Data Protection Act 2018

2018 CHAPTER 12

PART 2

GENERAL PROCESSING

CHAPTER 1

SCOPE AND DEFINITIONS

4 Processing to which this Part applies

(1) This Part is relevant to most processing of personal data.

(2) Chapter 2 of this Part—

(a) applies to the types of processing of personal data to which the GDPR applies by virtue of Article 2 of the GDPR, and

(b) supplements, and must be read with, the GDPR.

(3) Chapter 3 of this Part—

(a) applies to certain types of processing of personal data to which the GDPR does not apply (see section 21), and

(b) makes provision for a regime broadly equivalent to the GDPR to apply to such processing.

5 Definitions

(1) Terms used in Chapter 2 of this Part and in the GDPR have the same meaning in Chapter 2 as they have in the GDPR.

(2) In subsection (1), the reference to a term's meaning in the GDPR is to its meaning in the GDPR read with any provision of Chapter 2 which modifies the term's meaning for the purposes of the GDPR.

(3) Subsection (1) is subject to any provision in Chapter 2 which provides expressly for the term to have a different meaning and to section 204.

(4) Terms used in Chapter 3 of this Part and in the applied GDPR have the same meaning in Chapter 3 as they have in the applied GDPR.

(5) In subsection (4), the reference to a term's meaning in the applied GDPR is to its meaning in the GDPR read with any provision of Chapter 2 (as applied by Chapter 3) or Chapter 3 which modifies the term's meaning for the purposes of the applied GDPR.

(6) Subsection (4) is subject to any provision in Chapter 2 (as applied by Chapter 3) or Chapter 3 which provides expressly for the term to have a different meaning.

(7) A reference in Chapter 2 or Chapter 3 of this Part to the processing of personal data is to processing to which the Chapter applies.

(8) Sections 3 and 205 include definitions of other expressions used in this Part.

CHAPTER 2

THE GDPR

Meaning of certain terms used in the GDPR

6 Meaning of "controller"

(1) The definition of "controller" in Article 4(7) of the GDPR has effect subject to—

(a) subsection (2),

(b) section 209, and

(c) section 210.

(2) For the purposes of the GDPR, where personal data is processed only—

(a) for purposes for which it is required by an enactment to be processed, and

(b) by means by which it is required by an enactment to be processed,

the person on whom the obligation to process the data is imposed by the enactment (or, if different, one of the enactments) is the controller.

7 Meaning of "public authority" and "public body"

(1) For the purposes of the GDPR, the following (and only the following) are "public authorities" and "public bodies" under the law of the United Kingdom—

(a) a public authority as defined by the Freedom of Information Act 2000,

(b) a Scottish public authority as defined by the Freedom of Information (Scotland) Act 2002 (asp 13), and

(c) an authority or body specified or described by the Secretary of State in regulations,

subject to subsections (2), (3) and (4).

(2) An authority or body that falls within subsection (1) is only a "public authority" or "public body" for the purposes of the GDPR when performing a task carried out in the public interest or in the exercise of official authority vested in it.

(3) The references in subsection (1)(a) and (b) to public authorities and Scottish public authorities as defined by the Freedom of Information Act 2000 and the Freedom of Information (Scotland) Act 2002 (asp 13) do not include any of the following that fall within those definitions—

(a) a parish council in England;

(b) a community council in Wales;

(c) a community council in Scotland;

(d) a parish meeting constituted under section 13 of the Local Government Act 1972;

(e) a community meeting constituted under section 27 of that Act;

(f) charter trustees constituted—

(i) under section 246 of that Act,

(ii) under Part 1 of the Local Government and Public Involvement in Health Act 2007, or

(iii) by the Charter Trustees Regulations 1996 (S.I. 1996/263).

(4) The Secretary of State may by regulations provide that a person specified or described in the regulations that is a public authority described in subsection (1)(a) or (b) is not a "public authority" or "public body" for the purposes of the GDPR.

(5) Regulations under this section are subject to the affirmative resolution procedure.

