be provided free of charge. ~~Where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character, the controller may either:~~ [sch 9. para 4 and sch. 3 s2(5)]

~~(a) charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested; or~~

~~(b) refuse to act on the request.~~

~~The controller shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request.~~ [s. 7(2)(b)]

6.

Without prejudice to Article 11, where the controller has reasonable doubts concerning the identity of the natural person making the request referred to in Articles 15 to 21, the controller may —

(a) request the provision of additional information necessary to confirm the identity of the data subject; and

(b) delay dealing with the request until the identity is confirmed. [s. 8(2)(c)]

6A.

The Commissioner may publish (and amend or withdraw)—

(a) standardised icons for use in combination with information provided to data subjects under Articles 13 and 14;

(b) a notice stating that other persons may publish (and amend or withdraw) such icons, provided that the icons satisfy requirements specified in the notice as to the information to be presented by the icons and the procedures for providing the icons.

6B.

The Commissioner must not publish icons or a notice under paragraph 6A unless satisfied (as appropriate) that the icons give a meaningful overview of the intended processing in an easily visible, intelligible and clearly legible manner or that the notice will result in icons that do so.

7.

If standardised icons are published as described in paragraph 6A (and not withdrawn), the information to be provided to data subjects pursuant to Articles 13 and 14 may be provided in combination with the icons. Where the icons are presented electronically they shall be machine-readable.

Article 12A Vexatious or excessive requests

1.

Paragraph 2 applies where a request made by a data subject under or by virtue of Articles 15 to 22D or 34 is vexatious or excessive. [sch. 3 para 3 and s.7(3)]

2.

The controller may—

(a) charge a reasonable fee for dealing with the request (see section 12 of the 2018 Act), or

(b) refuse to act on the request.

3.

In any proceedings where there is an issue as to whether a request is vexatious or excessive, it is for the controller to show that it is.

4.

Whether a request is vexatious or excessive must be determined having regard to the circumstances of the request, including (so far as relevant)—

(a) the nature of the request,

(b) the relationship between the data subject and the controller,

(c) the resources available to the controller,

(d) the extent to which the request repeats a previous request made by the data subject to the controller,

(e) how long ago any previous request was made, and

(f) whether the request overlaps with other requests made by the data subject to the controller.

5.

Examples of requests that may be vexatious include requests that—

(a) are intended to cause distress,

(b) are not made in good faith, or

(c) are an abuse of process. [s. 7(3)]

Article 12B Meaning of "applicable time period"

1.

In Article 12, "the applicable time period" means the period of one month beginning with the relevant time, subject to paragraph 3.

2.

"The relevant time" means the latest of the following—

(a) when the controller receives the request in question;

(b) when the controller receives the information (if any) requested in connection with a request under Article 12(6);

(c) when the fee (if any) charged in connection with the request under Article 12A is paid.

3.

The controller may, by giving notice to the data subject, extend the applicable time period by two further months where that is necessary by reason of—

(a) the complexity of requests made by the data subject, or

(b) the number of such requests.

4.

A notice under paragraph 3 must—

(a) be given before the end of the period of one month beginning with the relevant time, and

(b) state the reasons for the delay.

5.

Where the controller reasonably requires further information in order to identify the information or processing activities to which a request under Article 15 relates—

(a) the controller may ask the data subject to provide the further information, and

(b) the period beginning with the day on which the controller makes the request and ending with the day on which the controller receives the information does not count towards—

(i) the applicable time period, or

(ii) the period described in paragraph 4(a).

6.

An example of a case in which a controller may reasonably require further information is where the controller processes a large amount of information concerning the data subject. [s. 8(3)]

S2 Information and Access to Personal Data

Article 13 Information to be provided where personal data are collected from the data subject

1.

Where personal data relating to a data subject are collected from the data subject, the controller shall, at the time when personal data are obtained, provide the data subject with all of the following information:

(a) the identity and the contact details of the controller ~~and, where applicable, of the controller's representative;~~ [s. 13(2)(b)]

(b) the contact details of the senior responsible individual ~~data protection officer~~, where applicable; [sch. 4 para 3]

(c) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;

(d) where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller or by a third party;

(e) the recipients or categories of recipients of the personal data, if any;

(f) where applicable, the fact that the controller intends to transfer personal data to a third country or international organisation and the existence or absence of relevant regulations under Article 45A ~~adequacy regulations under section 17A of the 2018 Act~~, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1), the safeguards relied on ~~reference to the appropriate or suitable safeguards~~ and the means by which to obtain a copy of them or where they have been made available. [sch. 7 para 2]

2.

In addition to the information referred to in paragraph 1, the controller shall, at the time when personal data are obtained, provide the data subject with the following further information necessary to ensure fair and transparent processing:

(a) the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;

(b) the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability;

(c) where the processing is based on point (a) of Article 6(1) or point (a) of Article 9(2), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;

(ca) the right to make a complaint to the controller under section 164A of the 2018 Act;

(d) the right to make a complaint to the Commissioner under section 165 of the 2018 Act ~~lodge a complaint with the Commissioner~~; [sch. 8 para 3]

(e) whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data;

(f) the existence of automated decision-making, including profiling, which is subject to the requirement to provide safeguards under Article 22C ~~referred to in Article 22(1) and (4)~~ and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject. [sch. 3 para 4]

3.

Where the controller intends to further process the personal data for a purpose other than that for which the personal data were collected, the controller shall provide the data subject prior to that further processing with information on that other purpose and with any relevant further information as referred to in paragraph 2.

4.

Paragraphs 1, 2 and 3 do not apply to the extent that ~~shall not apply where and insofar as~~ the data subject already has the information. [s. 9(1)]

5.

Paragraph 3 does not apply to the extent that—

(a) the controller intends to further process the personal data—

(i) for (and only for) the purposes of scientific or historical research, the purposes of archiving in the public interest or statistical purposes, and

(ii) in accordance with Article 84B, and

(b) providing the information is impossible or would involve a disproportionate effort. [s. 9(1)]

6.

For the purposes of paragraph 5(b), whether providing information would involve a disproportionate effort depends on, among other things, the number of data subjects, the age of the personal data and any appropriate safeguards applied to the processing.

[s. 9(1)]

Article 14 Information to be provided where personal data have not been obtained from the data subject

1.

Where personal data have not been obtained from the data subject, the controller shall provide the data subject with the following information:

(a) the identity and the contact details of the controller ~~and, where applicable, of the controller's representative~~; [s. 13(2)(c)]

(b) the contact details of the senior responsible individual ~~data protection officer~~, where applicable; [sch. 4 para 4]

(c) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;

(d) the categories of personal data concerned;

(e) the recipients or categories of recipients of the personal data, if any;

(f) where applicable, that the controller intends to transfer personal data to a recipient in a third country or international organisation and the existence or absence of relevant regulations under Article 45A ~~adequacy regulations under section 17A of the 2018 Act~~, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1), the safeguards relied on ~~reference to the appropriate or suitable safeguards~~ and the means to obtain a copy of them or where they have been made available. [sch. 7 para 3]

2.

In addition to the information referred to in paragraph 1, the controller shall provide the data subject with the following information necessary to ensure fair and transparent processing in respect of the data subject:

(a) the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;

(b) where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller or by a third party;

(c) the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject and to object to processing as well as the right to data portability;

(d) where processing is based on point (a) of Article 6(1) or point (a) of Article 9(2), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;

(da) the right to make a complaint to the controller (see section 164A of the 2018 Act);

(e) the right to make a complaint to the Commissioner under section 165 of the 2018 Act ~~lodge a complaint with the Commissioner~~; [sch. 8 para 4]

(f) from which source the personal data originate, and if applicable, whether it came from publicly accessible sources;

(g) the existence of automated decision-making, including profiling, which is subject to the requirement to provide safeguards under Article 22C ~~referred to in Article 22(1) and (4)~~ and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject. [sch. 3 para 5]

3.

The controller shall provide the information referred to in paragraphs 1 and 2:

(a) within a reasonable period after obtaining the personal data, but at the latest within one month, having regard to the specific circumstances in which the personal data are processed;

(b) if the personal data are to be used for communication with the data subject, at the latest at the time of the first communication to that data subject; or

(c) if a disclosure to another recipient is envisaged, at the latest when the personal data are first disclosed.

4.

Where the controller intends to further process the personal data for a purpose other than that for which the personal data were obtained, the controller shall provide the data subject prior to that further processing with information on that other purpose and with any relevant further information as referred to in paragraph 2.

5.

Paragraphs 1 to 4 shall not apply do not apply to the extent that ~~shall not apply where and insofar as~~ :

(a) the data subject already has the information;

~~(b) the provision of such information proves impossible or would involve a disproportionate effort, in particular for processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to the conditions and safeguards referred to in Article 89(1) or in so far as the obligation referred to in paragraph 1 of this Article is likely to render impossible or seriously impair the~~

~~achievement of the objectives of that processing. In such cases the controller shall take appropriate measures to protect the data subject's rights and freedoms and legitimate interests, including making the information publicly available;~~

(c) obtaining or disclosure is expressly laid down by a provision of domestic law which provides appropriate measures to protect the data subject's legitimate interests; ~~or~~

(d) ~~where~~ the personal data must remain confidential subject to an obligation of professional secrecy regulated by domestic law, including a statutory obligation of secrecy;

(e) providing the information is impossible or would involve a disproportionate effort, or

(f) the obligation referred to in paragraph 1 is likely to render impossible or seriously impair the achievement of the objectives of the processing for which the personal data are intended. [s. 9(2)]

6.

For the purposes of paragraph 5(e), whether providing information would involve a disproportionate effort depends on, among other things, the number of data subjects, the age of the personal data and any appropriate safeguards applied to the processing.

[s. 9(2)]

7.

A controller relying on paragraph 5(e) or (f) must take appropriate measures to protect the data subject's rights, freedoms and legitimate interests, including by making the information available publicly.

[s. 9(2)]

Article 15 Right of access by the data subject

1.

The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information:

(a) the purposes of the processing;

(b) the categories of personal data concerned;

(c) the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;

(d) where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;

(e) the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;

(ea) the right to make a complaint to the controller under section 164A of the 2018 Act;

(f) the right to make a complaint to the Commissioner under section 165 of the 2018 Act ~~lodge a complaint with the Commissioner~~; [sch. 8 para 5]

(g) where the personal data are not collected from the data subject, any available information as to their source;

(h) the existence of automated decision-making, including profiling, which is subject to the requirement to provide safeguards under Article 22C ~~referred to in Article 22(1) and (4)~~ and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject. [sch. 3 para 6]

2.

Where personal data are transferred to a third country or to an international organisation in reliance on Article 46, the data subject shall have the right to be informed of the safeguards provided in accordance with Article 46(1A)(a)(i) or (b)(i) for the purposes of ~~appropriate safeguards pursuant to Article 46 relating to~~ the transfer. [sch. 7 para 4]

3.

The controller shall provide a copy of the personal data undergoing processing. For any further copies requested by the data subject, the controller may charge a reasonable fee based on administrative costs. Where the data subject makes the request by electronic means, and unless otherwise requested by the data subject, the information shall be provided in a commonly used electronic form.

4.

The right to obtain a copy referred to in paragraph 3 shall not adversely affect the rights and freedoms of others.

S3 Rectification and Erasure

Article 16 Right to rectification

The data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement.

Article 17 Right to erasure ('right to be forgotten')

1.

The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:

(a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;

(b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing;

(c) the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2);

(d) the personal data have been unlawfully processed;

(e) the personal data have to be erased for compliance with a legal obligation under domestic law;

(f) the personal data have been collected in relation to the offer of information society services referred to in Article 8(1).

2.

Where the controller has made the personal data public and is obliged pursuant to paragraph 1 to erase the personal data, the controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data.

3.

Paragraphs 1 and 2 shall not apply to the extent that processing is necessary:

(a) for exercising the right of freedom of expression and information;

(b) for compliance with a legal obligation which requires processing under domestic law or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

(c) for reasons of public interest in the area of public health in accordance with points (h) and (i) of Article 9(2) as well as Article 9(3);

(d) for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 84B ~~89(1)~~ in so far as the right referred to in paragraph 1 is likely to render impossible or seriously impair the achievement of the objectives of that processing; or [s. 23(1)(c)]

(e) for the establishment, exercise or defence of legal claims.

Article 18 Right to restriction of processing

1.

The data subject shall have the right to obtain from the controller restriction of processing where one of the following applies:

(a) the accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy of the personal data;

(b) the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead;

(c) the controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims;

(d) the data subject has objected to processing pursuant to Article 21(1) pending the verification whether the legitimate grounds of the controller override those of the data subject.

2.

Where processing has been restricted under paragraph 1, such personal data shall, with the exception of storage, only be processed with the data subject's consent or for the establishment, exercise or defence of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest.

3.

A data subject who has obtained restriction of processing pursuant to paragraph 1 shall be informed by the controller before the restriction of processing is lifted.

Article 19 Notification obligation regarding rectification or erasure of personal data or restriction of processing

The controller shall communicate any rectification or erasure of personal data or restriction of processing carried out in accordance with Article 16, Article 17(1) and Article 18 to each recipient to whom the personal data have been disclosed, unless this proves impossible or involves disproportionate effort. The controller shall inform the data subject about those recipients if the data subject requests it.

Article 20 Right to data portability

1.

