The Data Protection (Law Enforcement and Related Matters) (Bailiwick of Guernsey) Ordinance, 2018

ARRANGEMENT OF SECTIONS

The Data Protection (Law Enforcement and Related Matters) (Bailiwick of Guernsey) Ordinance, 2018

THE STATES, in pursuance of their Resolution of the 26th April, 2017[a], and in exercise of the powers conferred on them by sections 103, 105, 107 and 108 of the Data Protection (Bailiwick of Guernsey) Law, 2017[b] following consultation with the Policy and Finance Committee of the States of Alderney, the Policy and Performance Committee of the Chief Pleas of Sark and the former Commissioner, hereby order:-

PART I

PRELIMINARY

Object of this Ordinance.

1. The object of this Ordinance is to –

(a) protect the rights of individuals in relation to their personal data, and provide for the free movement of personal data, in a manner equivalent to the Law Enforcement Directive,

(b) make other provisions considered appropriate in relation to the processing of personal data for a law enforcement purpose.

---

a Article VI of Billet d'État No. VIII of 2017.

b Order in Council No. * of 2018; as amended by the Data Protection (Commencement, Amendment and Transitional) (Bailiwick of Guernsey) Ordinance, 2018 and the Data Protection (General Provisions) (Bailiwick of Guernsey) Regulations, 2018.

Application of this Ordinance.

2. This Ordinance applies to the processing of personal data in the context of a competent authority for a law enforcement purpose.

Application of provisions of the Law.

3. (1) Subject to the modifications specified in Schedule 1, the following provisions of the Law apply in relation to any processing of personal data in the context of a competent authority for a law enforcement purpose –

(a) the provisions of Part I, except section 1,

(b) section 10, except subsection (7) of that section,

(c) section 11, except subsection (1)(b) of that section,

(d) section 37,

(e) the provisions of Part V, and

(f) the provisions of Parts XI to XVI, except section 96.

(2) No other provision of the Law applies in relation to any processing of personal data in the context of a competent authority for a law enforcement purpose.

PART II

DUTIES AND PRINCIPLES OF PROCESSING

Duty to comply with data protection principles.

4. (1) A controller must ensure that the processing of all personal data in relation to which the person is the controller complies with the principles in sections 5 to 10.

(2) The controller is responsible for, and must be able to demonstrate, compliance with those principles.

Lawfulness and fairness principle.

5. (1) Personal data must be processed lawfully and fairly.

(2) Processing of personal data for a law enforcement purpose is lawful only if, and to the extent that, the processing is carried out in the context of the controller discharging a function conferred or imposed on that controller by law, and –

(a) in the case of any personal data –

(i) the data subject has given consent to the processing for the law enforcement purpose,

(ii) the processing is necessary for the performance of a task carried out for the law enforcement purpose by a competent authority, or

(iii) the processing is authorised or required by any enactment,

and

(b) in the case of special category data, the processing additionally satisfies the condition in either subsection (3) or (4).

(3) The condition in this subsection is that –

(a) the data subject has given consent to the processing for the law enforcement purpose, and

(b) the controller has put in place appropriate safeguards for the significant interests of the data subject.

(4) The condition in this subsection is that –

(a) the processing is strictly necessary for the law enforcement purpose,

(b) the processing satisfies at least one condition in Schedule 2, and

(c) the controller has put in place appropriate safeguards for the significant interests of the data subject.

(5) The Committee may by regulations amend Schedule 2.

Purpose limitation principle.

6. (1) Personal data –

(a) must not be collected except for a specific, explicit and legitimate purpose, and

(b) once collected, must not be processed in the context of any controller in a manner incompatible with the purpose for which it was collected.

(2) For the purposes of subsection (1)(b), processing of personal data ("**the secondary processing"),** in the context of the controller that collected the data or another controller ("**the relevant controller**"), for a law enforcement purpose ("**the secondary law enforcement purpose**") other than the law enforcement purpose for which the data was collected is compatible with the law enforcement purpose for which the data was collected ("**the primary law enforcement purpose**") only if both the conditions in subsections (3) and (4) are satisfied.