Lawfulness of processing

8 Lawfulness of processing: public interest etc

In Article 6(1) of the GDPR (lawfulness of processing), the reference in point (e) to processing of personal data that is necessary for the performance of a task carried out in the public interest or in the exercise of the controller's official authority includes processing of personal data that is necessary for—

(a) the administration of justice,

(b) the exercise of a function of either House of Parliament,

(c) the exercise of a function conferred on a person by an enactment or rule of law,

(d) the exercise of a function of the Crown, a Minister of the Crown or a government department, or

(e) an activity that supports or promotes democratic engagement.

9 Child's consent in relation to information society services

In Article 8(1) of the GDPR (conditions applicable to child's consent in relation to information society services)—

(a) references to "16 years" are to be read as references to "13 years", and

(b) the reference to "information society services" does not include preventive or counselling services.

Special categories of personal data

10 Special categories of personal data and criminal convictions etc data

(1) Subsections (2) and (3) make provision about the processing of personal data described in Article 9(1) of the GDPR (prohibition on processing of special categories of personal data) in reliance on an exception in one of the following points of Article 9(2)—

(a) point (b) (employment, social security and social protection);

(b) point (g) (substantial public interest);

(c) point (h) (health and social care);

(d) point (i) (public health);

(e) point (j) (archiving, research and statistics).

(2) The processing meets the requirement in point (b), (h), (i) or (j) of Article 9(2) of the GDPR for authorisation by, or a basis in, the law of the United Kingdom or a part of the United Kingdom only if it meets a condition in Part 1 of Schedule 1.

(3) The processing meets the requirement in point (g) of Article 9(2) of the GDPR for a basis in the law of the United Kingdom or a part of the United Kingdom only if it meets a condition in Part 2 of Schedule 1.

(4) Subsection (5) makes provision about the processing of personal data relating to criminal convictions and offences or related security measures that is not carried out under the control of official authority.

(5) The processing meets the requirement in Article 10 of the GDPR for authorisation by the law of the United Kingdom or a part of the United Kingdom only if it meets a condition in Part 1, 2 or 3 of Schedule 1.

(6) The Secretary of State may by regulations—

(a) amend Schedule 1—

(i) by adding or varying conditions or safeguards, and

(ii) by omitting conditions or safeguards added by regulations under this section, and

(b) consequentially amend this section.

(7) Regulations under this section are subject to the affirmative resolution procedure.

11 Special categories of personal data etc: supplementary

(1) For the purposes of Article 9(2)(h) of the GDPR (processing for health or social care purposes etc), the circumstances in which the processing of personal data is carried out subject to the conditions and safeguards referred to in Article 9(3) of the GDPR (obligation of secrecy) include circumstances in which it is carried out—

(a) by or under the responsibility of a health professional or a social work professional, or

(b) by another person who in the circumstances owes a duty of confidentiality under an enactment or rule of law.

(2) In Article 10 of the GDPR and section 10, references to personal data relating to criminal convictions and offences or related security measures include personal data relating to—

(a) the alleged commission of offences by the data subject, or

(b) proceedings for an offence committed or alleged to have been committed by the data subject or the disposal of such proceedings, including sentencing.

Rights of the data subject

12 Limits on fees that may be charged by controllers

(1) The Secretary of State may by regulations specify limits on the fees that a controller may charge in reliance on—

(a) Article 12(5) of the GDPR (reasonable fees when responding to manifestly unfounded or excessive requests), or

(b) Article 15(3) of the GDPR (reasonable fees for provision of further copies).

(2) The Secretary of State may by regulations—

(a) require controllers of a description specified in the regulations to produce and publish guidance about the fees that they charge in reliance on those provisions, and

(b) specify what the guidance must include.

(3) Regulations under this section are subject to the negative resolution procedure.

13 Obligations of credit reference agencies

(1) This section applies where a controller is a credit reference agency (within the meaning of section 145(8) of the Consumer Credit Act 1974).

(2) The controller's obligations under Article 15(1) to (3) of the GDPR (confirmation of processing, access to data and safeguards for third country transfers) are taken to apply only to personal data relating to the data subject's financial standing, unless the data subject has indicated a contrary intention.

(3) Where the controller discloses personal data in pursuance of Article 15(1) to (3) of the GDPR, the disclosure must be accompanied by a statement informing the data subject of the data subject's rights under section 159 of the Consumer Credit Act 1974 (correction of wrong information).