The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, where:

(a) the processing is based on consent pursuant to point (a) of Article 6(1) or point (a) of Article 9(2) or on a contract pursuant to point (b) of Article 6(1); and

(b) the processing is carried out by automated means.

2.

In exercising his or her right to data portability pursuant to paragraph 1, the data subject shall have the right to have the personal data transmitted directly from one controller to another, where technically feasible.

3.

The exercise of the right referred to in paragraph 1 of this Article shall be without prejudice to Article 17. That right shall not apply to processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

4.

The right referred to in paragraph 1 shall not adversely affect the rights and freedoms of others.

S4 Right to Object ~~and Automated Individual Decision Making~~ [sch. 3 para 7]

Article 21 Right to object

1.

The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her which is based on point (e), (ea) or (f) of Article 6(1), including profiling based on those provisions. The controller shall no longer process the personal data unless

the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims. [s. 5(5)]

2.

Where personal data are processed for direct marketing purposes, the data subject shall have the right to object at any time to processing of personal data concerning him or her for such marketing, which includes profiling to the extent that it is related to such direct marketing.

3.

Where the data subject objects to processing for direct marketing purposes, the personal data shall no longer be processed for such purposes.

4.

At the latest at the time of the first communication with the data subject, the right referred to in paragraphs 1 and 2 shall be explicitly brought to the attention of the data subject and shall be presented clearly and separately from any other information.

5.

In the context of the use of information society services, Directive 2002/58/EC, the data subject may exercise his or her right to object by automated means using technical specifications, notwithstanding domestic law made before IP completion day implementing Directive 2002/58/EC of the European Parliament and of the Council of 12th July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector.

6.

Where personal data are processed for scientific or historical research purposes or statistical purposes ~~pursuant to Article 89(1)~~, the data subject, on grounds relating to his or her particular situation, shall have the right to object to processing of personal data concerning him or her, unless the processing is necessary for the performance of a task carried out for reasons of public interest. [s. 23(1)(d)]

~~**Article 22 Automated individual decision-making, including profiling**~~

~~1.~~

~~The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.~~

~~2.~~

~~Paragraph 1 shall not apply if the decision:~~

~~(a) is necessary for entering into, or performance of, a contract between the data subject and a data controller;~~

~~(b) is required or authorised by domestic law which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or~~

~~(c) is based on the data subject's explicit consent.~~

~~3.~~

~~In the cases referred to in points (a) and (c) of paragraph 2, the data controller shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain~~

~~human intervention on the part of the controller, to express his or her point of view and to contest the decision.~~

~~3A.~~

~~Section 14 of the 2018 Act, and regulations under that section, make provision to safeguard data subjects' rights, freedoms and legitimate interests in cases that fall within point (b) of paragraph 2 (but not within point (a) or (c) of that paragraph).~~

~~4.~~

~~Decisions referred to in paragraph 2 shall not be based on special categories of personal data referred to in Article 9(1), unless point (a) or (g) of Article 9(2) applies and suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place.~~ [s.11(1)]

Section 4A Automated individual decision-making

Article 22A Automated processing and significant decisions

1.

For the purposes of Articles 22B and 22C—

(a) a decision is based solely on automated processing if there is no meaningful human involvement in the taking of the decision, and

(b) a decision is a significant decision, in relation to a data subject, if—

(i) it produces a legal effect for the data subject, or

(ii) it has a similarly significant effect for the data subject.

2.

When considering whether there is meaningful human involvement in the taking of a decision include profiling and carrying out, a person must consider, among other things, the extent to which the decision is reached by means of profiling. [s. 11(1)]

Article 22B Restrictions on automated decision-making

1.

A significant decision based entirely or partly on special categories of personal data referred to in Article 9(1) may not be taken based solely on automated processing, unless one of the following conditions is met.

2.

The first condition is that the decision is based entirely on processing of personal data to which the data subject has given explicit consent.

3.

The second condition is that—

(a) the decision is—

(i) necessary for entering into, or performing, a contract between the data subject and a controller, or

(ii) required or authorised by law, and

(b) point (g) of Article 9(2) applies.

4.

A significant decision may not be taken based solely on automated processing if the processing of personal data carried out by, or on behalf of, the decision-maker for the purposes of the decision is carried out entirely or partly in reliance on Article 6(1)(ea). [s. 11(1)]

Article 22C Safeguards for automated decision-making

1.

Where a significant decision taken by or on behalf of a controller in relation to a data subject is—

(a) based entirely or partly on personal data, and

(b) based solely on automated processing,

the controller must ensure that safeguards for the data subject's rights, freedoms and legitimate interests are in place which comply with paragraph 2 and any regulations under Article 22D(4).

2.

The safeguards must consist of or include measures which—

(a) provide the data subject with information about decisions described in paragraph 1 taken in relation to the data subject;

(b) enable the data subject to make representations about such decisions;

(c) enable the data subject to obtain human intervention on the part of the controller in relation to such decisions;

(d) enable the data subject to contest such decisions. [s. 11(1)]

Article 22D Further provision about automated decision-making

1. The Secretary of State may by regulations provide that, for the purposes of Article 22A(1)(a), there is, or is not, to be taken to be meaningful human involvement in the taking of a decision in cases described in the regulations.

2. The Secretary of State may by regulations provide that, for the purposes of Article 22A(1)(b)(ii), a description of decision is, or is not, to be taken to have a similarly significant effect for the data subject.

3. Regulations under paragraph 1 or 2 may amend Article 22A.

4. The Secretary of State may by regulations make further provision about the safeguards required under Article 22C(1), including provision about what is, or is not, to be taken to satisfy a requirement under Article 22C(1) or (2).

5. Regulations under paragraph 4 may amend Article 22C—

(a) by adding or varying safeguards, and

(b) by omitting provision added by regulations under that paragraph.

6. Regulations under this Article are subject to the affirmative resolution procedure. [s. 11(1)]

S5 Restrictions

Article 23 Restrictions

1.

The Secretary of State may restrict the scope of the obligations and rights provided for in or under Articles 12 to 22D and Article 34, as well as Article 5 in so far as its provisions correspond to the rights and obligations provided for in or under Articles 12 to 22D, when such a restriction respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society to safeguard: [sch. 3 para 8]

(c) public security;

(d) 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;

(e) other important objectives of general public interest, in particular an important economic or financial interest of the United Kingdom, including monetary, budgetary and taxation a matters, public health and social security;

(f) the protection of judicial independence and judicial proceedings;

(g) the prevention, investigation, detection and prosecution of breaches of ethics for regulated professions;

(h) a monitoring, inspection or regulatory function connected, even occasionally, to the exercise of official authority in the cases referred to in points ~~(a)~~ (c) to (e) and (g); [sch 9. para 5]

(i) the protection of the data subject or the rights and freedoms of others;

(j) the enforcement of civil law claims.

2.

In particular, provision made in exercise of the power under paragraph 1 shall contain specific provisions at least, where relevant, as to:

(a) the purposes of the processing or categories of processing;

(b) the categories of personal data;

(c) the scope of the restrictions introduced;

(d) the safeguards to prevent abuse or unlawful access or transfer;

(e) the specification of the controller or categories of controllers;

(f) the storage periods and the applicable safeguards taking into account the nature, scope and purposes of the processing or categories of processing;

(g) the risks to the rights and freedoms of data subjects; and

(h) the right of data subjects to be informed about the restriction, unless that may be prejudicial to the purpose of the restriction.

3.

The Secretary of State may exercise the power under paragraph 1 only by making regulations under section 16 of the 2018 Act.

Chapter 4 Controller and Processor

S1 General Obligations of the controller [sch. 4 para 5]

Article 24 Responsibility of the controller

1.

Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate measures, including technical and organisational measures, to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary.

[s. 12(2)]

2.

Where proportionate in relation to processing activities, the measures referred to in paragraph 1 shall include the implementation of appropriate data protection policies by the controller.

3.

Adherence to approved codes of conduct as referred to in Article 40 or approved certification mechanisms as referred to in Article 42 may be used as a means of demonstrating ~~an element by which to demonstrate~~ compliance with the obligations of the controller. [sch 9. para 6]

Article 25 Data protection by design and by default

1.

Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate measures, including technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.
[s. 12(3)(a)]

2.

The controller shall implement appropriate measures, including technical and organisational measures, for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons. [s. 12(3)(b)]

3.

An approved certification mechanism pursuant to Article 42 may be used as a means of demonstrating ~~an element to demonstrate~~ compliance with the requirements set out in paragraphs 1 and 2 of this Article.
[sch 9. para 7]

Article 26 Joint controllers

1.

Where two or more controllers jointly determine the purposes and means of processing, they shall be joint controllers. They shall in a transparent manner determine their respective responsibilities for compliance with the obligations under this Regulation, in particular as regards the exercising of the rights of the data subject and their respective duties to provide the information referred to in Articles 13 and 14, by means of an arrangement between them unless, and in so far as, the respective responsibilities of the controllers are determined by domestic law. The arrangement may designate a contact point for data subjects.

2.

The arrangement referred to in paragraph 1 shall duly reflect the respective roles and relationships of the joint controllers *vis-à-vis* the data subjects. The essence of the arrangement shall be made available to the data subject.

3.

Irrespective of the terms of the arrangement referred to in paragraph 1, the data subject may exercise his or her rights under this Regulation in respect of and against each of the controllers.

~~**Article 27 Representatives of controllers or processors not established in the United Kingdom**~~
~~1.~~

~~Where Article 3(2) applies, the controller or the processor shall designate in writing a representative in the United Kingdom.~~

~~2.~~

~~The obligation laid down in paragraph 1 of this Article shall not apply to:~~

~~(a) processing which is occasional, does not include, on a large scale, processing of special categories of data as referred to in Article 9(1) or processing of personal data relating to criminal convictions and offences referred to in Article 10, and is unlikely to result in a risk to the rights and freedoms of natural persons, taking into account the nature, context, scope and purposes of the processing; or~~

~~(b) a public authority or body.~~

~~4.~~

~~The representative shall be mandated by the controller or processor to be addressed in addition to or instead of the controller or the processor by, in particular, the Commissioner and data subjects, on all issues related to processing, for the purposes of ensuring compliance with this Regulation.~~

~~5.~~

~~The designation of a representative by the controller or processor shall be without prejudice to legal actions which could be initiated against the controller or the processor themselves.~~ [s. 13(1)]

Section 1A Senior responsible individual

Article 27A Designation of senior responsible individual

1.

This Article and Articles 27B and 27C apply to a controller or processor that—

(a) is a public body, or

(b) carries out processing of personal data which, taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of individuals,

other than a court or tribunal acting in its judicial capacity.

2.

The controller or processor must designate one individual to be its senior responsible individual, subject to paragraph 3(b).

3.

Where the controller or processor is an organisation—

(a) a designated individual must be part of the organisation's senior management, and

(b) the controller or processor may designate two or more individuals to act jointly as its senior responsible

individual where the individuals are employed part-time and share a single role within the organisation's senior management.

4.

The controller or processor must—

(a) ensure that the current contact details of the senior responsible individual are publicly available, and

(b) send those details to the Commissioner.

5.

In this Article, "senior management", in relation to an organisation, means the individuals who play significant roles in the making of decisions about how the whole or a substantial part of its activities are to be managed or organised. [s. 14(2)]

Article 27B Senior responsible individual's tasks

1.

The senior responsible individual designated by a controller must be responsible at least for performing the tasks listed in paragraph 2 or securing that they are performed by another person.

2.

Those tasks are—

(a) monitoring compliance by the controller with the data protection legislation;

(b) ensuring that the controller develops, implements, reviews and updates measures to ensure its compliance with the data protection legislation;

(c) informing and advising the controller, any processor engaged by the controller and employees of the controller who carry out processing of personal data of their obligations under the data protection legislation;

(d) organising training for employees of the controller who carry out processing of personal data;

(e) dealing with complaints made to the controller in connection with the processing of personal data;

(f) dealing with personal data breaches;

(g) co-operating with the Commissioner on behalf of the controller;

(h) acting as the contact point for the Commissioner on issues relating to processing of personal data.

3.

The senior responsible individual designated by a processor must be responsible at least for performing the tasks listed in paragraph 4 or securing that they are performed by another person.

4.

Those tasks are—

(a) monitoring compliance by the processor with Articles 28, 30A and 32;

(b) co-operating with the Commissioner on behalf of the processor;

(c) acting as the contact point for the Commissioner on issues relating to processing of personal data.

5.

Where the performance of one of its tasks would result in a conflict of interests, the senior responsible individual must secure that the task is performed by another person.

6.

In deciding whether one or more of their tasks should be performed by another person (whether alone or jointly with others) and, if so, by whom, the senior responsible individual must consider, among other things—

(a) the other person's professional qualifications and knowledge of the data protection legislation,

(b) the resources likely to be available to the other person to carry out the task, and

(c) whether the other person is involved in day-to-day processing of personal data for the controller or processor and, if so, whether that affects the person's ability to perform the task. [s. 14(2)]

Article 27C Senior responsible individual's position

1.

A controller or processor must support its senior responsible individual in the performance of the individual's tasks, including by providing the individual with appropriate resources.

2.

A controller or processor must not dismiss or penalise its senior responsible individual for performing the individual's tasks.

3.

Where the senior responsible individual decides that one or more of its tasks should be performed by another person, the controller or processor must ensure that the person—

(a) has appropriate resources to perform the task,

(b) is not dismissed or penalised by the controller or processor for performing the task, and

(c) does not receive instructions about the performance of the task.