(3) The condition in this subsection is that –

(a) the consent of the data subject is obtained for the secondary processing (for the secondary law enforcement purpose),

(b) the secondary processing is for a historical or scientific purpose related to the secondary law enforcement purpose, or

(c) the secondary processing is carried out in the context of the relevant controller discharging a function conferred or imposed on the relevant controller by law.

(4) The condition in this subsection is that the secondary processing is necessary for and proportionate to the secondary law enforcement purpose.

(5) For the purposes of subsection (1)(b), processing of personal data for any purpose ("**that other purpose**") other than a law enforcement purpose is compatible with the law enforcement purpose for which the data was collected only if –

(a) the consent of the data subject is obtained for the processing for that other purpose,

(b) the processing for that other purpose is authorised by regulations made by the Committee for this purpose and carried out in accordance with those regulations, or

(c) the processing for that other purpose is authorised or required by any other enactment and carried out in accordance with the enactment.

Data minimisation principle.

7. Personal data processed must be adequate, relevant and not excessive in relation to the law enforcement purpose for which it is processed.

Accuracy principle.

8. (1) Personal data processed must be accurate and where applicable, kept up to date, and reasonable steps must be taken to ensure that personal data that is inaccurate (having regard to the law enforcement purpose for which it is processed) is erased or corrected without delay.

(2) In processing personal data for any law enforcement purpose, personal data based on facts must, so far as possible, be distinguished from personal data based on personal assessments.

(3) In processing personal data for any law enforcement purpose, a clear distinction must, where relevant and so far as practicable, be made between personal data relating to different categories of data subject, such as —

(a) persons suspected of having committed or being about to commit a criminal offence,

(b) persons convicted of a criminal offence,

(c) persons who are or may be victims of a criminal offence, and

(d) witnesses or other persons with information about criminal offences.

(4) All reasonable steps must be taken to ensure that personal data which is inaccurate, incomplete or no longer up to date is not transmitted or made available for any law enforcement purpose.

(5) For the purposes of subsection (4), so far as practicable—

(a) the quality of personal data (in relation to its accuracy, completeness and recentness) must be verified before it is transmitted or made available,

(b) in all transmissions of personal data, the necessary information enabling the recipient to assess the degree of accuracy, completeness and reliability of the data and the extent to which it is up to date must be included, and

(c) if, after personal data has been transmitted, it emerges that the data was incorrect or that the transmission was unlawful, the recipient must be notified without delay.

Storage limitation principle.

9. (1) Personal data must not be kept in a form that permits identification of the data subject any longer than is necessary for the law enforcement purpose for which it is processed.

(2) Appropriate technical or organisational measures must be established to ensure that the need for continued storage of personal data for any law enforcement purpose is reviewed periodically at appropriate intervals.

Integrity and confidentiality principle.

10. Personal data must be processed in a manner that ensures its security appropriately, including protecting it against unauthorised or unlawful processing

and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Transmission to be subject to any applicable conditions.

11. (1) This section applies where –

(a) a competent authority transmits personal data to another person, and

(b) this Ordinance or any other enactment imposes specific conditions in relation to the processing of the personal data by the competent authority.

(2) The competent authority must –

(a) inform the recipient of the personal data of those conditions, and

(b) require the recipient to comply with those conditions.

PART III
DATA SUBJECT RIGHTS

Controller's duties and data subject rights

Data subject's right to information.

12. (1) A data subject has a right to be given information in accordance with this section.

(2) A controller must publish or otherwise give data subjects the following information in accordance with subsection (5) —

(a) the identity and contact details of the controller and, where applicable, the controller's representative,

(b) the contact details of the data protection officer, where applicable,

(c) the purposes of the processing,

(d) information as to the existence of the data subject rights under sections 13 to 17,

(e) the complaints and appeals information, and

(f) the possibility of requesting the Authority to bring civil proceedings before a court under section 85 of the Law.

