Data Protection Act 2018

2018 CHAPTER 12

PART 4

INTELLIGENCE SERVICES PROCESSING

VALID FROM 25/05/2018

CHAPTER 1

SCOPE AND DEFINITIONS

Scope

82 Processing to which this Part applies

(1) This Part applies to—

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

(b) the processing by an intelligence service 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.

(2) In this Part, "intelligence service" means—

(a) the Security Service;

(b) the Secret Intelligence Service;

(c) the Government Communications Headquarters.

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

Definitions

83 Meaning of "controller" and "processor"

(1) In this Part, "controller" means the intelligence service which, alone or jointly with others—

(a) determines the purposes and means of the processing of personal data, or

(b) is the controller by virtue of subsection (2).

(2) 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 intelligence service on which the obligation to process the data is imposed by the enactment (or, if different, one of the enactments) is the controller.

(3) In this Part, "processor" means any person who processes personal data on behalf of the controller (other than a person who is an employee of the controller).

84 Other definitions

(1) This section defines other expressions used in this Part.

(2) "Consent", in relation to the processing of personal data relating to an individual, means a freely given, specific, informed and unambiguous indication of the individual's wishes by which the individual, by a statement or by a clear affirmative action, signifies agreement to the processing of the personal data.

(3) "Employee", in relation to any person, includes an individual who holds a position (whether paid or unpaid) under the direction and control of that person.

(4) "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.

(5) "Recipient", in relation to any personal data, means any person to whom the data is disclosed, whether a third party or not, but it does not include a person to whom disclosure is or may be made in the framework of a particular inquiry in accordance with the law.

(6) "Restriction of processing" means the marking of stored personal data with the aim of limiting its processing for the future.

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

CHAPTER 2

PRINCIPLES

VALID FROM 25/05/2018

Overview

85 Overview

(1) This Chapter sets out the six data protection principles as follows—

(a) section 86 sets out the first data protection principle (requirement that processing be lawful, fair and transparent);

(b) section 87 sets out the second data protection principle (requirement that the purposes of processing be specified, explicit and legitimate);

(c) section 88 sets out the third data protection principle (requirement that personal data be adequate, relevant and not excessive);

(d) section 89 sets out the fourth data protection principle (requirement that personal data be accurate and kept up to date);

(e) section 90 sets out the fifth data protection principle (requirement that personal data be kept for no longer than is necessary);

(f) section 91 sets out the sixth data protection principle (requirement that personal data be processed in a secure manner).

(2) Each of sections 86, 87 and 91 makes provision to supplement the principle to which it relates.

The data protection principles

86 The first data protection principle

(1) The first data protection principle is that the processing of personal data must be—

(a) lawful, and

(b) fair and transparent.

(2) The processing of personal data is lawful only if and to the extent that—

(a) at least one of the conditions in Schedule 9 is met, and

(b) in the case of sensitive processing, at least one of the conditions in Schedule 10 is also met.

(3) The Secretary of State may by regulations amend Schedule 10—

(a) by adding conditions;

(b) by omitting conditions added by regulations under paragraph (a).

(4) Regulations under subsection (3) are subject to the affirmative resolution procedure.

(5) In determining whether the processing of personal data is fair and transparent, regard is to be had to the method by which it is obtained.

(6) For the purposes of subsection (5), data is to be treated as obtained fairly and transparently if it consists of information obtained from a person who—

(a) is authorised by an enactment to supply it, or

(b) is required to supply it by an enactment or by an international obligation of the United Kingdom.

(7) In this section, "sensitive processing" means—

(a) the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership;

(b) the processing of genetic data for the purpose of uniquely identifying an individual;

(c) the processing of biometric data for the purpose of uniquely identifying an individual;

(d) the processing of data concerning health;

(e) the processing of data concerning an individual's sex life or sexual orientation;

(f) the processing of personal data as to—

(i) the commission or alleged commission of an offence by an individual, or

(ii) proceedings for an offence committed or alleged to have been committed by an individual, the disposal of such proceedings or the sentence of a court in such proceedings.