14 Automated decision-making authorised by law: safeguards

(1) This section makes provision for the purposes of Article 22(2)(b) of the GDPR (exception from Article 22(1) of the GDPR for significant decisions based solely on automated processing that are authorised by law and subject to safeguards for the data subject's rights, freedoms and legitimate interests).

(2) A decision is a "significant decision" for the purposes of this section if, in relation to a data subject, it—

(a) produces legal effects concerning the data subject, or

(b) similarly significantly affects the data subject.

(3) A decision is a "qualifying significant decision" for the purposes of this section if—

(a) it is a significant decision in relation to a data subject,

(b) it is required or authorised by law, and

(c) it does not fall within Article 22(2)(a) or (c) of the GDPR (decisions necessary to a contract or made with the data subject's consent).

(4) Where a controller takes a qualifying significant decision in relation to a data subject based solely on automated processing—

(a) the controller must, as soon as reasonably practicable, notify the data subject in writing that a decision has been taken based solely on automated processing, and

(b) the data subject may, before the end of the period of 1 month beginning with receipt of the notification, request the controller to—

(i) reconsider the decision, or

(ii) take a new decision that is not based solely on automated processing.

(5) If a request is made to a controller under subsection (4), the controller must, within the period described in Article 12(3) of the GDPR—

(a) consider the request, including any information provided by the data subject that is relevant to it,

(b) comply with the request, and

(c) by notice in writing inform the data subject of—

(i) the steps taken to comply with the request, and

(ii) the outcome of complying with the request.

(6) In connection with this section, a controller has the powers and obligations under Article 12 of the GDPR (transparency, procedure for extending time for acting on request, fees, manifestly unfounded or excessive requests etc) that apply in connection with Article 22 of the GDPR.

(7) The Secretary of State may by regulations make such further provision as the Secretary of State considers appropriate to provide suitable measures to safeguard a data subject's rights, freedoms and legitimate interests in connection with the taking of qualifying significant decisions based solely on automated processing.

(8) Regulations under subsection (7)—

(a) may amend this section, and

(b) are subject to the affirmative resolution procedure.

Restrictions on data subject's rights

15 Exemptions etc

(1) Schedules 2, 3 and 4 make provision for exemptions from, and restrictions and adaptations of the application of, rules of the GDPR.

(2) In Schedule 2—

(a) Part 1 makes provision adapting or restricting the application of rules contained in Articles 13 to 21 and 34 of the GDPR in specified circumstances, as allowed for by Article 6(3) and Article 23(1) of the GDPR;

(b) Part 2 makes provision restricting the application of rules contained in Articles 13 to 21 and 34 of the GDPR in specified circumstances, as allowed for by Article 23(1) of the GDPR;

(c) Part 3 makes provision restricting the application of Article 15 of the GDPR where this is necessary to protect the rights of others, as allowed for by Article 23(1) of the GDPR;

(d) Part 4 makes provision restricting the application of rules contained in Articles 13 to 15 of the GDPR in specified circumstances, as allowed for by Article 23(1) of the GDPR;

(e) Part 5 makes provision containing exemptions or derogations from Chapters II, III, IV, V and VII of the GDPR for reasons relating to freedom of expression, as allowed for by Article 85(2) of the GDPR;

(f) Part 6 makes provision containing derogations from rights contained in Articles 15, 16, 18, 19, 20 and 21 of the GDPR for scientific or historical research purposes, statistical purposes and archiving purposes, as allowed for by Article 89(2) and (3) of the GDPR.

(3) Schedule 3 makes provision restricting the application of rules contained in Articles 13 to 21 of the GDPR to health, social work, education and child abuse data, as allowed for by Article 23(1) of the GDPR.

(4) Schedule 4 makes provision restricting the application of rules contained in Articles 13 to 21 of the GDPR to information the disclosure of which is prohibited or restricted by an enactment, as allowed for by Article 23(1) of the GDPR.

(5) In connection with the safeguarding of national security and with defence, see Chapter 3 of this Part and the exemption in section 26.