(3) Where reasonable to do so in any specific case in order to enable a data subject to exercise data subject rights, the controller must also give the data subject the following further information in accordance with subsection (6) –

(a) information about the legal basis for the processing,

(b) information about the period for which the personal data is expected to be stored, or if that is not possible, the criteria used to determine that period,

(c) where applicable, information about the categories of recipients of the personal data (including recipients in authorised or unauthorised jurisdictions), and

(d) any other information necessary to enable the data subject to exercise the data subject rights.

(4) Without limiting the generality of subsection (3), an example of where it might be reasonable to give further information to a data subject under subsection (3) is where the personal data is collected without the knowledge of the data subject.

(5) The information required to be published or given to a data subject under subsection (2) must be published or given to the data subject –

(a) within a reasonable period of that personal data being processed in the context of the controller, having regard to the specific circumstances in which the personal data is so processed, and

(b) in any case, before or at the earlier of the following times –

(i) if the personal data is used for communication with the data subject, the time of the first communication with the data subject, and

(ii) if the personal data is disclosed to another recipient, the time when the personal data is first disclosed to any recipient.

(6) Any information required to be given to a data subject under subsection (3) must be given –

(a) as soon as practicable, and

(b) in any case, upon request by the data subject.

(7) For the avoidance of doubt, any information required to be given to data subjects under this section may be given wholly or partly using standardised icons, but any icon presented electronically must be machine-readable.

(8) In this section, "**adequacy decision**", in respect of any country, sector within a country or international organisation –

(a) means a decision made by the European Commission that the country, sector or international organisation concerned ensures an adequate level of protection within the meaning of Article 36 of the Law Enforcement Directive, and

(b) includes a finding of the European Commission under Article 31(2) of the former Directive, in force immediately before the commencement date, that the country, sector or international organisation concerned ensures an adequate level of protection within the

meaning of Article 25(2) of that former Directive, unless and until the European Commission revokes the finding or decides that the country, sector or international organisation concerned does not ensure an adequate level of protection within the meaning of Article 36 of the Law Enforcement Directive.

Right of access.

13. (1) An individual has a right to be given the following information in accordance with subsection (2) –

(a) confirmation as to whether or not personal data relating to the individual is being processed in the context of a controller, and

(b) if personal data relating to the individual is being processed in the context of a controller –

(i) one copy of the personal data,

(ii) the purposes and the legal basis of the processing,

(iii) the categories of personal data concerned,

(iv) any available information as to the source of the personal data,

(v) the recipients or categories of recipients to whom the personal data is disclosed, in particular recipients in any unauthorised jurisdiction,

(vi) the period for which the personal data is expected to be stored, or if that is not possible, the criteria used to determine that period,

(vii) information as to the existence of the data subject rights under sections 14 to 17,

(viii) the complaints and appeals information,

(ix) the possibility of requesting the Authority to bring civil proceedings before a court under section 85 of the Law, and

(x) information as to the personal data undergoing processing and any available information as to its origin.

(2) On request by an individual, the controller must give the individual that information.

Right to rectification or restriction of processing.

14. (1) Where a data subject disputes the accuracy or completeness of personal data, the data subject may make a written request to the controller to rectify

or change the personal data by stating the inaccuracy or explaining why the personal data is incomplete.

(2) On receipt of a request made in accordance with subsection (1), the controller must –

(a) take any reasonable steps available to the controller to check whether the personal data is inaccurate or incomplete, and

(b) take any action required by subsection (3) or (5).

(3) Where the controller is able, by taking reasonable steps, to verify that the personal data is inaccurate or incomplete, the controller must –

(a) rectify that personal data, or

(b) complete that personal data (taking into account the purposes of the processing), for example, by adding to the personal data a supplementary statement provided by the data subject.