4.

Paragraph 3(c) does not require the controller or processor to prevent instructions being given by the senior responsible individual or another person performing a task for the senior responsible individual, except where such instructions would involve a conflict of interests. [s. 14(2)]

Section 1B Processor etc [s. 14(2)]

Article 28 Processor

1.

Where processing is to be carried out on behalf of a controller, the controller shall use only processors providing sufficient guarantees to implement appropriate measures, including technical and organisational measures, in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject.

[s. 12(4)(a)]

2.

The processor shall not engage another processor without prior specific or general written authorisation of the controller. In the case of general written authorisation, the processor shall inform the controller of any intended changes concerning the addition or replacement of other processors, thereby giving the controller the opportunity to object to such changes.

3.

Processing by a processor shall be governed by a contract or other legal act under domestic law, that is binding on the processor with regard to the controller and that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller. That contract or other legal act shall stipulate, in particular, that the processor:

(a) processes the personal data only on documented instructions from the controller, including with regard to transfers of personal data to a third country or an international organisation, unless required to do so by domestic law; in such a case, the processor shall inform the controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest;

(b) ensures that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;

(c) takes all measures required pursuant to Article 32;

(d) respects the conditions referred to in paragraphs 2 and 4 for engaging another processor;

(e) taking into account the nature of the processing, assists the controller by appropriate measures, including technical and organisational measures, insofar as this is possible, for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III;

[s. 12(4)(b)]

(f) assists the controller in ensuring compliance with the obligations pursuant to Articles 32 to 36 taking into account the nature of processing and the information available to the processor;

(g) at the choice of the controller, deletes or returns all the personal data to the controller after the end of the provision of services relating to processing, and deletes existing copies unless domestic law requires storage of the personal data;

(h) makes available to the controller all information necessary to demonstrate compliance with the obligations laid down in this Article and allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller.

With regard to point (h) of the first subparagraph, the processor shall immediately inform the controller if, in its opinion, an instruction infringes this Regulation or other domestic law relating to data protection.

4.

Where a processor engages another processor for carrying out specific processing activities on behalf of the controller, the same data protection obligations as set out in the contract or other legal act between the controller and the processor as referred to in paragraph 3 shall be imposed on that other processor by way of a contract or other legal act under domestic law, in particular providing sufficient guarantees to implement appropriate measures, including technical and organisational measures, in such a manner that the processing will meet the requirements of this Regulation. Where that other processor fails to fulfil its data protection obligations, the initial processor shall remain fully liable to the controller for the performance of that other processor's obligations.

[s. 12(4)(c)]

5.

Adherence of a processor to an approved code of conduct as referred to in Article 40 or an approved certification mechanism as referred to in Article 42 may be used as a means of demonstrating ~~an element by which to demonstrate~~ sufficient guarantees as referred to in paragraphs 1 and 4 of this Article. [sch 9. para 8]

6.

Without prejudice to an individual contract between the controller and the processor, the contract or the other legal act referred to in paragraphs 3 and 4 of this Article may be based, in whole or in part, on standard contractual clauses referred to in paragraph 8 of this Article, including when they are part of a certification granted to the controller or processor pursuant to Articles 42 and 43.

8.

The Commissioner may adopt standard contractual clauses for the matters referred to in paragraph 3 and 4 of this Article.

9.

The contract or the other legal act referred to in paragraphs 3 and 4 shall be in writing, including in electronic form.

10.

Without prejudice to Articles 82, 83 and 84, if a processor infringes this Regulation by determining the purposes and means of processing, the processor shall be considered to be a controller in respect of that processing.

Article 29 Processing under the authority of the controller or processor

The processor and any person acting under the authority of the controller or of the processor, who has access

to personal data, shall not process those data except on instructions from the controller, unless required to do so by domestic law.

Section 1C Records and co-operation with the Commissioner [s. 15(2)]

~~Article 30 Records of processing activities~~

~~1.~~

~~Each controller and, where applicable, the controller's representative, shall maintain a record of processing activities under its responsibility. That record shall contain all of the following information:~~

~~(a) the name and contact details of the controller and, where applicable, the joint controller, the controller's representative and the data protection officer;~~

~~(b) the purposes of the processing;~~

~~(c) a description of the categories of data subjects and of the categories of personal data;~~

~~(d) the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organisations;~~

~~(e) where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards;~~

~~(f) where possible, the envisaged time limits for erasure of the different categories of data;~~

~~(g) where possible, a general description of the technical and organisational security measures referred to in Article 32(1) or, as appropriate, the security measures referred to in section 28(3) of the 2018 Act.~~

~~2.~~

~~Each processor and, where applicable, the processor's representative shall maintain a record of all categories of processing activities carried out on behalf of a controller, containing:~~

~~(a) the name and contact details of the processor or processors and of each controller on behalf of which the processor is acting, and, where applicable, of the controller's or the processor's representative, and the data protection officer;~~

~~(b) the categories of processing carried out on behalf of each controller;~~

~~(c) where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards;~~

~~(d) where possible, a general description of the technical and organisational security measures referred to in Article 32(1) or, as appropriate, the security measures referred to in section 28(3) of the 2018 Act.~~

~~3.~~

~~The records referred to in paragraphs 1 and 2 shall be in writing, including in electronic form.~~

~~4.~~

~~The controller or the processor and, where applicable, the controller's or the processor's representative, shall make the record available to the Commissioner on request.~~

~~5.~~

~~The obligations referred to in paragraphs 1 and 2 shall not apply to an enterprise or an organisation employing fewer than 250 persons unless the processing it carries out is likely to result in a risk to the rights and freedoms of data subjects, the processing is not occasional, or the processing includes special categories of data as referred to in Article 9(1) or personal data relating to criminal convictions and offences referred to in Article 10.~~

[s. 15(3)]

Article 30A Records of processing of personal data

1. In this Article—

(a) paragraphs 2 to 4, 8 and 9 apply to a controller that carries out processing of personal data which, taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of individuals, and

(b) paragraphs 5 to 9 apply to a processor that carries out such processing.

2. The controller must maintain appropriate records of processing of personal data carried out by or on behalf of the controller.

3. The controller's records must include at least the following information about the personal data in respect of which the controller is for the time being a controller—

(a) where the personal data is (including information about any personal data that is outside the United Kingdom),

(b) the purposes for which the controller is processing the personal data,

(c) the categories of person with whom the controller has shared, or intends to share, the personal data (including persons who are in third countries or international organisations),

(d) how long the controller intends to retain the personal data,

(e) whether the personal data includes special categories of personal data referred to in Article 9(1) and, if so, which categories, and

(f) whether the personal data includes personal data relating to criminal convictions and offences or related security measures referred to in Article 10(1) and, if so, which types of such data.

4. Where possible, the controller's records must include information about how it ensures that personal data is secure.

5. The processor must maintain appropriate records of its processing of personal data.

6. The processor's records must include at least the following information about the personal data in respect of which it is

for the time being a processor—

(a) the name and contact details of each controller on behalf of which the processor is acting, and

(b) where the personal data is (including information about any personal data that is outside the United Kingdom).

7. Where possible, the processor's records must include information about how it ensures that personal data is secure.

8. A controller or processor must make the records maintained under this Article available to the Commissioner on request.

9. In deciding what is appropriate for the purposes of this Article, a controller or processor must take into account, among other things—

(a) the nature, scope, context and purposes of processing carried out by or on behalf of the controller or by the processor,

(b) the risks for the rights and freedoms of individuals arising from that processing, including the likelihood of risks arising and their severity, and

(c) the resources available to the controller or processor. [s. 15(4)]

Article 31 Cooperation with the Commissioner

The controller and the processor ~~and, where applicable, their representatives,~~ shall cooperate, on request, with the Commissioner in the performance of the Commissioner's tasks. [s. 13(2)(e)]

S2 Security of Personal Data

Article 32 Security of processing

1.

Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

(a) the pseudonymisation and encryption of personal data;

(b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

(c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

(d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

2.

In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

3.

Adherence to an approved code of conduct as referred to in Article 40 or an approved certification mechanism as referred to in Article 42 may be used as a means of demonstrating ~~an element by which to demonstrate~~compliance with the requirements set out in paragraph 1 of this Article. [sch 9. para 9]

4.

The controller and processor shall take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller, unless he or she is required to do so by domestic law.

Article 33 Notification of a personal data breach to the Commissioner

1.

In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the Commissioner, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification under this paragraph is not made within 72 hours, it shall be accompanied by reasons for the delay.

2.

The processor shall notify the controller without undue delay after becoming aware of a personal data breach.

3.

The notification referred to in paragraph 1 shall at least:

(a) describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

(b) communicate the name and contact details of the senior responsible individual ~~data protection officer~~or other contact point where more information can be obtained; [sch. 4 para 6]

(c) describe the likely consequences of the personal data breach;

(d) describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

4.

Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.

5.

The controller shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable the Commissioner to verify compliance with this Article.

Article 34 Communication of a personal data breach to the data subject

1.

When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay.

2.

The communication to the data subject referred to in paragraph 1 of this Article shall describe in clear and plain language the nature of the personal data breach and contain at least the information and measures referred to in points (b), (c) and (d) of Article 33(3).

3.

The communication to the data subject referred to in paragraph 1 shall not be required if any of the following conditions are met:

(a) the controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption;

(b) the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects referred to in paragraph 1 is no longer likely to materialise;

(c) it would involve disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.

4.

If the controller has not already communicated the personal data breach to the data subject, the Commissioner, having considered the likelihood of the personal data breach resulting in a high risk, may require it to do so or may decide that any of the conditions referred to in paragraph 3 are met.

S3 ~~Data Protection Impact Assessment~~ Assessment of High Risk Processing and Prior Consultation [s. 17(2)]

Article 35 ~~Data protection impact assessment~~ Assessment of High Risk Processing [s. 17(3)(a)]

1.

Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of individuals ~~natural persons~~, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks.

[s. 17(3)(b)]

~~2.~~

~~The controller shall seek the advice of the data protection officer, where designated, when carrying out a data protection impact assessment.~~

~~3.~~

~~A data protection impact assessment referred to in paragraph 1 shall in particular be required in the case of:~~

~~(a) a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;~~

~~(b) processing on a large scale of special categories of data referred to in Article 9(1), or of personal data relating to criminal convictions and offences referred to in Article 10; or~~

~~(c) a systematic monitoring of a publicly accessible area on a large scale.~~

~~4.~~

~~The Commissioner shall establish and make public a list of the kind of processing operations which are subject to the requirement for an data protection impact assessment pursuant to paragraph 1.~~

~~5.~~

~~The Commissioner may also establish and make public a list of the kind of processing operations for which no data protection impact assessment pursuant to paragraph 1 is required.~~ [s. 17(3)(c)]

7.

The controller must produce a document recording compliance with this Article which includes at least—

(a) a summary of the purposes of the processing,

(b) an assessment of whether the processing is necessary for those purposes,

(c) an assessment of the risks to individuals referred to in paragraph 1, and

(d) a description of how the controller proposes to mitigate those risks.

~~The assessment shall contain at least:~~

~~(a) a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller;~~

~~(b) an assessment of the necessity and proportionality of the processing operations in relation to the purposes;~~

~~(c) an assessment of the risks to the rights and freedoms of data subjects referred to in paragraph 1; and~~

~~(d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned.~~

[s. 17(2)(d)]

8.

Compliance with approved codes of conduct referred to in Article 40 by the relevant controllers or processors shall be taken into due account in assessing the impact of the processing operations performed by such controllers or processors, for the purposes of an assessment required by paragraph 1. ~~in particular for the purposes of a data protection impact assessment.~~ [s. 17(2)(e)]

~~9.~~

~~Where appropriate, the controller shall seek the views of data subjects or their representatives on the intended processing, without prejudice to the protection of commercial or public interests or the security of processing operations.~~ [s. 17(2)(f)]

10.

In the case of processing pursuant to point (c) or (e) of Article 6(1), paragraphs 1 to 7 of this Article do not apply if an assessment of the envisaged processing operations on the protection of personal data ~~a data protection impact assessment~~ has already been carried out ~~for the processing~~ as part of a general impact assessment required by domestic law, unless domestic law provides otherwise.

[s. 17(2)(g)]

11.

~~Where necessary,~~ The controller shall carry out a review ~~to assess if processing is performed in accordance with the data protection impact assessment~~ of an assessment pursuant to paragraph 1 where necessary and at least when there is a change of the risk represented by processing operations. [s. 17(2)(h)]

Article 36 Prior consultation

1.

The controller may ~~shall~~ consult the Commissioner prior to processing where an ~~data protection impact~~ assessment under Article 35 indicates that the processing would result in a high risk to the rights and freedoms of individuals in the absence of measures taken by the controller to mitigate the risk. [s. 18(2)]

2.

Where the Commissioner is of the opinion that the intended processing referred to in paragraph 1 would infringe this Regulation, in particular where the controller has insufficiently identified or mitigated the risk, the supervisory authority shall, within period of up to eight weeks of receipt of the request for consultation, provide written advice to the controller and, where applicable to the processor, and may use any of its powers referred to in Article 58. That period may be extended by six weeks, taking into account the complexity of the intended processing. The Commissioner shall inform the controller and, where applicable, the processor, of any such extension within one month of receipt of the request for consultation together with the reasons for the delay. Those periods may be suspended until the Commissioner has obtained information the Commissioner has requested for the purposes of the consultation.

