Data Protection Act 2018

2018 CHAPTER 12

PART 3

LAW ENFORCEMENT PROCESSING

CHAPTER 4

CONTROLLER AND PROCESSOR

Overview and scope

55 Overview and scope

(1) This Chapter—

(a) sets out the general obligations of controllers and processors (see sections 56 to 65);

(b) sets out specific obligations of controllers and processors with respect to security (see section 66);

(c) sets out specific obligations of controllers and processors with respect to personal data breaches (see sections 67 and 68);

(d) makes provision for the designation, position and tasks of data protection officers (see sections 69 to 71).

(2) This Chapter applies only in relation to the processing of personal data for a law enforcement purpose.

(3) Where a controller is required by any provision of this Chapter to implement appropriate technical and organisational measures, the controller must (in deciding what measures are appropriate) take into account—

(a) the latest developments in technology,

(b) the cost of implementation,

(c) the nature, scope, context and purposes of processing, and

(d) the risks for the rights and freedoms of individuals arising from the processing.

General obligations

56 General obligations of the controller

(1) Each controller must implement appropriate technical and organisational measures to ensure, and to be able to demonstrate, that the processing of personal data complies with the requirements of this Part.

(2) Where proportionate in relation to the processing, the measures implemented to comply with the duty under subsection (1) must include appropriate data protection policies.

(3) The technical and organisational measures implemented under subsection (1) must be reviewed and updated where necessary.

57 Data protection by design and default

(1) Each controller must implement appropriate technical and organisational measures which are designed—

(a) to implement the data protection principles in an effective manner, and

(b) to integrate into the processing itself the safeguards necessary for that purpose.

(2) The duty under subsection (1) applies both at the time of the determination of the means of processing the data and at the time of the processing itself.

(3) Each controller must implement appropriate technical and organisational measures for ensuring that, by default, only personal data which is necessary for each specific purpose of the processing is processed.

(4) The duty under subsection (3) applies to—

(a) the amount of personal data collected,

(b) the extent of its processing,

(c) the period of its storage, and

(d) its accessibility.

(5) In particular, the measures implemented to comply with the duty under subsection (3) must ensure that, by default, personal data is not made accessible to an indefinite number of people without an individual's intervention.

58 Joint controllers

(1) Where two or more competent authorities 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.

59 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 provides guarantees to implement appropriate technical and organisational measures that are sufficient to secure that the processing will—

(a) meet the requirements of this Part, and

(b) ensure the protection of the rights of the data subject.

(3) The processor used by the controller may not engage another processor ("a sub-processor") without the prior written authorisation of the controller, which may be specific or general.

(4) Where the controller gives a general written authorisation to a processor, the processor must inform the controller if the processor proposes to add to the number of sub-processors engaged by it or to replace any of them (so that the controller has the opportunity to object to the proposal).

(5) The processing by the processor must be governed by a contract in writing between the controller and the processor setting out the following—

(a) the subject-matter and duration of the processing;

(b) the nature and purpose of the processing;

(c) the type of personal data and categories of data subjects involved;

(d) the obligations and rights of the controller and processor.

(6) The contract must, in particular, provide that the processor must—

(a) act only on instructions from the controller,

(b) ensure that the persons authorised to process personal data are subject to an appropriate duty of confidentiality,

(c) assist the controller by any appropriate means to ensure compliance with the rights of the data subject under this Part,

(d) at the end of the provision of services by the processor to the controller—

(i) either delete or return to the controller (at the choice of the controller) the personal data to which the services relate, and

(ii) delete copies of the personal data unless subject to a legal obligation to store the copies,

(e) make available to the controller all information necessary to demonstrate compliance with this section, and

(f) comply with the requirements of this section for engaging sub-processors.

(7) The terms included in the contract in accordance with subsection (6)(a) must provide that the processor may transfer personal data to a third country or international organisation only if instructed by the controller to make the particular transfer.

(8) 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.

60 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.

61 Records of processing activities

(1) Each controller must maintain a record of all categories of processing activities for which the controller is responsible.

(2) The controller's record must contain the following information—

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

(b) where applicable, the name and contact details of the joint controller;

(c) where applicable, the name and contact details of the data protection officer;

(d) the purposes of the processing;

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

(f) a description of the categories of—

(i) data subject, and

(ii) personal data;

(g) where applicable, details of the use of profiling;

(h) where applicable, the categories of transfers of personal data to a third country or an international organisation;

(i) an indication of the legal basis for the processing operations, including transfers, for which the personal data is intended;

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

(k) where possible, a general description of the technical and organisational security measures referred to in section 66.

(3) Each processor must maintain a record of all categories of processing activities carried out on behalf of a controller.