(4) Subsection (5) applies where –

(a) the data subject makes a written request to the controller to take either or both the actions specified in that subsection during the period it takes the controller to verify the accuracy or completeness of the personal data, or

(b) it is not reasonable to expect the controller to verify the accuracy or completeness of the personal data.

(5) Where this subsection applies, the controller –

(a) must add to the personal data a statement to the effect that the data subject disputes the accuracy or (as the case may be) completeness of that personal data, and

(b) may, if requested by the data subject, restrict processing of the personal data in a manner and for a time agreed with the data subject, except to the extent that the data subject gives consent to processing of that personal data in any other manner.

(6) Nothing in this section limits section 15.

Right to erasure.

15. (1) Whether or not the data subject disputes the accuracy or completeness of personal data, this section applies where –

(a) the processing of any personal data breaches or would breach section 4, including any of these principles –

(i) the principle in section 5(1) (lawfulness and fairness),

(ii) the principle in section 6(1) (purpose limitation),

(iii) the principle in section 7 (data minimisation),

(iv) the principle in section 8(1), (2), (3) or (4) (accuracy),

(v) the principle in section 9(1) or (2) (storage limitation), or

(vi) the principle in section 10 (integrity and confidentiality), or

(b) the controller has a duty imposed by law to erase the personal data, otherwise than under this section.

(2) The data subject has a right to require the controller to erase the personal data in accordance with subsections (3) and (4).

(3) The data subject may make a written request to the controller to erase the personal data, stating the grounds in subsection (1)(a) or (b) on which the data subject believes this section applies.

(4) On receipt of a request made in accordance with subsection (3), the controller must erase that personal data except as otherwise provided by subsection (5) or (6).

(5) Where the ground given by the data subject for believing that this section applies is that the personal data is inaccurate or incomplete, but its accuracy or completeness cannot be verified with reasonable efforts, the controller

may decide not to erase that data in respect of that ground, in which case the controller –

(a) must add to the personal data a statement to the effect that the data subject disputes the accuracy or (as the case may be) completeness of that personal data, and

(b) may, if requested by the data subject, restrict processing of the personal data in a manner and for a time agreed with the data subject, except to the extent that the data subject gives consent to processing of that personal data in any other manner.

(6) Where the controller believes on reasonable grounds that the personal data is required as evidence in any proceedings (including prospective proceedings) relating to a criminal offence within or outside the Bailiwick, the controller must restrict the processing of the personal data instead of erasing it.

(7) If a controller erases personal data under subsection (4) –

(a) the controller must notify any person ("**recipient**") to whom the controller has disclosed that data, and

(b) where a recipient is the controller of that personal data, the recipient must similarly erase that personal data.

(8) Nothing in this section affects or limits any duty imposed by law on the controller or any other person to erase the personal data, otherwise than under this section.

Actions required following rectification, restriction, etc.

16. (1) This section applies where a controller –

(a) rectifies or completes personal data under section 14(3),

(b) adds to or restricts the processing of personal data in accordance with section 14(5) or 15(5), or

(c) restricts the processing of personal data under section 15(6).

(2) The controller must, as soon as practicable, notify –

(a) any competent authority or other relevant authority from which the personal data originated, and

(b) any person ("**recipient**") to whom the controller has disclosed the personal data.

(3) If a recipient is the controller of that personal data, the recipient must similarly rectify, complete, add to or (as the case may be) restrict the processing of that data.

(4) A controller must inform the data subject before lifting any restriction on the processing of personal data.

Right not to be subjected to decisions based on automated processing .

17. (1) Subject to subsections (2) to (4) –

(a) a data subject has a right not to be subjected to an automatic decision, and

(b) a controller must not cause or permit a data subject to be subjected to an automatic decision.

(2) A controller may cause or permit a data subject to be subjected to an automatic decision where –

(a) the data subject has given consent to the automated processing, or

(b) the automated processing is –

(i) authorised by regulations made by the Committee for this purpose and carried out in accordance with those regulations, or

(ii) otherwise authorised or required by law.