3.

When consulting the Commissioner pursuant to paragraph 1, the controller shall provide the supervisory authority with:

(a) where applicable, the respective responsibilities of the controller, joint controllers and processors involved in the processing, in particular for processing within a group of undertakings;

(b) the purposes and means of the intended processing;

(c) the measures and safeguards provided to protect the rights and freedoms of data subjects pursuant to this Regulation;

(d) where applicable, the contact details of the senior responsible individual ~~data protection officer~~;
[s. 18(3)(a)]

(e) the ~~data protection impact~~ assessment provided for in Article 35; and [s. 18(3)(b)]

(f) any other information requested by the Commissioner.

4.

The relevant authority must consult the Commissioner during the preparation of a proposal for a legislative measure to be adopted by Parliament, the National Assembly for Wales, the Scottish Parliament or the Northern Ireland Assembly, or of a regulatory measure based on such a legislative measure, which relates to processing.

4A.

In paragraph 4, *"the relevant authority"* means—

(a) in relation to a legislative measure adopted by Parliament, or a regulatory measure based on such a legislative measure, the Secretary of State;

(b) in relation to a legislative measure adopted by the National Assembly for Wales, or a regulatory measure based on such a legislative measure, the Welsh Ministers;

(c) in relation to a legislative measure adopted by the Scottish Parliament, or a regulatory measure based on such a legislative measure, the Scottish Ministers;

(d) in relation to a legislative measure adopted by the Northern Ireland Assembly, or a regulatory measure based on such a legislative measure, the relevant Northern Ireland department.

~~S4 Data Protection Officer~~ [s. 14(3)]

~~Article 37 Designation of the data protection officer~~

~~1.~~

~~The controller and the processor shall designate a data protection officer in any case where:~~

~~(a) the processing is carried out by a public authority or body, except for courts and tribunals acting in their judicial capacity;~~

~~(b) the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or~~

~~(c) the core activities of the controller or the processor consist of processing on a large scale of special categories of data pursuant to Article 9 or personal data relating to criminal convictions and offences referred to in Article 10.~~

~~2.~~

~~A group of undertakings may appoint a single data protection officer provided that a data protection officer is easily accessible from each establishment.~~

~~3.~~

~~Where the controller or the processor is a public authority or body, a single data protection officer may be designated for several such authorities or bodies, taking account of their organisational structure and size.~~

~~4.~~

~~In cases other than those referred to in paragraph 1, the controller or processor or associations and other bodies representing categories of controllers or processors may designate a data protection officer. The data protection officer may act for such associations and other bodies representing controllers or processors.~~

~~5.~~

~~The data protection officer shall be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfil the tasks referred to in Article 39.~~

~~6.~~

~~The data protection officer may be a staff member of the controller or processor, or fulfil the tasks on the basis of a service contract.~~

~~7.~~

~~The controller or the processor shall publish the contact details of the data protection officer and communicate them to the Commissioner.~~ [s. 14(3)]

~~Article 38 Position of the data protection officer~~

~~1.~~

~~The controller and the processor shall ensure that the data protection officer is involved, properly and in a timely manner, in all issues which relate to the protection of personal data.~~

~~2.~~

~~The controller and processor shall support the data protection officer in performing the tasks referred to in Article 39 by providing resources necessary to carry out those tasks and access to personal data and processing operations, and to maintain his or her expert knowledge.~~

~~3.~~

~~The controller and processor shall ensure that the data protection officer does not receive any instructions regarding the exercise of those tasks. He or she shall not be dismissed or penalised by the controller or the processor for performing his tasks. The data protection officer shall directly report to the highest management level of the controller or the processor.~~

~~4.~~

~~Data subjects may contact the data protection officer with regard to all issues related to processing of their personal data and to the exercise of their rights under this Regulation.~~

~~5.~~

~~The data protection officer shall be bound by secrecy or confidentiality concerning the performance of his or her tasks, in accordance with domestic law.~~

~~6.~~

~~The data protection officer may fulfil other tasks and duties. The controller or processor shall ensure that any such tasks and duties do not result in a conflict of interests~~. [s. 14(3)]

~~Article 39 Tasks of the data protection officer~~

~~1.~~

~~The data protection officer shall have at least the following tasks:~~

~~(a) to inform and advise the controller or the processor and the employees who carry out processing of their obligations pursuant to this Regulation and to other domestic law relating to data protection;~~

~~(b) to monitor compliance with this Regulation, with other domestic law relating to data protection and with~~

~~the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits;~~

~~(c) to provide advice where requested as regards the data protection impact assessment and monitor its performance pursuant to Article 35;~~

~~(d) to cooperate with the Commissioner;~~

~~(e) to act as the contact point for the Commissioner on issues relating to processing, including the prior consultation referred to in Article 36, and to consult, where appropriate, with regard to any other matter.~~

~~2.~~

~~The data protection officer shall in the performance of his or her tasks have due regard to the risk associated with processing operations, taking into account the nature, scope, context and purposes of processing.~~

[s. 14(3)]

S5 Codes of Conduct and Certification

Article 40 Codes of conduct

1.

The Commissioner shall encourage the drawing up of codes of conduct intended to contribute to the proper application of this Regulation, taking account of the specific features of the various processing sectors and the specific needs of micro, small and medium-sized enterprises.

2.

Associations and other bodies representing categories of controllers or processors may prepare codes of conduct, or amend or extend such codes, for the purpose of specifying the application of this Regulation, such as with regard to:

(a) fair and transparent processing;

(b) the legitimate interests pursued by controllers in specific contexts;

(c) the collection of personal data;

(d) the pseudonymisation of personal data;

(e) the information provided to the public and to data subjects;

(f) the exercise of the rights of data subjects;

(g) the information provided to, and the protection of, children, and the manner in which the consent of the holders of parental responsibility over children is to be obtained;

(h) the measures and procedures referred to in Articles 24 and 25 and the measures to ensure security of processing referred to in Article 32;

(i) the notification of personal data breaches to the Commissioner and the communication of such personal data breaches to data subjects;

(j) the transfer of personal data to third countries or international organisations; or

(k) out-of-court proceedings and other dispute resolution procedures for resolving disputes between controllers and data subjects with regard to processing, without prejudice to the rights of data subjects pursuant to Articles 77 and 79.

3.

In addition to adherence by controllers or processors subject to this Regulation, codes of conduct approved pursuant to paragraph 5 of this Article may also be adhered to by controllers or processors that are not subject to this Regulation pursuant to Article 3 in order to provide ~~appropriate~~ safeguards within the framework of personal data transfers to third countries or international organisations under the terms referred to in point (e) of Article 46(2). Such controllers or processors shall make binding and enforceable commitments, via contractual or other legally binding instruments, to apply those ~~appropriate~~ safeguards including with regard to the rights of data subjects. [sch. 7 para 5(2)]

4.

A code of conduct referred to in paragraph 2 of this Article shall contain mechanisms which enable the body referred to in Article 41(1) to carry out the mandatory monitoring of compliance with its provisions by the controllers or processors which undertake to apply it, without prejudice to the tasks and powers of the Commissioner.

5.

Associations and other bodies referred to in paragraph 2 of this Article which intend to prepare a code of conduct or to amend or extend an existing code shall submit the draft code, amendment or extension to the Commissioner, who shall provide an opinion on whether the draft code, amendment or extension complies with this Regulation and shall approve that draft code, amendment or extension if the Commissioner finds that it is capable of providing ~~provides sufficient appropriate~~ safeguards for the purposes of Article 46.
[sch. 7 para 5(3)]

6.

Where the draft code, or amendment or extension is approved in accordance with paragraph 5, the Commissioner shall register and publish the code.

Article 41 Monitoring of approved codes of conduct

1.

Without prejudice to the tasks and powers of the Commissioner under Articles 57 and 58, the monitoring of compliance with a code of conduct pursuant to Article 40 may be carried out by a body which has an appropriate level of expertise in relation to the subject-matter of the code and is accredited for that purpose by the Commissioner.

2.

A body as referred to in paragraph 1 may be accredited to monitor compliance with a code of conduct where that body has:

(a) demonstrated its independence and expertise in relation to the subject-matter of the code to the satisfaction of the Commissioner;

(b) established procedures which allow it to assess the eligibility of controllers and processors concerned to

apply the code, to monitor their compliance with its provisions and to periodically review its operation;

(c) established procedures and structures to handle complaints about infringements of the code or the manner in which the code has been, or is being, implemented by a controller or processor, and to make those procedures and structures transparent to data subjects and the public; and

(d) demonstrated to the satisfaction of the Commissioner that its tasks and duties do not result in a conflict of interests.

4.

Without prejudice to the tasks and powers of the Commissioner and the provisions of Chapter VIII, a body as referred to in paragraph 1 of this Article shall, subject to appropriate safeguards, take appropriate action in cases of infringement of the code by a controller or processor, including suspension or exclusion of the controller or processor concerned from the code. It shall inform the Commissioner of such actions and the reasons for taking them.

5.

The Commissioner shall revoke the accreditation of a body as referred to in paragraph 1 if the requirements for accreditation are not, or are no longer, met or where actions taken by the body infringe this Regulation.

6.

This Article shall not apply to processing carried out by public authorities and bodies.

Article 42 Certification

1.

The Commissioner shall encourage the establishment of data protection certification mechanisms and of data protection seals and marks, for the purpose of demonstrating compliance with this Regulation of processing operations by controllers and processors. The specific needs of micro, small and medium-sized enterprises shall be taken into account.

2.

In addition to adherence by controllers or processors subject to this Regulation, data protection certification mechanisms, seals or marks approved pursuant to paragraph 5 of this Article may be established for the purpose of demonstrating the existence of ~~appropriate~~ safeguards provided by controllers or processors that are not subject to this Regulation pursuant to Article 3 within the framework of personal data transfers to third countries or international organisations under the terms referred to in point (f) of Article 46(2). Such controllers or processors shall make binding and enforceable commitments, via contractual or other legally binding instruments, to apply those ~~appropriate~~ safeguards, including with regard to the rights of data subjects.

[sch. 7 para 6]

3.

The certification shall be voluntary and available via a process that is transparent.

4.

A certification pursuant to this Article does not reduce the responsibility of the controller or the processor for compliance with this Regulation and is without prejudice to the tasks and powers of the Commissioner.

5.

A certification pursuant to this Article shall be issued by the certification bodies referred to in Article 43 or by the

Commissioner, on the basis of criteria approved by the Commissioner pursuant to Article 58(3).

6.

The controller or processor which submits its processing to the certification mechanism shall provide the certification body referred to in Article 43, or where applicable, the Commissioner, with all information and access to its processing activities which are necessary to conduct the certification procedure.

7.

Certification shall be issued to a controller or processor for a maximum period of three years and may be renewed, under the same conditions, provided that the relevant criteria continue to be met. Certification shall be withdrawn, as applicable, by the certification bodies referred to in Article 43 or by the Commissioner where the criteria for the certification are not or are no longer met.

8.

The Commissioner shall collate all certification mechanisms and data protection seals and marks in a register and shall make them publicly available by any appropriate means.

Article 43 Certification bodies

1.

Without prejudice to the tasks and powers of the Commissioner under Articles 57 and 58, certification bodies which have an appropriate level of expertise in relation to data protection shall, after informing the Commissioner in order to allow it to exercise its powers pursuant to point (h) of Article 58(2) where necessary, issue and renew certification. In accordance with section 17 of the 2018 Act, those certification bodies may only be accredited by one or both of the following:

(a) the Commissioner;

(b) the UK national accreditation body named in accordance with Regulation (EC) No 765/2008 of the European Parliament and of the Council in accordance with EN-ISO/IEC 17065/2012 and with the additional requirements established by the Commissioner.

2.

Certification bodies referred to in paragraph 1 shall be accredited in accordance with that paragraph only where they have:

(a) demonstrated their independence and expertise in relation to the subject-matter of the certification to the satisfaction of the Commissioner;

(b) undertaken to respect the criteria referred to in Article 42(5) and approved by the Commissioner;

(c) established procedures for the issuing, periodic review and withdrawal of data protection certification, seals and marks;

(d) established procedures and structures to handle complaints about infringements of the certification or the manner in which the certification has been, or is being, implemented by the controller or processor, and to make those procedures and structures transparent to data subjects and the public; and

(e) demonstrated, to the satisfaction of the Commissioner, that their tasks and duties do not result in a

conflict of interests.

3.

The accreditation of certification bodies as referred to in paragraphs 1 and 2 of this Article shall take place on the basis of requirements approved by the Commissioner. In the case of accreditation pursuant to point (b) of paragraph 1 of this Article, those requirements shall complement those envisaged in Regulation (EC) No 765/2008 and the technical rules that describe the methods and procedures of the certification bodies.

4.

The certification bodies referred to in paragraph 1 shall be responsible for the proper assessment leading to the certification or the withdrawal of such certification without prejudice to the responsibility of the controller or processor for compliance with this Regulation. The accreditation shall be issued for a maximum period of five years and may be renewed on the same conditions provided that the certification body meets the requirements set out in this Article.

5.

The certification bodies referred to in paragraph 1 shall provide the Commissioner with the reasons for granting or withdrawing the requested certification.

6.

