



Data Protection Act 2018

2018 CHAPTER 12

PART 2

GENERAL PROCESSING

CHAPTER 3

OTHER GENERAL PROCESSING

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),

Status: This is the original version (as it was originally enacted).

- (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—

Status: This is the original version (as it was originally enacted).

- (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.