(4) The processor's record must contain the following information—

(a) the name and contact details of the processor and of any other processors engaged by the processor in accordance with section 59(3);

(b) the name and contact details of the controller on behalf of which the processor is acting;

(c) where applicable, the name and contact details of the data protection officer;

(d) the categories of processing carried out on behalf of the controller;

(e) where applicable, details of transfers of personal data to a third country or an international organisation where explicitly instructed to do so by the controller, including the identification of that third country or international organisation;

(f) where possible, a general description of the technical and organisational security measures referred to in section 66.

(5) The controller and the processor must make the records kept under this section available to the Commissioner on request.

62 Logging

(1) A controller (or, where personal data is processed on behalf of the controller by a processor, the processor) must keep logs for at least the following processing operations in automated processing systems—

(a) collection;
(b) alteration;
(c) consultation;
(d) disclosure (including transfers);
(e) combination;
(f) erasure.

(2) The logs of consultation must make it possible to establish—

(a) the justification for, and date and time of, the consultation, and
(b) so far as possible, the identity of the person who consulted the data.

(3) The logs of disclosure must make it possible to establish—

(a) the justification for, and date and time of, the disclosure, and
(b) so far as possible—
(i) the identity of the person who disclosed the data, and
(ii) the identity of the recipients of the data.

(4) The logs kept under subsection (1) may be used only for one or more of the following purposes—

(a) to verify the lawfulness of processing;
(b) to assist with self-monitoring by the controller or (as the case may be) the processor, including the conduct of internal disciplinary proceedings;
(c) to ensure the integrity and security of personal data;
(d) the purposes of criminal proceedings.

(5) The controller or (as the case may be) the processor must make the logs available to the Commissioner on request.

63 Co-operation with the Commissioner

Each controller and each processor must co-operate, on request, with the Commissioner in the performance of the Commissioner's tasks.

64 Data protection impact assessment

(1) Where a type of processing is likely to result in a high risk to the rights and freedoms of individuals, the controller must, prior to the processing, carry out a data protection impact assessment.

(2) A data protection impact assessment is an assessment of the impact of the envisaged processing operations on the protection of personal data.

(3) A data protection impact assessment must include the following—

(a) a general description of the envisaged processing operations;
(b) an assessment of the risks to the rights and freedoms of data subjects;
(c) the measures envisaged to address those risks;
(d) safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Part, taking into account the rights and legitimate interests of the data subjects and other persons concerned.

(4) In deciding whether a type of processing is likely to result in a high risk to the rights and freedoms of individuals, the controller must take into account the nature, scope, context and purposes of the processing.

65 Prior consultation with the Commissioner

(1) This section applies where a controller intends to create a filing system and process personal data forming part of it.

(2) The controller must consult the Commissioner prior to the processing if a data protection impact assessment prepared under section 64 indicates that the processing of the data would result in a high risk to the rights and freedoms of individuals (in the absence of measures to mitigate the risk).

(3) Where the controller is required to consult the Commissioner under subsection (2), the controller must give the Commissioner—
(a) the data protection impact assessment prepared under section 64, and
(b) any other information requested by the Commissioner to enable the Commissioner to make an assessment of the compliance of the processing with the requirements of this Part.

(4) Where the Commissioner is of the opinion that the intended processing referred to in subsection (1) would infringe any provision of this Part, the Commissioner must provide written advice to the controller and, where the controller is using a processor, to the processor.

(5) The written advice must be provided before the end of the period of 6 weeks beginning with receipt of the request for consultation by the controller or the processor.

(6) The Commissioner may extend the period of 6 weeks by a further period of 1 month, taking into account the complexity of the intended processing.

(7) If the Commissioner extends the period of 6 weeks, the Commissioner must—
(a) inform the controller and, where applicable, the processor of any such extension before the end of the period of 1 month beginning with receipt of the request for consultation, and
(b) provide reasons for the delay.

Obligations relating to security

66 Security of processing

(1) Each controller and each processor must implement appropriate technical and organisational measures to ensure a level of security 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.

Obligations relating to personal data breaches

67 Notification of a personal data breach to the Commissioner

(1) If a controller becomes aware of a personal data breach in relation to personal data for which the controller is responsible, the controller must notify the breach to the Commissioner—

(a) without undue delay, and

(b) where feasible, not later than 72 hours after becoming aware of it.

(2) Subsection (1) does not apply if the personal data breach is unlikely to result in a risk to the rights and freedoms of individuals.

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

(4) Subject to subsection (5), 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 data protection officer or other 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.

(5) Where and to the extent that it is not possible to provide all the information mentioned in subsection (4) at the same time, the information may be provided in phases without undue further delay.

(6) The controller must record the following information in relation to a personal data breach—

(a) the facts relating to the breach,

(b) its effects, and

(c) the remedial action taken.

(7) The information mentioned in subsection (6) must be recorded in such a way as to enable the Commissioner to verify compliance with this section.