16 Power to make further exemptions etc by regulations

(1) The following powers to make provision altering the application of the GDPR may be exercised by way of regulations made by the Secretary of State under this section—

(a) the power in Article 6(3) for Member State law to lay down a legal basis containing specific provisions to adapt the application of rules of the GDPR where processing is necessary for compliance with a legal obligation, for the performance of a task in the public interest or in the exercise of official authority;

(b) the power in Article 23(1) to make a legislative measure restricting the scope of the obligations and rights mentioned in that Article where necessary and proportionate to safeguard certain objectives of general public interest;

(c) the power in Article 85(2) to provide for exemptions or derogations from certain Chapters of the GDPR where necessary to reconcile the protection of personal data with the freedom of expression and information.

(2) Regulations under this section may—

(a) amend Schedules 2 to 4—

(i) by adding or varying provisions, and

(ii) by omitting provisions added by regulations under this section, and

(b) consequentially amend section 15.

(3) Regulations under this section are subject to the affirmative resolution procedure.

Accreditation of certification providers

17 Accreditation of certification providers

(1) Accreditation of a person as a certification provider is only valid when carried out by—

(a) the Commissioner, or

(b) the national accreditation body.

(2) The Commissioner may only accredit a person as a certification provider where the Commissioner—

(a) has published a statement that the Commissioner will carry out such accreditation, and

(b) has not published a notice withdrawing that statement.

(3) The national accreditation body may only accredit a person as a certification provider where the Commissioner—

(a) has published a statement that the body may carry out such accreditation, and

(b) has not published a notice withdrawing that statement.

(4) The publication of a notice under subsection (2)(b) or (3)(b) does not affect the validity of any accreditation carried out before its publication.

(5) Schedule 5 makes provision about reviews of, and appeals from, a decision relating to accreditation of a person as a certification provider.

(6) The national accreditation body may charge a reasonable fee in connection with, or incidental to, the carrying out of the body's functions under this section, Schedule 5 and Article 43 of the GDPR.

(7) The national accreditation body must provide the Secretary of State with such information relating to its functions under this section, Schedule 5 and Article 43 of the GDPR as the Secretary of State may reasonably require.

(8) In this section—

"certification provider" means a person who issues certification for the purposes of Article 42 of the GDPR;

"the national accreditation body" means the national accreditation body for the purposes of Article 4(1) of Regulation (EC) No 765/2008 of the European Parliament and of the Council of 9 July 2008 setting out the requirements for accreditation and market surveillance relating to the marketing of products and repealing Regulation (EEC) No 339/93.

Transfers of personal data to third countries etc

18 Transfers of personal data to third countries etc

(1) The Secretary of State may by regulations specify, for the purposes of Article 49(1)(d) of the GDPR—

(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.

(2) 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 authorised by an adequacy decision under Article 45(3) of the GDPR, and

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

(3) Regulations under this section—

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

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

(4) For the purposes of this section, an urgency statement is a reasoned statement that the Secretary of State considers it desirable for the regulations to come into force without delay.

Specific processing situations

19 Processing for archiving, research and statistical purposes: safeguards

(1) This section makes provision about—

(a) processing of personal data that is necessary for archiving purposes in the public interest,

(b) processing of personal data that is necessary for scientific or historical research purposes, and

(c) processing of personal data that is necessary for statistical purposes.

(2) Such processing does not satisfy the requirement in Article 89(1) of the GDPR for the processing to be subject to appropriate safeguards for the rights and freedoms of the data subject if it is likely to cause substantial damage or substantial distress to a data subject.

(3) Such processing does not satisfy that requirement if the processing is carried out for the purposes of measures or decisions with respect to a particular data subject, unless the purposes for which the processing is necessary include the purposes of approved medical research.

(4) In this section—

"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 (a) to (e) of section 1(5) of the Health and Social Care (Reform) Act (Northern Ireland) 2009 (c. 1 (N.I.)).

(5) The Secretary of State may by regulations change the meaning of "approved medical research" for the purposes of this section, including by amending subsection (4).

(6) Regulations under subsection (5) are subject to the affirmative resolution procedure.

Minor definition

20 Meaning of "court"

Section 5(1) (terms used in this Chapter to have the same meaning as in the GDPR) does not apply to references in this Chapter to a court and, accordingly, such references do not include a tribunal.