The requirements referred to in paragraph 3 of this Article and the criteria referred to in Article 42(5) shall be made public by the Commissioner in an easily accessible form.

7.

Without prejudice to Chapter VIII, the Commissioner or the UK national accreditation body shall revoke an accreditation of a certification body pursuant to paragraph 1 of this Article where the conditions for the accreditation are not, or are no longer, met or where actions taken by a certification body infringe this Regulation.

Chapter 5 Transfer of Personal Data to Third Countries or International Organisations

~~**Article 44 General principle for transfers**~~

~~Any transfer of personal data which are undergoing processing or are intended for processing after transfer to a third country or to an international organisation shall take place only if, subject to the other provisions of this Regulation, the conditions laid down in this Chapter are complied with by the controller and processor, including for onward transfers of personal data from the third country or an international organisation to another third country or to another international organisation. All provisions in this Chapter shall be applied in order to ensure that the level of protection of natural persons guaranteed by this Regulation is not undermined.~~

Article 44A General principles for transfers

1.

A controller or processor may transfer personal data to a third country or an international organisation only if—

(a) the condition in paragraph 2 is met, and

(b) the transfer is carried out in compliance with the other provisions of this Regulation.

2.

The condition is met if the transfer—

(a) is approved by regulations under Article 45A that are in force at the time of the transfer,

(b) is made subject to appropriate safeguards (see Article 46), or

(c) is made in reliance on a derogation for specific situations (see Article 49).

3.

A transfer may not be made in reliance on paragraph 2(b) or (c) if, or to the extent that, it would breach a restriction in regulations under Article 49A. [sch. 5 para 2]

~~**Article 45 Transfers on the basis of an adequacy decision**~~

~~1.~~

~~A transfer of personal data to a third country or an international organisation may take place where it is based on adequacy regulations (see section 17A of the 2018 Act). Such a transfer shall not require any specific authorisation.~~

~~2.~~

~~When assessing the adequacy of the level of protection for the purposes of sections 17A and 17B of the 2018 Act, the Secretary of State shall, in particular, take account of the following elements:~~

~~(a) the rule of law, respect for human rights and fundamental freedoms, relevant legislation, both general and sectoral, including concerning public security, defence, national security and criminal law and the access of public authorities to personal data, as well as the implementation of such legislation, data protection rules, professional rules and security measures, including rules for the onward transfer of personal data to another third country or international organisation which are complied with in that country or international organisation, case-law, as well as effective and enforceable data subject rights and effective administrative and judicial redress for the data subjects whose personal data are being transferred;~~

~~(b) the existence and effective functioning of one or more independent supervisory authorities in the third country or to which an international organisation is subject, with responsibility for ensuring and enforcing compliance with the data protection rules, including adequate enforcement powers, for assisting and advising the data subjects in exercising their rights and for cooperation with the Commissioner; and~~

~~(c) the international commitments the third country or international organisation concerned has entered into, or other obligations arising from legally binding conventions or instruments as well as from its participation in multilateral or regional systems, in particular in relation to the protection of personal data.~~

~~7.~~

~~The amendment or revocation of regulations under section 17A of the 2018 Act is without prejudice to transfers of personal data to the third country, a territory or one or more specified sectors within that third country, or the international organisation in question pursuant to Articles 46 to 49.~~ [sch. 5 para 3]

Article 45A Transfers approved by regulations

1.

For the purposes of Article 44A, the Secretary of State may by regulations approve transfers of personal data to—

(a) a third country, or

(b) an international organisation.

2.

The Secretary of State may only make regulations under this Article approving transfers to a third country or international organisation if the Secretary of State considers that the data protection test is met in relation to the transfers (see Article 45B).

3.

In making regulations under this Article, the Secretary of State may have regard to any matter which the Secretary of State considers relevant, including the desirability of facilitating transfers of personal data to and from the United Kingdom.

4.

Regulations under this Article may, among other things—

(a) make provision in relation to a third country or international organisation specified in the regulations or a description of country or organisation;

(b) approve all transfers of personal data to a third country or international organisation or only transfers specified or described in the regulations;

(c) identify a transfer of personal data by any means, including by reference to—

(i) a sector or geographic area within a third country,

(ii) the controller or processor,

(iii) the recipient of the personal data,

(iv) the personal data transferred,

(v) the means by which the transfer is made, or

(vi) relevant legislation, schemes, lists or other arrangements or documents, as they have effect from time to time;

(d) confer a discretion on a person.

5.

Regulations under this Article are subject to the negative resolution procedure.

[sch. 5 para 4]

Article 45B The data protection test

1.

For the purposes of Article 45A, the data protection test is met in relation to transfers of personal data to a third country or international organisation if the standard of the protection provided for data subjects with regard to general processing of personal data in the country or by the organisation is not materially lower than the standard of the protection provided for data subjects by or under—

(a) this Regulation,(b) Part 2 of the 2018 Act, and

(c) Parts 5 to 7 of that Act, so far as relevant to general processing.

2.

In considering whether the data protection test is met in relation to transfers of personal data to a third country or international organisation, the Secretary of State must consider, among other things—

(a) respect for the rule of law and for human rights in the country or by the organisation,

(b) the existence, and powers, of an authority responsible for enforcing the protection of data subjects with regard to the processing of personal data in the country or by the organisation,

(c) arrangements for judicial or non-judicial redress for data subjects in connection with such processing,

(d) rules about the transfer of personal data from the country or by the organisation to other countries or international organisations,

(e) relevant international obligations of the country or organisation, and

(f) the constitution, traditions and culture of the country or organisation.

3.

In paragraphs 1 and 2—

(a) the references to the protection provided for data subjects are to that protection taken as a whole,

(b) the references to general processing are to processing to which this Regulation applies or equivalent types of processing in the third country or by the international organisation (as appropriate), and

(c) the references to processing of personal data in the third country or by the international organisation are references only to the processing of personal data transferred from the United Kingdom.

4.

When the data protection test is applied only to certain transfers to a third country or international organisation that are specified or described, or to be specified or described, in regulations (in accordance with Article 45A(4)(b))—

(a) the references in paragraphs 1 to 3 to personal data are to be read as references only to personal data likely to be the subject of such transfers, and

(b) the reference in paragraph 2(d) to the transfer of personal data to other countries or international organisations is to be read as a including the transfer of personal data within the third country or

international organisation. [sch. 5 para 4]

Article 45C Transfers approved by regulations: monitoring

1.

The Secretary of State must, on an ongoing basis, monitor developments in third countries and international organisations that could affect decisions to make regulations under Article 45A or to amend or revoke such regulations.

2.

Where the Secretary of State becomes aware that the data protection test is no longer met in relation to transfers approved, or of a description approved, in regulations under Article 45A, the Secretary of State must, to the extent necessary, amend or revoke the regulations.

3.

Where regulations under Article 45A are amended or revoked in accordance with paragraph 2, the Secretary of State must enter into consultations with the third country or international organisation concerned with a view to improving the protection provided to data subjects with regard to the processing of personal data in the country or by the organisation.

4.

The Secretary of State must publish—

(a) a list of the third countries and international organisations, and the descriptions of such countries and organisations, which are for the time being approved by regulations under Article 45A as places or persons to which personal data may be transferred, and

(b) a list of the third countries and international organisations, and the descriptions of such countries and organisations, which have been but are no longer approved by such regulations.

5.

In the case of regulations under Article 45A which approve only certain transfers to a third country or international organisation specified or described in the regulations (in accordance with Article 45A(4)(b)), the lists published under paragraph 4 must specify or describe the relevant transfers. [sch. 5 para 5]

Article 46 Transfers subject to appropriate safeguards

~~1.~~

~~In the absence of adequacy regulations under section 17A of the 2018 Act, a controller or processor may transfer personal data to a third country or an international organisation only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available.~~ [sch. 5 para 6(2)]

1A.

A transfer of personal data to a third country or an international organisation by a controller or processor is made subject to appropriate safeguards only—

(a) in a case in which—

(i) safeguards are provided in connection with the transfer as described in paragraph 2 or 3 or regulations made under Article 47A(4), and

(ii) the controller or processor, acting reasonably and proportionately, considers that the data protection test is met in relation to the transfer or that type of transfer (see paragraph 6), or

(b) in a case in which—

(i) safeguards are provided in accordance with paragraph 2(a) by an instrument that is intended to be relied on in connection with the transfer or that type of transfer, and

(ii) each public body that is a party to the instrument, acting reasonably and proportionately, considers that the data protection test is met in relation to the transfers, or types of transfer, intended to be made in reliance on the instrument (see paragraph 6). [sch. 5 para 6(3)]

2.

The ~~appropriate~~ safeguards referred to in paragraph 1A(a) may be provided for, without requiring any specific authorisation from the Commissioner, by:

(a) a legally binding and enforceable instrument between a public body and another relevant person or persons ~~public authorities or bodies~~;

(b) binding corporate rules approved in accordance with Article 47;

(c) standard data protection clauses specified in regulations made by the Secretary of State under Article 47A(1) ~~section 17C of the 2018 Act~~ and for the time being in force;

(d) standard data protection clauses specified in a document issued (and not withdrawn) by the Commissioner under section 119A of the 2018 Act and for the time being in force;

(e) an approved code of conduct pursuant to Article 40 together with binding and enforceable commitments of the controller or processor in the third country to apply the safeguards provided by the code ~~appropriate safeguards~~, including as regards data subjects' rights; or

(f) an approved certification mechanism pursuant to Article 42 together with binding and enforceable commitments of the controller or processor in the third country to apply the safeguards provided by the mechanism ~~appropriate safeguards~~, including as regards data subjects' rights. [sch. 5 para 6(4)]

3.

With authorisation from the Commissioner, the ~~appropriate~~ safeguards referred to in paragraph 1A(a) may also be provided for, ~~in particular~~, by:

(a) contractual clauses between the controller or processor and the controller, processor or the recipient of the personal data in the third country or international organisation; or

(b) provisions to be inserted into administrative arrangements between a public body and another relevant person or persons ~~public authorities or bodies~~ which include enforceable and effective data subject rights.

[sch. 5 para 6(5)]

4. ……

5. ……

6.

For the purposes of this Article, the data protection test is met in relation to a transfer, or a type of transfer, of personal data if, after the transfer, the standard of the protection provided for the data subject with regard to that personal data by the safeguards required under paragraph 1A, and (where relevant) by other means, would not be materially lower than the standard of the protection provided for the data subject with regard to the personal data by or under—

(a) this Regulation,

(b) Part 2 of the 2018 Act, and

(c) Parts 5 to 7 of that Act, so far as relevant to processing to which this Regulation applies.

7.

For the purposes of paragraph 1A(a)(ii) and (b)(ii), what is reasonable and proportionate is to be determined by reference to all the circumstances, or likely circumstances, of the transfer or type of transfer, including the nature and volume of the personal data transferred.

8.

In this Article—

(a) references to the protection provided for the data subject are to that protection taken as a whole;

(b) "relevant person" means a public body or another person exercising functions of a public nature.

[sch. 5 para 6(6)]

Article 47 Transfers subject to appropriate safeguards: Binding corporate rules [sch. 5 para 7]

1.

The Commissioner shall approve binding corporate rules, provided that they:

(a) are legally binding and apply to and are enforced by every member concerned of the group of undertakings, or group of enterprises engaged in a joint economic activity, including their employees;

(b) expressly confer enforceable rights on data subjects with regard to the processing of their personal data; and

(c) fulfil the requirements laid down in paragraph 2.

2.

The binding corporate rules referred to in paragraph 1 shall specify at least:

(a) the structure and contact details of the group of undertakings, or group of enterprises engaged in a joint economic activity and of each of its members;

(b) the data transfers or set of transfers, including the categories of personal data, the type of processing and its purposes, the type of data subjects affected and the identification of the third country or countries in question;

(c) their legally binding nature, both internally and externally;

(d) the application of the general data protection principles, in particular purpose limitation, data minimisation, limited storage periods, data quality, data protection by design and by default, legal basis for processing, processing of special categories of personal data, measures to ensure data security, and the requirements in respect of onward transfers to bodies not bound by the binding corporate rules;

(e) the rights of data subjects in regard to processing and the means to exercise those rights, including the right to protection in connection with decisions (including profiling) based solely on automated processing in accordance with, and with regulations made under, Articles 22A to 22D ~~the right not to be subject to decisions based solely on automated processing, including profiling in accordance with Article 22~~ the right to make a complaint to the controller under section 164A of the 2018 Act, the right to make a complaint to the Commissioner under section 165 of the 2018 Act, the right to lodge a complaint ~~lodge a complaint with the Commissioner and~~ before a court in accordance with Article 79 (see section 180 of the 2018 Act), and to obtain redress and, where appropriate, compensation for a breach of the binding corporate rules;
[sch. 3 para 9 and sch. 8 para 6]

(f) the acceptance by the controller or processor established in the United Kingdom of liability for any breaches of the binding corporate rules by any member concerned not established in the United Kingdom; the controller or the processor shall be exempt from that liability, in whole or in part, only if it proves that that member is not responsible for the event giving rise to the damage;

(g) how the information on the binding corporate rules, in particular on the provisions referred to in points (d), (e) and (f) of this paragraph is provided to the data subjects in addition to Articles 13 and 14;

(h) the tasks of any senior responsible individual ~~data protection officer designated in accordance with Article 37~~ or any other person or entity in charge of the monitoring compliance with the binding corporate rules within the group of undertakings, or group of enterprises engaged in a joint economic activity, as well as monitoring training and complaint-handling; [sch. 4 para 7]

(i) the complaint procedures;

(j) the mechanisms within the group of undertakings, or group of enterprises engaged in a joint economic activity for ensuring the verification of compliance with the binding corporate rules. Such mechanisms shall include data protection audits and methods for ensuring corrective actions to protect the rights of the data subject. Results of such verification should be communicated to the person or entity referred to in point (h) and to the board of the controlling undertaking of a group of undertakings, or of the group of enterprises engaged in a joint economic activity, and should be available upon request to the Commissioner;

(k) the mechanisms for reporting and recording changes to the rules and reporting those changes to the Commissioner;

(l) the cooperation mechanism with the Commissioner to ensure compliance by any member of the group of undertakings, or group of enterprises engaged in a joint economic activity, in particular by making available to the supervisory authority the results of verifications of the measures referred to in point (j);

(m) the mechanisms for reporting to the Commissioner any legal requirements to which a member of the group of undertakings, or group of enterprises engaged in a joint economic activity is subject in a third country which are likely to have a substantial adverse effect on the guarantees provided by the binding corporate rules; and

(n) the appropriate data protection training to personnel having permanent or regular access to personal data.