(8) Where a personal data breach involves personal data that has been transmitted by or to a person who is a controller under the law of another member State, the information mentioned in subsection (6) must be communicated to that person without undue delay.

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

68 Communication of a personal data breach to the data subject

(1) Where a personal data breach is likely to result in a high risk to the rights and freedoms of individuals, the controller must inform the data subject of the breach without undue delay.

(2) The information given to the data subject must include the following—

(a) a description of the nature of the breach;

(b) the name and contact details of the data protection officer or other 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.

(3) The duty under subsection (1) does not apply where—

(a) the controller has implemented appropriate technological and organisational protection measures which were applied to the personal data affected by the breach,

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

(c) it would involve a disproportionate effort.

(4) An example of a case which may fall within subsection (3)(a) is where measures that render personal data unintelligible to any person not authorised to access the data have been applied, such as encryption.

(5) In a case falling within subsection (3)(c) (but not within subsection (3)(a) or (b)), the information mentioned in subsection (2) must be made available to the data subject in another equally effective way, for example, by means of a public communication.

(6) Where the controller has not informed the data subject of the breach the Commissioner, on being notified under section 67 and after considering the likelihood of the breach resulting in a high risk, may—

(a) require the controller to notify the data subject of the breach, or

(b) decide that the controller is not required to do so because any of paragraphs (a) to (c) of subsection (3) applies.

(7) The controller may restrict, wholly or partly, the provision of information to the data subject under subsection (1) to the extent that and for so long as the restriction is, having regard to the fundamental rights and legitimate interests of the data subject, a necessary and proportionate measure to—

(a) avoid obstructing an official or legal inquiry, investigation or procedure;

(b) avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties;

(c) protect public security;

(d) protect national security;

(e) protect the rights and freedoms of others.

(8) Subsection (6) does not apply where the controller's decision not to inform the data subject of the breach was made in reliance on subsection (7).

(9) The duties in section 52(1) and (2) apply in relation to information that the controller is required to provide to the data subject under this section as they apply in relation to information that the controller is required to provide to the data subject under Chapter 3 .

Data protection officers

69 Designation of a data protection officer

(1) The controller must designate a data protection officer, unless the controller is a court, or other judicial authority, acting in its judicial capacity.

(2) When designating a data protection officer, the controller must have regard to the professional qualities of the proposed officer, in particular—

(a) the proposed officer's expert knowledge of data protection law and practice, and

(b) the ability of the proposed officer to perform the tasks mentioned in section 71.

(3) The same person may be designated as a data protection officer by several controllers, taking account of their organisational structure and size.

(4) The controller must publish the contact details of the data protection officer and communicate these to the Commissioner.

70 Position of data protection officer

(1) The controller must ensure that the data protection officer is involved, properly and in a timely manner, in all issues which relate to the protection of personal data.

(2) The controller must provide the data protection officer with the necessary resources and access to personal data and processing operations to enable the data protection officer to—

(a) perform the tasks mentioned in section 71, and

(b) maintain his or her expert knowledge of data protection law and practice.

(3) The controller—

(a) must ensure that the data protection officer does not receive any instructions regarding the performance of the tasks mentioned in section 71;

(b) must ensure that the data protection officer does not perform a task or fulfil a duty other than those mentioned in this Part where such task or duty would result in a conflict of interests;

(c) must not dismiss or penalise the data protection officer for performing the tasks mentioned in section 71.

(4) A data subject may contact the data protection officer with regard to all issues relating to—

(a) the processing of that data subject's personal data, or

(b) the exercise of that data subject's rights under this Part.

(5) The data protection officer, in the performance of this role, must report to the highest management level of the controller.

71 Tasks of data protection officer

(1) The controller must entrust the data protection officer with at least the following tasks—

(a) informing and advising the controller, any processor engaged by the controller, and any employee of the controller who carries out processing of personal data, of that person's obligations under this Part,

(b) providing advice on the carrying out of a data protection impact assessment under section 64 and monitoring compliance with that section,

(c) co-operating with the Commissioner,

(d) acting as the contact point for the Commissioner on issues relating to processing, including in relation to the consultation mentioned in section 65, and consulting with the Commissioner, where appropriate, in relation to any other matter,

(e) monitoring compliance with policies of the controller in relation to the protection of personal data, and

(f) monitoring compliance by the controller with this Part.

(2) In relation to the policies mentioned in subsection (1)(e), the data protection officer's tasks include—

(a) assigning responsibilities under those policies,

(b) raising awareness of those policies,

(c) training staff involved in processing operations, and

(d) conducting audits required under those policies.

(3) In performing the tasks set out in subsections (1) and (2), the data protection officer must have regard to the risks associated with processing operations, taking into account the nature, scope, context and purposes of processing.