Data Protection Act 2018

2018 CHAPTER 12

PART 2

GENERAL PROCESSING

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.