Article 47A Transfers subject to appropriate safeguards: further provision

1.

The Secretary of State may by regulations specify standard data protection clauses which the Secretary of State considers are capable of securing that the data protection test set out in Article 46 is met in relation to transfers of personal data generally or in relation to a type of transfer specified in the regulations.

2.

The Secretary of State must keep under review the standard data protection clauses specified in regulations under paragraph 1 that are for the time being in force.

3.

Regulations under paragraph 1 are subject to the negative resolution procedure.

4.

The Secretary of State may by regulations make provision about further safeguards that may be relied on for the purposes of Article 46(1A)(a).

5.

The Secretary of State may only make regulations under paragraph 4 if the Secretary of State considers that the further safeguards are capable of securing that the data protection test set out in Article 46 is met in relation to transfers of personal data generally or in relation to a type of transfer specified in the regulations.

6.

Regulations under paragraph 4 may (among other things)—

(a) make provision by adopting safeguards prepared or published by another person;

(b) make provision about ways of providing safeguards which require authorisation from the Commissioner;

(c) amend Article 46 by—

(i) adding ways of providing safeguards, or

(ii) varying or omitting ways of providing safeguards which were added by regulations under this Article.

7.

Regulations under paragraph 4 are subject to the affirmative resolution procedure. [sch. 5 para 8]

[Article 48 Repealed – by prior legislative change]

Article 49 Derogations for specific situations

1.

In the absence of approval by regulations under Article 45A and of compliance with Article 46 (appropriate safeguards) ~~adequacy regulations under section 17A of the 2018 Act, or of appropriate safeguards pursuant to Article 46, including binding corporate rules~~, a transfer or a set of transfers of personal data to a third country or an international organisation shall take place only on one of the following conditions:

(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 approval by regulations under Article 45A ~~an adequacy decision~~ and appropriate safeguards; [sch. 5 para 9(2)]

(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.

Where a transfer could not be based on ~~a provision in~~ Article 45A or 46, including the provisions on binding corporate rules, and none of the derogations for a specific situation referred to in the first subparagraph of this paragraph is applicable, a transfer to a third country or an international organisation may take place only if the transfer 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. The controller shall inform the Commissioner of the transfer. The controller shall, in addition to providing the information referred to in Articles 13 and 14, inform the data subject of the transfer and on the

compelling legitimate interests pursued. [sch. 5 para 9(3)]

2.

A transfer pursuant to point (g) of the first subparagraph of paragraph 1 shall not involve the entirety of the personal data or entire categories of the personal data contained in the register. Where the register is intended for consultation by persons having a legitimate interest, the transfer shall be made only at the request of those persons or if they are to be the recipients.

3.

Points (a), (b) and (c) of the first subparagraph of paragraph 1 and the second subparagraph thereof shall not apply to activities carried out by public authorities in the exercise of their public powers.

4.

The public interest referred to in point (d) of the first subparagraph of paragraph 1 must be public interest that is recognised in domestic law (whether in regulations under paragraph 4A ~~section 18(1) of the 2018 Act~~ or otherwise) . [sch. 5 para 9(4)]

4A.

The Secretary of State may by regulations specify for the purposes of point (d) of paragraph 1—

(a) circumstances in which a transfer of personal data to a third country or international organisation is to be taken to be necessary for important reasons of public interest, and

(b) circumstances in which a transfer of personal data to a third country or international organisation which is not required by an enactment is not to be taken to be necessary for important reasons of public interest. [sch. 5 para 9(5)]

~~5A.~~

~~This Article and Article 46 are subject to restrictions in regulations under section 18(2) of the 2018 Act.~~ [sch. 5 para 9(6)]

6.

The controller or processor shall document the assessment as well as the suitable safeguards referred to in the second subparagraph of paragraph 1 of this Article in the records referred to in Article 30A. [sch. 4 para 8]

7.

Regulations under this Article—

(a) are subject to the made affirmative resolution procedure where the Secretary of State has made an urgency statement in respect of them;

(b) otherwise, are subject to the affirmative resolution procedure.

8.

For the purposes of this Article, an urgency statement is a reasoned statement that the Secretary of State considers it desirable for the regulations to come into force without delay. [sch. 5 para 9(7)]

Article 49A

Restriction in the public interest

1.

The Secretary of State may by regulations restrict the transfer of a category of personal data to a third country or international organisation where—

(a) the transfer is not approved by regulations under Article 45A for the time being in force, and

(b) the Secretary of State considers the restriction to be necessary for important reasons of public interest.

2.

Regulations under this Article—

(a) are subject to the made affirmative resolution procedure where the Secretary of State has made an urgency statement in respect of them;

(b) otherwise, are subject to the affirmative resolution procedure.

3.

For the purposes of this Article, an urgency statement is a reasoned statement that the Secretary of State considers it desirable for the regulations to come into force without delay. [sch. 5 para 10]

Article 50 International cooperation for the protection of personal data

In relation to third countries and international organisations, the Commissioner shall take appropriate steps to:

(a) develop international cooperation mechanisms to facilitate the effective enforcement of legislation for the protection of personal data;

(b) provide international mutual assistance in the enforcement of legislation for the protection of personal data, including through notification, complaint referral, investigative assistance and information exchange, subject to appropriate safeguards for the protection of personal data and other fundamental rights and freedoms;

(c) engage relevant stakeholders in discussion and activities aimed at furthering international cooperation in the enforcement of legislation for the protection of personal data;

(d) promote the exchange and documentation of personal data protection legislation and practice, including on jurisdictional conflicts with third countries.

Chapter 6 The Commissioner

S1 Independent Status

Article 51 Monitoring the application of this Regulation

1.

The Commissioner is responsible for monitoring the application of this Regulation, in order to protect the fundamental rights and freedoms of natural persons in relation to processing and to facilitate the free flow of personal data.

Article 52 Independence

1.

The Commissioner shall act with complete independence in performing tasks and exercising powers in accordance with this Regulation.

2.

The Commissioner shall, in the performance of tasks and exercise of powers in accordance with this Regulation, remain free from external influence, whether direct or indirect, and shall neither seek nor take instructions from anybody.

3.

The Commissioner shall refrain from any action incompatible with the Commissioner's duties and shall not, while holding office, engage in any incompatible occupation, whether gainful or not.

[Articles 53, 54 Repealed – by prior legislative change]

S2 Tasks and Powers

[Articles 55, 56 Repealed – by prior legislative change]

Article 57 Tasks

1.

Without prejudice to other tasks set out under this Regulation, the Commissioner must:

(a) monitor and enforce the application of this Regulation;

(b) promote public awareness and understanding of the risks, rules, safeguards and rights in relation to processing. Activities addressed specifically to children shall receive specific attention;

(c) advise Parliament, the government, and other institutions and bodies on legislative and administrative measures relating to the protection of natural persons' rights and freedoms with regard to processing;

(d) promote the awareness of controllers and processors of their obligations under this Regulation;

(e) upon request, provide information to any data subject concerning the exercise of their rights under this Regulation and, if appropriate, cooperate with foreign designated authorities to that end;

~~(f) handle complaints lodged by a data subject, or by a body, organisation or association in accordance with Article 80, and investigate, to the extent appropriate, the subject matter of the complaint and inform the complainant of the progress and the outcome of the investigation within a reasonable period, in particular if~~

~~further investigation or coordination with a foreign designated authority is necessary;~~ [sch. 8 para 7(a)]

(h) conduct investigations on the application of this Regulation, including on the basis of information received from a foreign designated authority or other public authority;

(i) monitor relevant developments, insofar as they have an impact on the protection of personal data, in particular the development of information and communication technologies and commercial practices;

(j) adopt standard contractual clauses referred to in Article 28(8) and issue standard data protection clauses referred to in point (d) of Article 46(2);

(k) ~~establish and maintain a list of kinds of processing operations in relation to the requirement for data protection impact assessment pursuant to Article 35(4)~~; produce and publish a document containing examples of types of processing which the Commissioner considers are likely to result in a high risk to the rights and freedoms of individuals (for the purposes of Articles 27A, 30A and 35); [s. 17(4)]

(l) give advice on the processing operations referred to in Article 36(2);

(m) encourage the drawing up of codes of conduct pursuant to Article 40(1) and provide an opinion and approve such codes of conduct ~~which provide sufficient safeguards~~, pursuant to Article 40(5);
[sch. 7 para 7(a)]

(n) encourage the establishment of data protection certification mechanisms and of data protection seals and marks pursuant to Article 42(1), and approve the criteria of certification pursuant to Article 42(5);

(o) where applicable, carry out a periodic review of certifications issued in accordance with Article 42(7);

(oa) maintain a public register of certification mechanisms and data protection seals and marks pursuant to Article 42(8) and of controllers or processors established in third countries and certified pursuant to Article 42(7);

(p) draft and publish the requirements for accreditation of a body for monitoring codes of conduct pursuant to Article 41 and of a certification body pursuant to Article 43;

(q) conduct the accreditation of a body for monitoring codes of conduct pursuant to Article 41 and of a certification body pursuant to Article 43;

(r) authorise contractual clauses and provisions referred to in Article 46(3) and provide authorisation required under regulations made under Article 47A;

(s) approve binding corporate rules pursuant to Article 47;

(sa) provide authorisation required under regulations made under Article 47A. [sch. 7 para 7(b)]

(u) keep internal records of infringements of this Regulation and of measures taken in accordance with Article 58(2); and

(v) fulfil any other tasks related to the protection of personal data.

~~2.~~

~~The Commissioner shall facilitate the submission of complaints referred to in point (f) of paragraph 1 by measures such as a complaint submission form which can also be completed electronically, without excluding other means of communication.~~ [sch. 8 para 7(b)]

3.

The performance of the Commissioner's tasks is to be free of charge for the data subject and, where applicable, for the senior responsible individual ~~data protection officer~~. [sch. 4 para 9]

~~4.~~

~~Where requests are manifestly unfounded or excessive, in particular because of their repetitive character, the Commissioner may charge a reasonable fee based on administrative costs, or refuse to act on the request. The supervisory authority shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request.~~ [s. 32(4)]

Article 58 Powers

1.

The Commissioner has all of the following investigative powers:

(a) to order the controller and the processor, ~~and, where applicable, the controller's or the processor's representative~~ to provide any information it requires for the performance of its tasks; [s. 13(2)(f)]

(b) to carry out investigations in the form of data protection audits;

(c) to carry out a review on certifications issued pursuant to Article 42(7);

(d) to notify the controller or the processor of an alleged infringement of this Regulation;

I(e) to obtain, from the controller and the processor, access to all personal data and to all information necessary for the performance of the Commissioner's tasks;

(f) to obtain access to any premises of the controller and the processor, including to any data processing equipment and means, in accordance with domestic law.

2.

The Commissioner has all of the following corrective powers:

(a) to issue warnings to a controller or processor that intended processing operations are likely to infringe provisions of this Regulation;

(b) to issue reprimands to a controller or a processor where processing operations have infringed provisions of this Regulation;

(c) to order the controller or the processor to comply with the data subject's requests to exercise his or her rights pursuant to this Regulation;

(d) to order the controller or processor to bring processing operations into compliance with the provisions of

this Regulation, where appropriate, in a specified manner and within a specified period;

(e) to order the controller to communicate a personal data breach to the data subject;

(f) to impose a temporary or definitive limitation including a ban on processing;

(g) to order the rectification or erasure of personal data or restriction of processing pursuant to Articles 16, 17 and 18 and the notification of such actions to recipients to whom the personal data have been disclosed pursuant to Article 17(2) and Article 19;

(h) to withdraw a certification or to order the certification body to withdraw a certification issued pursuant to Articles 42 and 43, or to order the certification body not to issue certification if the requirements for the certification are not or are no longer met;

(i) to impose an administrative fine pursuant to Article 83, in addition to, or instead of measures referred to in this paragraph, depending on the circumstances of each individual case;

(j) to order the suspension of data flows to a recipient in a third country or to an international organisation.

3.