CHAPTER 3

OTHER GENERAL PROCESSING

Scope

21 Processing to which this Chapter applies

(1) This Chapter applies to the automated or structured processing of personal data in the course of—

(a) an activity which is outside the scope of European Union law, or

(b) an activity which falls within the scope of Article 2(2)(b) of the GDPR (common foreign and security policy activities),

provided that the processing is not processing by a competent authority for any of the law enforcement purposes (as defined in Part 3) or processing to which Part 4 (intelligence services processing) applies.

(2) This Chapter also applies to the manual unstructured processing of personal data held by an FOI public authority.

(3) This Chapter does not apply to the processing of personal data by an individual in the course of a purely personal or household activity.

(4) In this section—

"the automated or structured processing of personal data" means—

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

(b) 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;

"the manual unstructured processing of personal data" means the processing of personal data which is not the automated or structured processing of personal data.

(5) In this Chapter, "FOI public authority" means—

(a) a public authority as defined in the Freedom of Information Act 2000, or

(b) a Scottish public authority as defined in the Freedom of Information (Scotland) Act 2002 (asp 13).

(6) References in this Chapter to personal data "held" by an FOI public authority are to be interpreted—

(a) in relation to England and Wales and Northern Ireland, in accordance with section 3(2) of the Freedom of Information Act 2000, and

(b) in relation to Scotland, in accordance with section 3(2), (4) and (5) of the Freedom of Information (Scotland) Act 2002 (asp 13),

but such references do not include information held by an intelligence service (as defined in section 82) on behalf of an FOI public authority.

(7) But personal data is not to be treated as "held" by an FOI public authority for the purposes of this Chapter, where—

(a) section 7 of the Freedom of Information Act 2000 prevents Parts 1 to 5 of that Act from applying to the personal data, or

(b) section 7(1) of the Freedom of Information (Scotland) Act 2002 (asp 13) prevents that Act from applying to the personal data.

Application of the GDPR

22 Application of the GDPR to processing to which this Chapter applies

(1) The GDPR applies to the processing of personal data to which this Chapter applies but as if its Articles were part of an Act extending to England and Wales, Scotland and Northern Ireland.

(2) Chapter 2 of this Part applies for the purposes of the applied GDPR as it applies for the purposes of the GDPR.

(3) In this Chapter, "the applied Chapter 2 " means Chapter 2 of this Part as applied by this Chapter.

(4) Schedule 6 contains provision modifying—

(a) the GDPR as it applies by virtue of subsection (1) (see Part 1);

(b) Chapter 2 of this Part as it applies by virtue of subsection (2) (see Part 2).

(5) A question as to the meaning or effect of a provision of the applied GDPR, or the applied Chapter 2 , is to be determined consistently with the interpretation of the equivalent provision of the GDPR, or Chapter 2 of this Part, as it applies otherwise than by virtue of this Chapter, except so far as Schedule 6 requires a different interpretation.

23 Power to make provision in consequence of regulations related to the GDPR

(1) The Secretary of State may by regulations make provision in connection with the processing of personal data to which this Chapter applies which is equivalent to that made by GDPR regulations, subject to such modifications as the Secretary of State considers appropriate.

(2) In this section, "GDPR regulations" means regulations made under section 2(2) of the European Communities Act 1972 which make provision relating to the GDPR.

(3) Regulations under subsection (1) may apply a provision of GDPR regulations, with or without modification.

(4) Regulations under subsection (1) may amend or repeal a provision of—

(a) the applied GDPR;

(b) this Chapter;

(c) Parts 5 to 7, in so far as they apply in relation to the applied GDPR.

(5) Regulations under this section are subject to the affirmative resolution procedure.

Exemptions etc

24 Manual unstructured data held by FOI public authorities

(1) The provisions of the applied GDPR and this Act listed in subsection (2) do not apply to personal data to which this Chapter applies by virtue of section 21(2) (manual unstructured personal data held by FOI public authorities).