(3) Subsection (2) does not apply to an automatic decision based on automated processing of special category data unless –

(a) the data subject has given consent to the automated processing of that special category data, or

(b) the automated processing of that kind or description of special category data is –

(i) specifically authorised by regulations made by the Committee for this purpose and carried out in accordance with those regulations, or

(ii) specifically authorised or specifically required by any other enactment and carried out in accordance with the enactment.

(4) Where a controller causes or permits a data subject to be subjected to an automatic decision under subsection (2) –

(a) the controller must, as soon as reasonably practicable, inform the data subject that an automatic decision has been taken based solely on automated processing of personal data relating to the data subject, and

(b) the data subject may, before the end of the period of 21 days 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)(b), the controller must, before the end of the period of 21 days beginning with receipt of the request—

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

(b) comply with the request, and

(c) inform the data subject of—

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

(ii) the outcome of complying with the request

(6) The Committee may by regulations make further provisions to provide suitable measures to safeguard the significant interests of data subjects in connection with automatic decisions.

(7) In this section –

"**automated processing**", in relation to any automatic decision, means the automated processing on which the automatic decision is based, and

"**automatic decision**", in relation to any data subject, means a decision that –

(a) is based solely on automated processing of personal data relating to the data subject, and

(b) affects the significant interests of the data subject.

Controller must facilitate exercise of data subject rights.

18. A controller must take reasonable steps to facilitate the exercise of data subject rights.

Exceptions and further provisions relating to controller's duties and data subject rights

General exemption for judicial decisions, etc.

19. (1) Nothing in sections 12 to 16 applies in relation to the processing of judicial data in the course of a crime-related investigation or proceedings relating to a criminal offence within or outside the Bailiwick.

(2) In this section –

"**crime-related investigation**" means –

(a) any criminal investigation within or outside the Bailiwick, or

(b) any investigation under or for the purposes of a criminal proceeds enactment, and

"**judicial data**" means personal data contained in a judicial decision or in other documents, relating to the crime-related investigation or (as the case may be) the proceedings relating to a criminal offence within or outside the Bailiwick, which are created by or on behalf of a court or other judicial authority.

Application and effect of sections 21 to 23.

20. (1) Sections 21 to 23 apply where an individual has made a request to the controller under any of sections 13 to 15 –

(a) to give the individual any information to which the individual has a data subject right, or

(b) to take any action.

(2) Sections 13 to 15 are subject to sections 21 to 23.

(3) In sections 21 to 23 –

"**request**" means the request made by the individual, and

"**requestor**" means the individual making a request.

Compliance with request to exercise data subject right.

21. (1) Subject to the following provisions of this section, sections 22 to 24 and any other exception or exemption provided by section 13, 14 or 15 or any other provision of this Ordinance, the controller must both comply with the request and notify the requestor of any action taken in compliance with the request –

(a) as soon as practicable, and

(b) in any event within the designated period.

(2) If a controller fails to comply with any part of a request, the controller must give the requestor notice in accordance with subsection (3) of –

(a) the controller's reasons for not so complying,

(b) the complaints and appeals information, and

(c) the possibility of requesting the Authority to bring civil proceedings before a court under section 85 of the Law.

(3) The notification in subsection (2) must be given to the requestor –

(a) as soon as practicable, and

(b) in any event within the designated period.

(4) The controller may extend the time allowed for notification under subsection (1)(b) or (3)(b) by a further two months where necessary, taking into account the complexity and number of requests, but in this event the controller must notify the requestor, within the designated period, of –

(a) any such extension, and

(b) the reasons for the extension.

(5) In this section –

"**the designated period**", in relation to a request, means the period of one month following the relevant day, and

"**the relevant day**", in relation to a request, means the latest of the following days –

(a) the day on which the controller receives the request,

(b) the day on which the controller receives any information reasonably necessary to confirm the identity of the requestor, and

(c) the day on which any fee or charge payable under this Ordinance in respect of any information or action requested is paid to the controller.