Commencement Information

I1 S. 86 in force at Royal Assent for specified purposes, see s. 212(2)(f)

VALID FROM 25/05/2018

87 The second data protection principle

(1) The second data protection principle is that—

(a) the purpose for which personal data is collected on any occasion must be specified, explicit and legitimate, and

(b) personal data so collected must not be processed in a manner that is incompatible with the purpose for which it is collected.

(2) Paragraph (b) of the second data protection principle is subject to subsections (3) and (4).

(3) Personal data collected by a controller for one purpose may be processed for any other purpose of the controller that collected the data or any purpose of another controller provided that—

(a) the controller is authorised by law to process the data for that purpose, and

(b) the processing is necessary and proportionate to that other purpose.

(4) Processing of personal data is to be regarded as compatible with the purpose for which it is collected if the processing—

(a) consists of—

(i) processing for archiving purposes in the public interest,

(ii) processing for the purposes of scientific or historical research, or

(iii) processing for statistical purposes, and

(b) is subject to appropriate safeguards for the rights and freedoms of the data subject.

VALID FROM 25/05/2018

88 The third data protection principle

The third data protection principle is that personal data must be adequate, relevant and not excessive in relation to the purpose for which it is processed.

VALID FROM 25/05/2018

89 The fourth data protection principle

The fourth data protection principle is that personal data undergoing processing must be accurate and, where necessary, kept up to date.

VALID FROM 25/05/2018

90 The fifth data protection principle

The fifth data protection principle is that personal data must be kept for no longer than is necessary for the purpose for which it is processed.

VALID FROM 25/05/2018

91 The sixth data protection principle

(1) The sixth data protection principle is that personal data must be processed in a manner that includes taking appropriate security measures as regards risks that arise from processing personal data.

(2) The risks referred to in subsection (1) include (but are not limited to) accidental or unauthorised access to, or destruction, loss, use, modification or disclosure of, personal data.

CHAPTER 3

RIGHTS OF THE DATA SUBJECT

VALID FROM 25/05/2018

Overview

92 Overview

(1) This Chapter sets out the rights of the data subject as follows—

(a) section 93 deals with the information to be made available to the data subject;

(b) sections 94 and 95 deal with the right of access by the data subject;

(c) sections 96 and 97 deal with rights in relation to automated processing;

(d) section 98 deals with the right to information about decision-making;

(e) section 99 deals with the right to object to processing;

(f) section 100 deals with rights to rectification and erasure of personal data.

(2) In this Chapter, "the controller", in relation to a data subject, means the controller in relation to personal data relating to the data subject.

Rights

VALID FROM 16/09/2019

93 Right to information

(1) The controller must give a data subject the following information—

(a) the identity and the contact details of the controller;

(b) the legal basis on which, and the purposes for which, the controller processes personal data;

(c) the categories of personal data relating to the data subject that are being processed;

(d) the recipients or the categories of recipients of the personal data (if applicable);

(e) the right to lodge a complaint with the Commissioner and the contact details of the Commissioner;

(f) how to exercise rights under this Chapter;

(g) any other information needed to secure that the personal data is processed fairly and transparently.

(2) The controller may comply with subsection (1) by making information generally available, where the controller considers it appropriate to do so.

(3) The controller is not required under subsection (1) to give a data subject information that the data subject already has.

(4) Where personal data relating to a data subject is collected by or on behalf of the controller from a person other than the data subject, the requirement in subsection (1) has effect, in relation to the personal data so collected, with the following exceptions—

(a) the requirement does not apply in relation to processing that is authorised by an enactment;

(b) the requirement does not apply in relation to the data subject if giving the information to the data subject would be impossible or involve disproportionate effort.

94 Right of access

(1) An individual is entitled to obtain from a controller—

(a) confirmation as to whether or not personal data concerning the individual is being processed, and

(b) where that is the case—

(i) communication, in intelligible form, of the personal data of which that individual is the data subject, and

(ii) the information set out in subsection (2).