The Commissioner has all of the following authorisation and advisory powers:

(a) to advise the controller in accordance with the prior consultation procedure referred to in Article 36;

(b) 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;

(d) to issue an opinion and approve draft codes of conduct pursuant to Article 40(5);

(e) to accredit certification bodies pursuant to Article 43;

(f) to issue certifications and approve criteria of certification in accordance with Article 42(5);

(g) to adopt standard data protection clauses referred to in Article 28(8) and in point (d) of Article 46(2);

(h) to authorise contractual clauses referred to in point (a) of Article 46(3);

(i) to authorise administrative arrangements referred to in point (b) of Article 46(3);

(j) to approve binding corporate rules pursuant to Article 47.

(k) to provide authorisation required under regulations made under Article 47A; [sch. 7 para 8]

3A.

In the 2018 Act, section 115(4) to (9) provide that the Commissioner's functions under this Article are subject to certain safeguards.

~~**Article 59 Activity reports**~~

~~The Commissioner shall draw up an annual report on the Commissioner's activities, which may include a list of types of infringement notified and types of measures taken in accordance with Article 58(2). The Commissioner must arrange for those reports to be laid before Parliament and send a copy to the Secretary of State. They shall be made available to the public.~~ [sch 9. para 11]

[Chapter 7 Repealed – by prior legislative change]

Chapter 8 Remedies, Liability and Penalties

~~**Article 77 Right to lodge a complaint with the Commissioner**~~
~~1.~~

~~Without prejudice to any other administrative or judicial remedy, every data subject shall have the right to lodge a complaint with the Commissioner if the data subject considers that the processing of personal data relating to him or her infringes this Regulation.~~

~~2.~~

~~The Commissioner shall inform the complainant on the progress and the outcome of the complaint including the possibility of a judicial remedy pursuant to Article 78.~~ [sch. 8 para 8]

Article 78 Right to an effective judicial remedy against the Commissioner
1.

Without prejudice to any other administrative or non-judicial remedy, each natural or legal person shall have the right to an effective judicial remedy against a legally binding decision of the Commissioner concerning them.

2.

Without prejudice to any other administrative or non-judicial remedy, each data subject shall have the right to an effective judicial remedy where the Commissioner does not handle a complaint or does not inform the data subject within three months on the progress or outcome of the complaint lodged pursuant to Article 77.

Article 79 Right to an effective judicial remedy against a controller or processor

1.

Without prejudice to any available administrative or non-judicial remedy, including the right to lodge a complaint with the Commissioner pursuant to Article 77, each data subject shall have the right to an effective judicial remedy where he or she considers that his or her rights under this Regulation have been infringed as a result of the processing of his or her personal data in non-compliance with this Regulation.

Article 80 Representation of data subjects

1.

The data subject shall have the right to mandate a body or other organisation which meets the conditions in section 187(3) and (4) of the 2018 Act to make a complaint under section 164A or 165 of the 2018 Act ~~lodge the complaint~~ on his or her behalf, to exercise the rights referred to in Articles ~~77,~~ 78 and 79 on his or her behalf, and to exercise the right to receive compensation referred to in Article 82 on his or her behalf.
[sch. 8 para 9(2)]

2.

The Secretary of State may provide that any body, organisation or association referred to in paragraph 1 of this Article, independently of a data subject's mandate, has the right to make a complaint under section 164A or 165 of the 2018 Act ~~lodge a complaint with the Commissioner~~ and to exercise the rights referred to in Articles 78

and 79 if it considers that the rights of a data subject under this Regulation have been infringed as a result of the processing. [sch. 8 para 9(3)]

3.

The Secretary of State may exercise the power under paragraph 2 of this Article only by making regulations under section 190 of the 2018 Act.

[Article 81 Repealed – by prior legislative change]

Article 82 Right to compensation and liability

1.

Any person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered.

2.

Any controller involved in processing shall be liable for the damage caused by processing which infringes this Regulation. A processor shall be liable for the damage caused by processing only where it has not complied with obligations of this Regulation specifically directed to processors or where it has acted outside or contrary to lawful instructions of the controller.

3.

A controller or processor shall be exempt from liability under paragraph 2 if it proves that it is not in any way responsible for the event giving rise to the damage.

4.

Where more than one controller or processor, or both a controller and a processor, are involved in the same processing and where they are, under paragraphs 2 and 3, responsible for any damage caused by processing, each controller or processor shall be held liable for the entire damage in order to ensure effective compensation of the data subject.

5.

Where a controller or processor has, in accordance with paragraph 4, paid full compensation for the damage suffered, that controller or processor shall be entitled to claim back from the other controllers or processors involved in the same processing that part of the compensation corresponding to their part of responsibility for the damage, in accordance with the conditions set out in paragraph 2.

Article 83 General conditions for imposing administrative fines

1.

The Commissioner shall ensure that the imposition of administrative fines pursuant to this Article in respect of infringements of this Regulation referred to in paragraphs 4, 5 and 6 shall in each individual case be effective, proportionate and dissuasive.

2.

Administrative fines shall, depending on the circumstances of each individual case, be imposed in addition to, or instead of, measures referred to in points (a) to (h) and (j) of Article 58(2). When deciding whether to impose an administrative fine and deciding on the amount of the administrative fine in each individual case due regard shall be given to the following:

(a) the nature, gravity and duration 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;

(b) the intentional or negligent character of the infringement;

(c) any action taken by the controller or processor to mitigate the damage suffered by data subjects, including any consultation under Article 36(1); [sch. 4 para 10(2)]

(d) the degree of responsibility of the controller or processor taking into account ~~technical and organisational~~ measures implemented by them pursuant to Articles 25 and 32; [sch. 4 para 10(3)]

(e) any relevant previous infringements by the controller or processor;

(f) the degree of cooperation with the Commissioner, in order to remedy the infringement and mitigate the possible adverse effects of the infringement;

(g) the categories of personal data affected by the infringement;

(h) the manner in which the infringement became known to the Commissioner, in particular whether, and if so to what extent, the controller or processor notified the infringement;

(i) where measures referred to in Article 58(2) have previously been ordered against the controller or processor concerned with regard to the same subject-matter, compliance with those measures;

(j) adherence to approved codes of conduct pursuant to Article 40 or approved certification mechanisms pursuant to Article 42; and

(k) 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.

3.

If a controller or processor intentionally or negligently, for the same or linked processing operations, infringes several provisions of this Regulation, the total amount of the administrative fine shall not exceed the amount specified for the gravest infringement.

4.

Infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to £8,700,000, or in the case of an undertaking, up to 2 % of the total worldwide annual turnover of the preceding financial year, whichever is higher:

(a) the obligations of the controller and the processor pursuant to Articles 8, 11, 25 to 36 ~~39~~ and 42 and 43; [sch. 4 para 10(4)]

(b) the obligations of the certification body pursuant to Articles 42 and 43;

(c) the obligations of the monitoring body pursuant to Article 41(4).

5.

Infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative

fines up to £17,500,000, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher:

(a) the basic principles for processing, including conditions for consent, pursuant to Articles 5, 6, 7 and 9;

(b) the data subjects' rights pursuant to Articles 12 to 22D;

(c) the transfers of personal data to a recipient in a third country or an international organisation pursuant to Articles 44A to 49; [sch. 3 para 10 and sch. 7 para 9]

(d) any obligations under Part 5 or 6 of Schedule 2 to the 2018 Act or regulations made under section 16(1)(c) of the 2018 Act;

(e) non-compliance with an order or a temporary or definitive limitation on processing or the suspension of data flows by the Commissioner pursuant to Article 58(2) or failure to provide access in violation of Article 58(1).

6.

Non-compliance with an order by the Commissioner as referred to in Article 58(2) shall, in accordance with paragraph 2 of this Article, be subject to administrative fines up to £17,500,000, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher.

10.

In the 2018 Act, section 115(9) makes provision about the exercise of the Commissioner's functions under this Article.

Article 84 Penalties

Part 6 of the 2018 Act makes further provision about penalties applicable to infringements of this Regulation.

CHAPTER 8A Safeguards for processing for research, archiving or statistical purposes

Article 84A Research, archives and statistics

1. This Chapter makes provision about the processing of personal data—

(a) for the purposes of scientific research or historical research,

(b) for the purposes of archiving in the public interest, or

(c) for statistical purposes.

2. Those purposes are referred to in this Chapter as "RAS purposes". [s. 22(2)]

Article 84B Additional requirements when processing for RAS purposes

1. Processing of personal data for RAS purposes must be carried out subject to appropriate safeguards for the rights and freedoms of the data subject.

2. Processing of personal data for RAS purposes must be carried out in a manner which does not permit the identification of a living individual.

3. Paragraph 2 does not apply—

(a) to the collection of personal data (whether from the data subject or otherwise), or

(b) to cases in which the RAS purposes cannot be fulfilled by further processing in the manner described in that paragraph.

4. For the purposes of paragraph 2, processing permits the identification of a living individual only in cases described in section 3A(2) and (3) of the 2018 Act (information relating to an identifiable living individual).

[s. 22(2)]

Article 84C Appropriate safeguards

1. This Article makes provision about when the requirement under Article 84B(1) for processing of personal data to be carried out subject to appropriate safeguards is satisfied.

2.

The requirement is not satisfied if the processing is likely to cause substantial damage or substantial distress to a data subject to whom the personal data relates.

3.

The requirement is not satisfied if the processing is carried out for the purposes of measures or decisions with respect to a particular data subject to whom the personal data relates, except where the purposes for which the processing is carried out include the purposes of approved medical research.

4.

The requirement is only satisfied if the safeguards include technical and organisational measures for the purpose of ensuring respect for the principle of data minimisation (see Article 5(1)(c)), such as, for example, pseudonymisation.

5.

In this Article—

"approved medical research" means medical research carried out by a person who has approval to carry out that research from—

(a) a research ethics committee recognised or established by the Health Research Authority

under Chapter 2 of Part 3 of the Care Act 2014, or

(b) a body appointed by any of the following for the purpose of assessing the ethics of research involving individuals—

(i) the Secretary of State, the Scottish Ministers, the Welsh Ministers or a Northern Ireland department;

(ii) a relevant NHS body;

(iii) United Kingdom Research and Innovation or a body that is a Research Council for the purposes of the Science and Technology Act 1965;

(iv) an institution that is a research institution for the purposes of Chapter 4A of Part 7 of the Income Tax (Earnings and Pensions) Act 2003 (see section 457 of that Act);

"relevant NHS body" means—

(a) an NHS trust or NHS foundation trust in England,

(b) an NHS trust or Local Health Board in Wales,

(c) a Health Board or Special Health Board constituted under section 2 of the National Health Service (Scotland) Act 1978,

(d) the Common Services Agency for the Scottish Health Service, or

(e) any of the health and social care bodies in Northern Ireland falling within paragraphs (b) to (e) of section 1(5) of the Health and Social Care (Reform) Act (Northern Ireland) 2009 (c. 1 (N.I.)). [s. 22(2)]

Article 84D Appropriate safeguards: further provision

1.

The Secretary of State may by regulations make further provision about when the requirement for appropriate safeguards under Article 84B(1) is satisfied.

2.

The power under this Article includes power to amend Article 84C by adding, varying or omitting provision, except that it does not include power—

(a) to vary or omit paragraph 1 of that Article, or

(b) to omit any of paragraphs 2 to 4 of that Article.

3.

Regulations under this Article are subject to the affirmative resolution procedure. [s. 22(2)]

Chapter 9 Provisions Relating to other Specific Processing Situations [s. 22(3)]

Article 85 Processing and freedom of expression and information

2.

For processing carried out for journalistic purposes or the purpose of academic artistic or literary expression, the Secretary of State may provide for exemptions or derogations from Chapter II (principles), Chapter III (rights of the data subject), Chapter IV (controller and processor), Chapter V (transfer of personal data to third countries or international organisations), Chapter VI (the Commissioner) and Chapter IX (specific data processing situations) if they are necessary to reconcile the right to the protection of personal data with the freedom of expression and information.

2A.

The Secretary of State may exercise the power under paragraph 2 of this Article only by making regulations under section 16 of the 2018 Act.

Article 86 Processing and public access to official documents

1.

Personal data in official documents held by a public authority or a public body or a private body for the performance of a task carried out in the public interest may be disclosed by the authority or body in accordance with domestic law to which the public authority or body is subject in order to reconcile public access to official documents with the right to the protection of personal data pursuant to this Regulation.

2.

Chapter 3 of Part 2 of the 2018 Act makes provision about the application of this Regulation to the manual unstructured processing of personal data held by an FOI public authority (as defined in Article 2).

Article 86A Processing and national security and defence

Chapter 3 of Part 2 of the 2018 Act makes provision about the application of this Regulation where processing is carried out, or exemption from a provision of this Regulation is required, for the purposes of safeguarding national security or for defence purposes.

[Articles 87, 88 Repealed – by prior legislative change]

~~**Article 89 Safeguards and derogations relating to processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes**~~

~~1.~~

~~Processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, shall be subject to appropriate safeguards, in accordance with this Regulation, for the rights and freedoms of the data subject. Those safeguards shall ensure that technical and organisational measures are in place in particular in order to ensure respect for the principle of data minimisation. Those measures may include pseudonymisation provided that those purposes can be fulfilled in that manner. Where those purposes can be fulfilled by further processing which does not permit or no longer permits the identification of data subjects, those purposes shall be fulfilled in that manner.~~

~~1A.~~

~~In the 2018 Act, section 19 makes provision about when the requirements in paragraph 1 are satisfied.~~

[s. 22(4)]

[Articles 90, 91 Repealed – by prior legislative change]

CHAPTER 9A Regulations

Article 91A Regulations made by Secretary of State

1. This Article makes provision about regulations made by the Secretary of State under this Regulation ("UK GDPR regulations").