Requirement to verify identity.

22. (1) Where a controller has any reason to doubt the requestor's identity, the controller may request the provision of any additional information that is reasonably necessary to confirm it.

(2) If, despite taking reasonable steps to confirm the requestor's identity, a controller is unable to do so –

(a) the requestor is not entitled to exercise any data subject right conferred on the requestor in relation to the controller, and

(b) the controller is not required to give the information or take the action requested by the individual.

Exceptions based on nature of request.

23. (1) If any part of a request is manifestly unfounded, the controller may refuse to give the information or take the action requested in that part of the request.

(2) If any part of a request is frivolous, vexatious, unnecessarily repetitive or otherwise excessive, the controller may –

(a) refuse to give the information or take any action requested in that part of the request, or

(b) in exceptional circumstances, give that information or take that action but charge a reasonable fee for the administrative costs of so doing.

(3) For the avoidance of doubt, if any question is raised in any proceedings under this Ordinance as to whether or not any part of a request is manifestly unfounded or frivolous, vexatious, unnecessarily repetitive or otherwise excessive within the meaning of subsection (1) or (2), the controller bears the burden of proof on the balance of probabilities to show that it is.

Restrictions on duty to provide information on grounds of obstruction, prejudice, etc.

24. (1) Despite any provision of this Ordinance to the contrary, a controller may wholly or partly restrict the publication of information or provision of information to a data subject or the Authority under any information duty to the extent that and for so long as the restriction is, having regard to the significant interests of the data subject, a necessary and proportionate measure to —

(a) avoid obstructing an official or legal inquiry, investigation or procedure within or outside the Bailiwick,

(b) avoid prejudicing the prevention, detection, investigation or prosecution of a criminal offence within or outside the Bailiwick,

(c) avoid prejudicing any proceedings relating to a criminal offence within or outside the Bailiwick,

(d) protect public security or the security of the British Islands, or

(e) protect the significant interests of any individual.

(2) Where the provision of information to a data subject is wholly or partly restricted under subsection (1), the controller must as soon as practicable –

(a) give the data subject the following information —

(i) a statement to the effect that the provision of information has been restricted,

(ii) the reasons for the restriction,

(iii) the complaints and appeals information, and

(iv) the possibility of requesting the Authority to bring civil proceedings before a court under section 85 of the Law, and

(b) record the reasons for the restriction.

(3) Neither subsection (2)(a) nor (2)(b) applies where complying with those provisions would undermine the purpose of the restriction.

(4) In this section, "**information duty**" means -

(a) a duty imposed on the controller to publish information or give information to the data subject under –

(i) section 12(2) or (3),

(ii) section 13(2),

(iii) section 21(1) or (2), or

(iv) section 35(1), or

(b) a duty imposed on the controller to give information to the Authority under section 34(2).

PART IV

DUTIES OF CONTROLLERS AND PROCESSORS

Duty of controllers to give information or take action

Requirements to give information or take action.

25. (1) Where any provision of this Ordinance requires a controller to give a person any information, whether or not in response to a request, the controller must give the information to the person –

(a) in writing, unless the information is given in response to a request and the person requests that it be given orally, in which case it may be given orally after verifying the identity of that person,

(b) if the information is given in response to a request and the request is made by electronic means, by similar or commonly used electronic means unless otherwise requested by the person, in which case it may be given by the other means requested after verifying the identity of that person,

(c) if the information is given in writing, in a concise, transparent, easily visible, easily accessible, intelligible and clearly legible form, and

(d) in any case –

(i) in clear and plain language, and

(ii) if the person is a child, in a manner suitable for a child.

(2) Where any provision of this Ordinance requires a controller to give a person any information or take any action, whether or not in response to a request, the information must be given or (as the case may be) the action taken free of any charge except where otherwise –

(a) prescribed by regulations made by the Committee, or

(b) specified by any other provision of this Ordinance.