(2) Those provisions are—

(a) in Chapter II of the applied GDPR (principles)—

(i) Article 5(1)(a) to (c), (e) and (f) (principles relating to processing, other than the accuracy principle),

(ii) Article 6 (lawfulness),

(iii) Article 7 (conditions for consent),

(iv) Article 8(1) and (2) (child's consent),

(v) Article 9 (processing of special categories of personal data),

(vi) Article 10 (data relating to criminal convictions etc), and

(vii) Article 11(2) (processing not requiring identification);

(b) in Chapter III of the applied GDPR (rights of the data subject)—

(i) Article 13(1) to (3) (personal data collected from data subject: information to be provided),

(ii) Article 14(1) to (4) (personal data collected other than from data subject: information to be provided),

(iii) Article 20 (right to data portability), and

(iv) Article 21(1) (objections to processing);

(c) in Chapter V of the applied GDPR, Articles 44 to 49 (transfers of personal data to third countries or international organisations);

(d) sections 170 and 171 of this Act;

(see also paragraph 1(2) of Schedule 18).

(3) In addition, the provisions of the applied GDPR listed in subsection (4) do not apply to personal data to which this Chapter applies by virtue of section 21(2) where the personal data relates to appointments, removals, pay, discipline, superannuation or other personnel matters in relation to—

(a) service in any of the armed forces of the Crown;

(b) service in any office or employment under the Crown or under any public authority;

(c) service in any office or employment, or under any contract for services, in respect of which power to take action, or to determine or approve the action taken, in such matters is vested in—

(i) Her Majesty,

(ii) a Minister of the Crown,

(iii) the National Assembly for Wales,

(iv) the Welsh Ministers,

(v) a Northern Ireland Minister (within the meaning of the Freedom of Information Act 2000), or

(vi) an FOI public authority.

(4) Those provisions are—

(a) the remaining provisions of Chapters II and III (principles and rights of the data subject);

(b) Chapter IV (controller and processor);

(c) Chapter IX (specific processing situations).

(5) A controller is not obliged to comply with Article 15(1) to (3) of the applied GDPR (right of access by the data subject) in relation to personal data to which this Chapter applies by virtue of section 21(2) if—

(a) the request under that Article does not contain a description of the personal data, or

(b) the controller estimates that the cost of complying with the request so far as relating to the personal data would exceed the appropriate maximum.

(6) Subsection (5)(b) does not remove the controller's obligation to confirm whether or not personal data concerning the data subject is being processed unless the estimated cost of complying with that obligation alone in relation to the personal data would exceed the appropriate maximum.

(7) An estimate for the purposes of this section must be made in accordance with regulations under section 12(5) of the Freedom of Information Act 2000.

(8) In subsections (5) and (6), "the appropriate maximum" means the maximum amount specified by the Secretary of State by regulations.

(9) Regulations under subsection (8) are subject to the negative resolution procedure.

25 Manual unstructured data used in longstanding historical research

(1) The provisions of the applied GDPR listed in subsection (2) do not apply to personal data to which this Chapter applies by virtue of section 21(2) (manual unstructured personal data held by FOI public authorities) at any time when—

(a) the personal data—

(i) is subject to processing which was already underway immediately before 24 October 1998, and

(ii) is processed only for the purposes of historical research, and

(b) the processing is not carried out—

(i) for the purposes of measures or decisions with respect to a particular data subject, or

(ii) in a way that causes, or is likely to cause, substantial damage or substantial distress to a data subject.

(2) Those provisions are—

(a) in Chapter II of the applied GDPR (principles), Article 5(1)(d) (the accuracy principle), and

(b) in Chapter III of the applied GDPR (rights of the data subject)—

(i) Article 16 (right to rectification), and

(ii) Article 17(1) and (2) (right to erasure).

(3) The exemptions in this section apply in addition to the exemptions in section 24.

26 National security and defence exemption

(1) A provision of the applied GDPR or this Act mentioned in subsection (2) does not apply to personal data to which this Chapter applies if exemption from the provision is required for—

(a) the purpose of safeguarding national security, or

(b) defence purposes.