(2) That information is—

(a) the purposes of and legal basis for the processing;

(b) the categories of personal data concerned;

(c) the recipients or categories of recipients to whom the personal data has been disclosed;

(d) the period for which the personal data is to be preserved;

(e) the existence of a data subject's rights to rectification and erasure of personal data (see section 100);

(f) the right to lodge a complaint with the Commissioner and the contact details of the Commissioner;

(g) any information about the origin of the personal data concerned.

(3) A controller is not obliged to provide information under this section unless the controller has received such reasonable fee as the controller may require, subject to subsection (4).

(4) The Secretary of State may by regulations—

(a) specify cases in which a controller may not charge a fee;

(b) specify the maximum amount of a fee.

(5) Where a controller—

(a) reasonably requires further information—

(i) in order that the controller be satisfied as to the identity of the individual making a request under subsection (1), or

(ii) to locate the information which that individual seeks, and

(b) has informed that individual of that requirement,

the controller is not obliged to comply with the request unless the controller is supplied with that further information.

(6) Where a controller cannot comply with the request without disclosing information relating to another individual who can be identified from that information, the controller is not obliged to comply with the request unless—

(a) the other individual has consented to the disclosure of the information to the individual making the request, or

(b) it is reasonable in all the circumstances to comply with the request without the consent of the other individual.

(7) In subsection (6), the reference to information relating to another individual includes a reference to information identifying that individual as the source of the information sought by the request.

(8) Subsection (6) is not to be construed as excusing a controller from communicating so much of the information sought by the request as can be communicated without disclosing the identity of the other individual concerned, whether by the omission of names or other identifying particulars or otherwise.

(9) In determining for the purposes of subsection (6)(b) whether it is reasonable in all the circumstances to comply with the request without the consent of the other individual concerned, regard must be had, in particular, to—

(a) any duty of confidentiality owed to the other individual,

(b) any steps taken by the controller with a view to seeking the consent of the other individual,

(c) whether the other individual is capable of giving consent, and

(d) any express refusal of consent by the other individual.

(10) Subject to subsection (6), a controller must comply with a request under subsection (1) —

(a) promptly, and

(b) in any event before the end of the applicable time period.

(11) If a court is satisfied on the application of an individual who has made a request under subsection (1) that the controller in question has failed to comply with the request in contravention of this section, the court may order the controller to comply with the request.

(12) A court may make an order under subsection (11) in relation to a joint controller whose responsibilities are determined in an arrangement under section 104 only if the controller is responsible for compliance with the obligation to which the order relates.

(13) The jurisdiction conferred on a court by this section is exercisable by the High Court or, in Scotland, by the Court of Session.

(14) In this section—

"the applicable time period" means—

(a) the period of 1 month, or

(b) such longer period, not exceeding 3 months, as may be specified in regulations made by the Secretary of State,

beginning with the relevant time;

"the relevant time", in relation to a request under subsection (1), means the latest of the following—

(a) when the controller receives the request,

(b) when the fee (if any) is paid, and

(c) when the controller receives the information (if any) required under subsection (5) in connection with the request.

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

Commencement Information

I2 S. 94 in force at Royal Assent for specified purposes, see s. 212(2)(f)

VALID FROM 25/05/2018

95 Right of access: supplementary

(1) The controller must comply with the obligation imposed by section 94(1)(b)(i) by supplying the data subject with a copy of the information in writing unless—

(a) the supply of such a copy is not possible or would involve disproportionate effort, or

(b) the data subject agrees otherwise;

and where any of the information referred to in section 94(1)(b)(i) is expressed in terms which are not intelligible without explanation the copy must be accompanied by an explanation of those terms.

(2) Where a controller has previously complied with a request made under section 94 by an individual, the controller is not obliged to comply with a subsequent identical or similar request under that section by that individual unless a reasonable interval has elapsed between compliance with the previous request and the making of the current request.