(3) Regulations made for the purposes of subsection (2)(a) may prescribe –

(a) the fee or charge payable for the information or action, or

(b) the basis on which the amount of the fee or charge payable is to be calculated or ascertained.

Duty to take steps to ensure compliance

Duty to take reasonable steps for compliance.

26. (1) A controller must take reasonable steps (including technical and organisational measures) –

(a) to ensure that processing of personal data is carried out in compliance with this Ordinance, and

(b) to be able to demonstrate such compliance upon request by the Authority.

(2) In discharging the duty in subsection (1), the controller must take into account –

(a) the nature, scope, context and purpose of the processing,

(b) the likelihood and severity of risks posed to the significant interest of data subjects, if processing is not carried out in compliance with this Ordinance,

(c) best practices in technical measures, organisational measures and any other steps that may be taken for the purposes of subsection (1), and

(d) the costs of implementing appropriate measures.

Data protection measures by design and default.

27. (1) When determining the purposes and means of processing personal data, a controller must establish and carry out proportionate technical and organisational measures to –

(a) effectively comply with the data protection principles,

(b) ensure, by default, that only personal data that is necessary for each specific purpose of processing is processed, and

(c) integrate any other necessary safeguards into the processing to comply with this Ordinance and safeguard data subject rights.

(2) The measures required by subsection (1)(a) may include pseudonymisation.

(3) Subsection (1)(b) requires measures to limit, by default –

(a) the amount of personal data collected,

(b) the extent of its processing,

(c) the period of its storage, and

(d) its accessibility, in particular ensuring that personal data is not made accessible to an indefinite number of persons without human intervention.

(4) Nothing in this section affects or limits the controller's duties under section 26(1).

Joint controllers.

28. (1) Where two or more controllers ("**joint controllers**") jointly determine the purposes and means of processing of personal data, they must

explicitly agree on their respective responsibilities for compliance with duties of controllers under this Ordinance, in particular their duties under Part III.

(2) The agreement required by subsection (1) must –

(a) specify the respective roles, relationships, responsibilities and duties of each joint controller, in relation to the data subjects, and

(b) designate the controller which is to be the contact point for data subjects.

(3) Regardless of the terms and conditions of any agreement under subsection (1) or any other agreement –

(a) a data subject may exercise any data subject right against any joint controller, and

(b) each joint controller remains jointly and severally liable for the performance of any duty imposed on a controller by this Ordinance.

(4) Subsections (1) and (2) do not apply where the respective responsibilities of joint controllers are clearly determined by law otherwise than under this section.

Duties of controllers and processors in relation to each other and processing activities

Duties of controllers in relation to processors.

29. (1) A controller must not cause or permit a processor to process personal data unless both the conditions in subsections (2) and (3) are satisfied.

(2) The condition in this subsection is that the processor provides the controller with sufficient guarantees that reasonable technical and organisational measures will be established and carried out by the processor –

(a) to ensure that the processing meets the requirements of this Ordinance, and

(b) to safeguard data subject rights.

(3) The condition in this subsection is that there is a legally binding agreement in writing between the controller and the processor setting out –

(a) the subject matter of the processing,

(b) the duration of the processing,

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

(d) the category of personal data to be processed,

(e) the categories of data subjects,

(f) the duties and rights of the controller, and

(g) the duties imposed on the processor by sections 30 and 31.

Duties of processors in relation to controllers.

30. (1) A processor must –

(a) subject to paragraph (b), process personal data only on written instructions from the controller, including with regard to transfers of personal data to an unauthorised jurisdiction,

(b) where a processor is required by law to process personal data contrary to paragraph (a), inform the controller of that requirement (unless prohibited by an enactment) before so processing the personal data,

(c) ensure that any person authorised by the processor to process the personal data is legally bound to a duty of confidentiality,

(d) at the controller's discretion, after the end of the provision of services relating to processing, and unless required to store the personal data by an enactment –

(i) delete all personal data, or

(ii) return all personal data to the controller, and

delete existing copies,

(e) put in place reasonable technical and organisational measures to assist the controller to exercise or perform the controller's duties under Part III, and

(f) make available to the controller all information necessary to demonstrate compliance with this section and sections 29 and 31.