2. Before making UK GDPR regulations, the Secretary of State must consult—

(a) the Commissioner, and

(b) such other persons as the Secretary of State considers appropriate.

3. Paragraph 2 does not apply to regulations made under Article 49 or 49A where the Secretary of State has made an urgency statement in respect of them.

4. UK GDPR regulations may—

(a) make different provision for different purposes;

(b) include consequential, supplementary, incidental, transitional, transitory or saving provision.

5. UK GDPR regulations are to be made by statutory instrument.

6. For the purposes of this Regulation, where regulations are subject to "the negative resolution procedure", the statutory instrument containing the regulations is subject to annulment in pursuance of a resolution of either House of Parliament.

7. For the purposes of this Regulation, where regulations are subject to "the affirmative resolution procedure", the regulations may not be made unless a draft of the statutory instrument containing them has been laid before Parliament and approved by a resolution of each House of Parliament.

8. For the purposes of this Regulation, where regulations are subject to "the made affirmative resolution procedure"—

(a) the statutory instrument containing the regulations must be laid before Parliament after being made, together with the urgency statement in respect of them, and

(b) the regulations cease to have effect at the end of the period of 120 days beginning with the day on which the instrument is made, unless within that period the instrument is approved by a resolution of each House of Parliament.

9. In calculating the period of 120 days, no account is to be taken of any whole days that fall within a period during which—

(a) Parliament is dissolved or prorogued, or

(b) both Houses of Parliament are adjourned for more than 4 days.

10. Where regulations cease to have effect as a result of paragraph 8, that does not—

(a) affect anything previously done under the regulations, or

(b) prevent the making of new regulations.

11. Any provision that may be included in UK GDPR regulations subject to the negative resolution procedure may be made by regulations made under this Regulation or another enactment that are subject to the affirmative resolution procedure or the made affirmative resolution procedure.

12. A requirement under this Article to consult may be satisfied by consultation before, as well as by consultation after, the provision conferring the power to make regulations comes into force.

13. In this Article, "urgency statement", in relation to regulations, means a reasoned statement that the Secretary of State considers it desirable for the regulations to come into force without delay.

[s. 44(1)]

[Chapter 10 Repealed – by prior legislative change]

Chapter 11 Final Provisions

Article 94 Repeal of Directive 95/46/EC

2.

References to Directive 95/46/EC of the European Parliament and of the Council of 24th October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (which ceased to have effect on 25th May 2018) shall be construed as references to this Regulation. References to the Working Party on the Protection of Individuals with regard to the Processing of Personal Data established by Article 29 of Directive 95/46/EC shall be construed as references to the European Data Protection Board established by the EU GDPR (as defined in section 3 of the 2018 Act).

Article 95 Relationship with Directive 2002/58/EC

This Regulation shall not impose additional obligations on natural or legal persons in relation to processing in connection with the provision of publicly available electronic communications services in public communication networks in the United Kingdom in relation to matters for which they are subject to specific obligations with the same objective set out in domestic law made before IP completion day implementing Directive 2002/58/EC of the European Parliament and of the Council of 12th July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector.

Article 96 Relationship with previously concluded Agreements

International agreements involving the transfer of personal data to third countries or international organisations which were concluded by the United Kingdom or the Commissioner prior to 24 May 2016, and which comply with domestic law as applicable prior to that date, shall remain in force until amended, replaced or revoked.

[Articles 97, 98, 99 Repealed – by prior legislative change]

Done at Brussels, 27 April 2016.

For the European Parliament
The President
M. *Schulz*
For the Council
The President
J.A. *Hennis-Plasschaert*

ANNEX 1

LAWFULNESS OF PROCESSING: RECOGNISED LEGITIMATE INTERESTS

Disclosure for purposes of processing described in Article 6(1)(e)

1.

This condition is met where—

(a) the processing is necessary for the purposes of making a disclosure of personal data to another person in response to a request from the other person, and

(b) the request states that the other person needs the personal data for the purposes of carrying out processing described in Article 6(1)(e) that has a legal basis that satisfies Article 6(3).

National security, public security and defence

2.

This condition is met where the processing is necessary—

(a) for the purposes of safeguarding national security,

(b) for the purposes of protecting public security, or

(c) for defence purposes.

Emergencies

3.

This condition is met where the processing is necessary for the purposes of responding to an emergency.

4.

In paragraph 3, "emergency" has the same meaning as in Part 2 of the Civil Contingencies Act 2004.

Crime

5.

This condition is met where the processing is necessary for the purposes of—

(a) detecting, investigating or preventing crime, or

(b) apprehending or prosecuting offenders.

Safeguarding vulnerable individuals

6.

This condition is met where the processing is necessary for the purposes of safeguarding a vulnerable individual.

7.

In paragraph 6—

"safeguarding", in relation to a vulnerable individual, means—

(a) protecting a vulnerable individual from neglect or physical, mental or emotional harm, or

(b) protecting the physical, mental or emotional well-being of a vulnerable individual;

"vulnerable individual" means an individual—

(a) aged under 18, or

(b) aged 18 or over and at risk.

8.

For the purposes of paragraph 7—
(a) protection of an individual, or of the well-being of an individual, includes both protection relating to a particular individual and protection relating to a type of individual, and
(b) an individual aged 18 or over is "at risk" if the controller has reasonable cause to suspect that the individual—
(i) has needs for care and support,
(ii) is experiencing, or at risk of, neglect or physical, mental or emotional harm, and
(iii) as a result of those needs is unable to protect themselves against the neglect, harm or risk.

Democratic engagement

9.

This condition is met where—
(a) the processing is carried out for the purposes of democratic engagement, and
(b) the data subject is aged 14 or over.

10.

For the purposes of paragraph 9, processing is carried out for the purposes of democratic engagement if—
(a) the processing—
(i) is carried out by an elected representative or a person acting with the authority of such a representative, and
(ii) is necessary for the purposes of discharging the elected representative's functions or for the purposes of the elected representative's democratic engagement activities,
(b) the processing—
(i) is carried out by a person or organisation included in a register maintained under section 23 of the Political Parties, Elections and Referendums Act 2000, and
(ii) is necessary for the purposes of the person's or organisation's democratic engagement activities, for the purposes of assisting an elected representative with their functions or democratic engagement activities or for the purposes of assisting with a candidate's campaign for election as an elected representative,
(c) the processing—
(i) is carried out by a candidate for election as an elected representative or a person acting with the authority of such a candidate, and
(ii) is necessary for the purposes of the candidate's campaign for election,
(d) the processing—
(i) is carried out by a permitted participant in relation to a referendum or a person acting with the authority of such a person, and
(ii) is necessary for the purposes of the permitted participant's campaigning in connection with the referendum, or
(e) the processing—
(i) is carried out by an accredited campaigner in relation to a recall petition or a person acting with the authority of such a person, and
(ii) is necessary for the purposes of the accredited campaigner's campaigning in connection with the recall petition.

11.

In paragraph 10—

"accredited campaigner" has the meaning given in Part 5 of Schedule 3 to the Recall of MPs Act 2015;

"candidate", in relation to election as an elected representative, has the meaning given by the

provisions listed in the relevant entry in the second column of the table in paragraph 12;

"democratic engagement activities" means activities whose purpose is to support or promote democratic engagement;

"elected representative" means a person listed in the first column of the table in paragraph 12 and see also paragraphs 13 and 14;

"permitted participant" has the same meaning as in Part 7 of the Political Parties, Elections and Referendums Act 2000 (referendums) (see section 105 of that Act);

"recall petition" has the same meaning as in the Recall of MPs Act 2015 (see section 1(2) of that Act);

"referendum" means a referendum or other poll held on one or more questions specified in, or in accordance with, an enactment.

12. This is the table referred to in paragraph 11—

Elected representative	*Candidate for election as an elected representative*
(a) a member of the House of Commons	*section 118A of the Representation of the People Act 1983*
(b) a member of the Senedd	*article 84(2) of the National Assembly for Wales (Representation of the People) Order 2007 (S.I. 2007/236)*
(c) a member of the Scottish Parliament	*article 80(1) of the Scottish Parliament (Elections etc) Order 2015 (S.S.I. 2015/425)*
(d) a member of the Northern Ireland Assembly	*section 118A of the Representation of the People Act 1983, as applied by the Northern Ireland Assembly (Elections) Order 2001 (S.I. 2001/2599)*
(e) an elected member of a local authority within the meaning of section 270(1) of the Local Government Act 1972, namely— (i) in England, a county council, a district council, a London borough council or a parish council; (ii) in Wales, a county council, a county borough council or a community council;	*section 118A of the Representation of the People Act 1983*
(f) an elected mayor of a local authority within the meaning of Part 1A or 2 of the Local Government Act 2000	*section 118A of the Representation of the People Act 1983, as applied by the Local Authorities (Mayoral Elections) (England and Wales) Regulations 2007 (S.I. 2007/1024)*
(g) a mayor for the area of a combined authority established under section 103 of the Local Democracy, Economic Development and Construction Act 2009	*section 118A of the Representation of the People Act 1983, as applied by the Combined Authorities (Mayoral Elections) Order 2017 (S.I. 2017/67)*
(h) the Mayor of London or an elected member of the London Assembly	*section 118A of the Representation of the People Act 1983*
(i) an elected member of the Common Council of the City of London	*section 118A of the Representation of the People Act 1983*
(j) an elected member of the Council of the Isles of Scilly	*section 118A of the Representation of the People Act 1983*
(k) an elected member of a council constituted under section 2 of the Local Government etc (Scotland) Act 1994	*section 118A of the Representation of the People Act 1983*
(l) an elected member of a district council within the meaning of the Local Government Act (Northern Ireland) 1972 (c. 9 (N.I.))	*section 130(3A) of the Electoral Law Act (Northern Ireland) 1962 (c. 9 (N.I.))*

(m) a police and crime commissioner	*article 3 of the Police and Crime Commissioner Elections Order 2012 (S.I. 2012/1917)*

13.

For the purposes of the definition of "elected representative" in paragraph 11, a person who is—
(a) a member of the House of Commons immediately before Parliament is dissolved,
(b) a member of the Senedd immediately before Senedd Cymru is dissolved,
(c) a member of the Scottish Parliament immediately before that Parliament is dissolved, or
(d) a member of the Northern Ireland Assembly immediately before that Assembly is dissolved,
is to be treated as if the person were such a member until the end of the fourth day after the day on which the subsequent general election in relation to that Parliament or Assembly is held.

14.

For the purposes of the definition of "elected representative" in paragraph 11, a person who is an elected member of the Common Council of the City of London and whose term of office comes to an end at the end of the day preceding the annual Wardmotes is to be treated as if the person were such a member until the end of the fourth day after the day on which those Wardmotes are held. [s. 5(6)]

ANNEX 2
PURPOSE LIMITATION: PROCESSING TO BE TREATED AS COMPATIBLE WITH ORIGINAL PURPOSE

Disclosure for purposes of processing described in Article 6(1)(e)

1. This condition is met where—
(a)
(i) the processing is necessary for the purposes of making a disclosure of personal data to another person in response to a request from the other person, and
(ii) is not carried out by a public authority in the performance of its tasks, and
(b) the request states that the other person needs the personal data for the purposes of carrying out processing that—
(i) is described in Article 6(1)(e),
(ii) has a legal basis that satisfies Article 6(3), and
(iii) is necessary to safeguard an objective listed in Article 23(1)(c) to (j).

Public security

2.

This condition is met where the processing is necessary for the purposes of protecting public security.

Emergencies

3.

This condition is met where the processing is necessary for the purposes of responding to an emergency.

4.

In paragraph 2, "emergency" has the same meaning as in Part 2 of the Civil Contingencies Act 2004.

Crime

5.

This condition is met where the processing is necessary for the purposes of—
(a) detecting, investigating or preventing crime, or

(b) apprehending or prosecuting offenders.

Protection of vital interests of data subjects and others

6.

This condition is met where the processing is necessary for the purposes of protecting the vital interests of the data subject or another individual.

Safeguarding vulnerable individuals

7.

This condition is met where the processing is necessary for the purposes of safeguarding a vulnerable individual.

8.

In paragraph 7—

"safeguarding", in relation to a vulnerable individual, means—
(a) protecting a vulnerable individual from neglect or physical, mental or emotional harm, or
(b) protecting the physical, mental or emotional well-being of a vulnerable individual;

"vulnerable individual" means an individual—
(a) aged under 18, or
(b) aged 18 or over and at risk.

9.

For the purposes of paragraph 8—
(a) protection of an individual, or of the well-being of an individual, includes both protection relating to a particular individual and protection relating to a type of individual, and
(b) an individual aged 18 or over is "at risk" if the controller has reasonable cause to suspect that the individual—
(i) has needs for care and support,
(ii) is experiencing, or at risk of, neglect or physical, mental or emotional harm, and
(iii) as a result of those needs is unable to protect themselves against the neglect, harm or risk.

Taxation

10.

This condition is met where the processing is carried out for the purposes of the assessment or collection of a tax or duty or an imposition of a similar nature.

Legal obligations

11.

This condition is met where the processing is necessary for the purposes of complying with an obligation of the controller under an enactment, a rule of law or an order of a court or tribunal.

[s. 6(6)]