(3) In determining for the purposes of subsection (2) whether requests under section 94 are made at reasonable intervals, regard must be had to—

(a) the nature of the data,

(b) the purpose for which the data is processed, and

(c) the frequency with which the data is altered.

(4) The information to be supplied pursuant to a request under section 94 must be supplied by reference to the data in question at the time when the request is received, except that it may take account of any amendment or deletion made between that time and the time when the information is supplied, being an amendment or deletion that would have been made regardless of the receipt of the request.

(5) For the purposes of section 94(6) to (8), an individual can be identified from information to be disclosed to a data subject by a controller if the individual can be identified from—

(a) that information, or

(b) that and any other information that the controller reasonably believes the data subject making the request is likely to possess or obtain.

VALID FROM 25/05/2018

96 Right not to be subject to automated decision-making

(1) The controller may not take a decision significantly affecting a data subject that is based solely on automated processing of personal data relating to the data subject.

(2) Subsection (1) does not prevent such a decision being made on that basis if—

(a) the decision is required or authorised by law,

(b) the data subject has given consent to the decision being made on that basis, or

(c) the decision is a decision taken in the course of steps taken—

(i) for the purpose of considering whether to enter into a contract with the data subject,

(ii) with a view to entering into such a contract, or

(iii) in the course of performing such a contract.

(3) For the purposes of this section, a decision that has legal effects as regards an individual is to be regarded as significantly affecting the individual.

VALID FROM 25/05/2018

97 Right to intervene in automated decision-making

(1) This section applies where—

(a) the controller takes a decision significantly affecting a data subject that is based solely on automated processing of personal data relating to the data subject, and

(b) the decision is required or authorised by law.

(2) This section does not apply to such a decision if—

(a) the data subject has given consent to the decision being made on that basis, or

(b) the decision is a decision taken in the course of steps taken—

(i) for the purpose of considering whether to enter into a contract with the data subject,

(ii) with a view to entering into such a contract, or

(iii) in the course of performing such a contract.

(3) The controller must as soon as reasonably practicable notify the data subject that such a decision has been made.

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

(a) to reconsider the decision, or

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

(5) If a request is made to the controller under subsection (4), the controller must, before the end of the period of 1 month beginning with receipt of the request—

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

(b) by notice in writing inform the data subject of the outcome of that consideration.

(6) For the purposes of this section, a decision that has legal effects as regards an individual is to be regarded as significantly affecting the individual.

VALID FROM 25/05/2018

98 Right to information about decision-making

(1) Where—

(a) the controller processes personal data relating to a data subject, and

(b) results produced by the processing are applied to the data subject,

the data subject is entitled to obtain from the controller, on request, knowledge of the reasoning underlying the processing.

(2) Where the data subject makes a request under subsection (1), the controller must comply with the request without undue delay.

VALID FROM 25/05/2018

99 Right to object to processing

(1) A data subject is entitled at any time, by notice given to the controller, to require the controller—

(a) not to process personal data relating to the data subject, or

(b) not to process such data for a specified purpose or in a specified manner,

on the ground that, for specified reasons relating to the situation of the data subject, the processing in question is an unwarranted interference with the interests or rights of the data subject.

(2) Where the controller—

(a) reasonably requires further information—

(i) in order that the controller be satisfied as to the identity of the individual giving notice under subsection (1), or

(ii) to locate the data to which the notice relates, and

(b) has informed that individual of that requirement,

the controller is not obliged to comply with the notice unless the controller is supplied with that further information.

(3) The controller must, before the end of 21 days beginning with the relevant time, give a notice to the data subject—

(a) stating that the controller has complied or intends to comply with the notice under subsection (1), or

(b) stating the controller's reasons for not complying with the notice to any extent and the extent (if any) to which the controller has complied or intends to comply with the notice under subsection (1).

(4) If the controller does not comply with a notice under subsection (1) to any extent, the data subject may apply to a court for an order that the controller take steps for complying with the notice.