(2) The provisions are—

(a) Chapter II of the applied GDPR (principles) except for—

(i) Article 5(1)(a) (lawful, fair and transparent processing), so far as it requires processing of personal data to be lawful;

(ii) Article 6 (lawfulness of processing);

(iii) Article 9 (processing of special categories of personal data);

(b) Chapter III of the applied GDPR (rights of data subjects);

(c) in Chapter IV of the applied GDPR—

(i) Article 33 (notification of personal data breach to the Commissioner);

(ii) Article 34 (communication of personal data breach to the data subject);

(d) Chapter V of the applied GDPR (transfers of personal data to third countries or international organisations);

(e) in Chapter VI of the applied GDPR—

(i) Article 57(1)(a) and (h) (Commissioner's duties to monitor and enforce the applied GDPR and to conduct investigations);

(ii) Article 58 (investigative, corrective, authorisation and advisory powers of Commissioner);

(f) Chapter VIII of the applied GDPR (remedies, liabilities and penalties) except for—

(i) Article 83 (general conditions for imposing administrative fines);

(ii) Article 84 (penalties);

(g) in Part 5 of this Act—

(i) in section 115 (general functions of the Commissioner), subsections (3) and (8);

(ii) in section 115, subsection (9), so far as it relates to Article 58(2)(i) of the applied GDPR;

(iii) section 119 (inspection in accordance with international obligations);

(h) in Part 6 of this Act—

(i) sections 142 to 154 and Schedule 15 (Commissioner's notices and powers of entry and inspection);

(ii) sections 170 to 173 (offences relating to personal data);

(i) in Part 7 of this Act, section 187 (representation of data subjects).

27 National security: certificate

(1) Subject to subsection (3), a certificate signed by a Minister of the Crown certifying that exemption from all or any of the provisions listed in section 26(2) is, or at any time was, required in relation to any personal data for the purpose of safeguarding national security is conclusive evidence of that fact.

(2) A certificate under subsection (1)—

(a) may identify the personal data to which it applies by means of a general description, and

(b) may be expressed to have prospective effect.

(3) Any person directly affected by a certificate under subsection (1) may appeal to the Tribunal against the certificate.

(4) If, on an appeal under subsection (3), the Tribunal finds that, applying the principles applied by a court on an application for judicial review, the Minister did not have reasonable grounds for issuing a certificate, the Tribunal may—

(a) allow the appeal, and

(b) quash the certificate.

(5) Where, in any proceedings under or by virtue of the applied GDPR or this Act, it is claimed by a controller that a certificate under subsection (1) which identifies the personal data to which it applies by means of a general description applies to any personal data, another party to the proceedings may appeal to the Tribunal on the ground that the certificate does not apply to the personal data in question.

(6) But, subject to any determination under subsection (7), the certificate is to be conclusively presumed so to apply.

(7) On an appeal under subsection (5), the Tribunal may determine that the certificate does not so apply.

(8) A document purporting to be a certificate under subsection (1) is to be—

(a) received in evidence, and

(b) deemed to be such a certificate unless the contrary is proved.

(9) A document which purports to be certified by or on behalf of a Minister of the Crown as a true copy of a certificate issued by that Minister under subsection (1) is—

(a) in any legal proceedings, evidence of that certificate;

(b) in any legal proceedings in Scotland, sufficient evidence of that certificate.

(10) The power conferred by subsection (1) on a Minister of the Crown is exercisable only by—

(a) a Minister who is a member of the Cabinet, or

(b) the Attorney General or the Advocate General for Scotland.

28 National security and defence: modifications to Articles 9 and 32 of the applied GDPR

(1) Article 9(1) of the applied GDPR (prohibition on processing of special categories of personal data) does not prohibit the processing of personal data to which this Chapter applies to the extent that the processing is carried out—

(a) for the purpose of safeguarding national security or for defence purposes, and

(b) with appropriate safeguards for the rights and freedoms of data subjects.

(2) Article 32 of the applied GDPR (security of processing) does not apply to a controller or processor to the extent that the controller or the processor (as the case may be) is processing personal data to which this Chapter applies for—

(a) the purpose of safeguarding national security, or

(b) defence purposes.

(3) Where Article 32 of the applied GDPR does not apply, the controller or the processor must implement security measures appropriate to the risks arising from the processing of the personal data.

(4) For the purposes of subsection (3), where the processing of personal data is carried out wholly or partly by automated means, the controller or the processor must, following an evaluation of the risks, implement measures designed to—

(a) prevent unauthorised processing or unauthorised interference with the systems used in connection with the processing,

(b) ensure that it is possible to establish the precise details of any processing that takes place,

(c) ensure that any systems used in connection with the processing function properly and may, in the case of interruption, be restored, and

(d) ensure that stored personal data cannot be corrupted if a system used in connection with the processing malfunctions.