(5) If the court is satisfied that the controller should comply with the notice (or should comply to any extent), the court may order the controller to take such steps for complying with the notice (or for complying with it to that extent) as the court thinks fit.

(6) A court may make an order under subsection (5) in relation to a joint controller whose responsibilities are determined in an arrangement under section 104 only if the controller is responsible for compliance with the obligation to which the order relates.

(7) The jurisdiction conferred on a court by this section is exercisable by the High Court or, in Scotland, by the Court of Session.

(8) In this section, "the relevant time", in relation to a notice under subsection (1), means—

(a) when the controller receives the notice, or

(b) if later, when the controller receives the information (if any) required under subsection (2) in connection with the notice.

VALID FROM 25/05/2018

100 Rights to rectification and erasure

(1) If a court is satisfied on the application of a data subject that personal data relating to the data subject is inaccurate, the court may order the controller to rectify that data without undue delay.

(2) If a court is satisfied on the application of a data subject that the processing of personal data relating to the data subject would infringe any of sections 86 to 91, the court may order the controller to erase that data without undue delay.

(3) If personal data relating to the data subject must be maintained for the purposes of evidence, the court may (instead of ordering the controller to rectify or erase the personal data) order the controller to restrict its processing without undue delay.

(4) If—

(a) the data subject contests the accuracy of personal data, and

(b) the court is satisfied that the controller is not able to ascertain whether the data is accurate or not,

the court may (instead of ordering the controller to rectify or erase the personal data) order the controller to restrict its processing without undue delay.

(5) A court may make an order under this section in relation to a joint controller whose responsibilities are determined in an arrangement under section 104 only if the controller is responsible for carrying out the rectification, erasure or restriction of processing that the court proposes to order.

(6) The jurisdiction conferred on a court by this section is exercisable by the High Court or, in Scotland, by the Court of Session.

VALID FROM 25/05/2018

CHAPTER 4

CONTROLLER AND PROCESSOR

Overview

101 Overview

This Chapter sets out—

(a) the general obligations of controllers and processors (see sections 102 to 106);

(b) specific obligations of controllers and processors with respect to security (see section 107);

(c) specific obligations of controllers and processors with respect to personal data breaches (see section 108).

General obligations

VALID FROM 16/09/2019

102 General obligations of the controller

Each controller must implement appropriate measures—

(a) to ensure, and

(b) to be able to demonstrate, in particular to the Commissioner,

that the processing of personal data complies with the requirements of this Part.

VALID FROM 16/09/2019

103 Data protection by design

(1) Where a controller proposes that a particular type of processing of personal data be carried out by or on behalf of the controller, the controller must, prior to the processing, consider the impact of the proposed processing on the rights and freedoms of data subjects.

(2) A controller must implement appropriate technical and organisational measures which are designed to ensure that—

(a) the data protection principles are implemented, and

(b) risks to the rights and freedoms of data subjects are minimised.

VALID FROM 16/09/2019

104 Joint controllers

(1) Where two or more intelligence services jointly determine the purposes and means of processing personal data, they are joint controllers for the purposes of this Part.

(2) Joint controllers must, in a transparent manner, determine their respective responsibilities for compliance with this Part by means of an arrangement between them, except to the extent that those responsibilities are determined under or by virtue of an enactment.

(3) The arrangement must designate the controller which is to be the contact point for data subjects.

VALID FROM 16/09/2019

105 Processors

(1) This section applies to the use by a controller of a processor to carry out processing of personal data on behalf of the controller.

(2) The controller may use only a processor who undertakes—

(a) to implement appropriate measures that are sufficient to secure that the processing complies with this Part;

(b) to provide to the controller such information as is necessary for demonstrating that the processing complies with this Part.

(3) If a processor determines, in breach of this Part, the purposes and means of processing, the processor is to be treated for the purposes of this Part as a controller in respect of that processing.

106 Processing under the authority of the controller or processor

A processor, and any person acting under the authority of a controller or processor, who has access to personal data may not process the data except—

(a) on instructions from the controller, or

(b) to comply with a legal obligation.

Obligations relating to security

107 Security of processing

(1) Each controller and each processor must implement security measures appropriate to the risks arising from the processing of personal data.

(2) In the case of automated processing, each controller and each 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 it,

(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.

VALID FROM 16/09/2019

Obligations relating to personal data breaches

108 Communication of a personal data breach

(1) If a controller becomes aware of a serious personal data breach in relation to personal data for which the controller is responsible, the controller must notify the Commissioner of the breach without undue delay.

(2) Where the notification to the Commissioner is not made within 72 hours, the notification must be accompanied by reasons for the delay.

(3) Subject to subsection (4), the notification must include—

(a) a description of 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) the name and contact details of the contact point from whom more information can be obtained;

(c) a description of the likely consequences of the personal data breach;

(d) a description of 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 to the extent that it is not possible to provide all the information mentioned in subsection (3) at the same time, the information may be provided in phases without undue further delay.

(5) If a processor becomes aware of a personal data breach (in relation to data processed by the processor), the processor must notify the controller without undue delay.

(6) Subsection (1) does not apply in relation to a personal data breach if the breach also constitutes a relevant error within the meaning given by section 231(9) of the Investigatory Powers Act 2016.

(7) For the purposes of this section, a personal data breach is serious if the breach seriously interferes with the rights and freedoms of a data subject.

VALID FROM 25/05/2018

CHAPTER 5

TRANSFERS OF PERSONAL DATA OUTSIDE THE UNITED KINGDOM

109 Transfers of personal data outside the United Kingdom

(1) A controller may not transfer personal data to—

(a) a country or territory outside the United Kingdom, or

(b) an international organisation,

unless the transfer falls within subsection (2).

(2) A transfer of personal data falls within this subsection if the transfer is a necessary and proportionate measure carried out—

(a) for the purposes of the controller's statutory functions, or

(b) for other purposes provided for, in relation to the controller, in section 2(2)(a) of the Security Service Act 1989 or section 2(2)(a) or 4(2)(a) of the Intelligence Services Act 1994.

CHAPTER 6

EXEMPTIONS

VALID FROM 25/05/2018

110 National security

(1) A provision mentioned in subsection (2) does not apply to personal data to which this Part applies if exemption from the provision is required for the purpose of safeguarding national security.

(2) The provisions are—

(a) Chapter 2 (the data protection principles), except section 86(1)(a) and (2) and Schedules 9 and 10;

(b) Chapter 3 (rights of data subjects);

(c) in Chapter 4 , section 108 (communication of a personal data breach to the Commissioner);

(d) in Part 5—

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

(ii) in Schedule 13 (other general functions of the Commissioner), paragraphs 1(a) and (g) and 2;

(e) in Part 6—

(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);
(iii) sections 174 to 176 (provision relating to the special purposes).

VALID FROM 25/05/2018

111 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 mentioned in section 110(2) is, or at any time was, required for the purpose of safeguarding national security in respect of any personal data 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 the issuing of 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 the certificate, the Tribunal may—
(a) allow the appeal, and
(b) quash the certificate.

(5) Where, in any proceedings under or by virtue of 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, and
(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.

VALID FROM 25/05/2018

112 Other exemptions

Schedule 11 provides for further exemptions.

113 Power to make further exemptions

(1) The Secretary of State may by regulations amend Schedule 11—

(a) by adding exemptions from any provision of this Part;

(b) by omitting exemptions added by regulations under paragraph (a).

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

Commencement Information

I3 S. 113 in force at Royal Assent for specified purposes, see s. 212(2)(f)

Status:
Point in time view as at 23/05/2018. This version of this part contains provisions that are not valid for this point in time.

Changes to legislation:
Data Protection Act 2018, PART 4 is up to date with all changes known to be in force on or before 11 April 2024. There are changes that may be brought into force at a future date. Changes that have been made appear in the content and are referenced with annotations.