(2) The processor must immediately inform the controller if, in the processor's opinion, an instruction given by the controller to the processor breaches this Ordinance or any other enactment.

(3) Where a controller or processor ("**the authorising person**") gives any person ("**the authorised person**"), other than an employee of the controller or (as the case may be) processor, access to any personal data –

(a) subsections (1)(a) and (b) and (2) apply to the authorised person as if the authorised person were a processor, and

(b) the authorising person must take reasonable steps to ensure that the authorised person complies with the duties imposed on that person under subsections (1)(a) and (b) and (2) as given effect by paragraph (a) of this subsection.

Duties of processors in relation to further processing by another processor.

31. (1) A processor ("**primary processor**") must not engage another processor ("**secondary processor**") to process personal data unless –

(a) the controller has specifically authorised the secondary processor to process the personal data, or

(b) the controller has generally authorised the primary processor to engage other processors to process the personal data, and the engagement of the secondary processor complies with the requirement in subsection (2).

(2) Subsection (1)(b) refers to the requirement that the primary processor must, before engaging the secondary processor (including any processor engaged to add to or replace the secondary processor) –

(a) notify the controller of the proposed engagement, and

(b) give the controller an opportunity to object to the engagement.

(3) This section does not apply where the secondary processor –

(a) is an employee of the primary processor, or

(b) processes the personal data under the direction and control of the primary processor.

PART V

SECURITY OF PERSONAL DATA

Duty to take reasonable steps to ensure security.

32. (1) A controller or processor must take reasonable steps to ensure a level of security appropriate to the personal data, in particular where the personal data is special category data.

(2) The steps required under subsection (1) may include technical and organisational measures such as –

(a) pseudonymising and encrypting personal data,

(b) ensuring that the controller or processor has and retains the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services,

(c) ensuring that the controller or processor has and retains the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident, and

(d) establishing and implementing a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

(3) In discharging the duty in subsection (1), the controller or processor must take into account –

(a) the nature, scope, context and purpose of the processing,

(b) the likelihood and severity of risks posed to the significant interest of data subjects, if the personal data is not secure,

(c) best practices in technical measures, organisational measures and any other steps that may be taken for the purposes of subsection (1), and

(d) the costs of implementing appropriate measures.

(4) The risks mentioned in subsection (3)(b) include risks presented by processing, in particular from –

(a) accidental or unlawful destruction, loss or alteration of personal data, or

(b) unauthorised disclosure of, or access to, personal data.

Special security measures in respect of automated processing.

33. (1) Where automated processing of personal data is concerned, the steps required to be taken by a controller or processor under section 32 must include appropriate technical and organisational measures designed to –

(a) deny unauthorised persons access to processing equipment (referred to as "equipment access control" in the Law Enforcement Directive),

(b) prevent the unauthorised reading, copying, modification or removal of data media (referred to as "data media control" in the Law Enforcement Directive),

(c) prevent the unauthorised input of personal data and the unauthorised inspection, modification or deletion of stored personal data (referred to as "storage control" in the Law Enforcement Directive),

(d) prevent the use of automated processing systems by unauthorised persons using data communication equipment (referred to as "user control" in the Law Enforcement Directive),

(e) ensure that persons authorised to use an automated processing system have access only to the personal data covered by their access authorisation (referred to as "data access control" in the Law Enforcement Directive),

(f) ensure that it is possible to verify and establish the persons to which personal data have been or may be transmitted or made available using data communication equipment (referred to as

"communication control" in the Law Enforcement Directive),

(g) ensure that it is subsequently possible to verify and establish which personal data have been input into automated processing systems and when and by whom the personal data were input (referred to as "input control" in the Law Enforcement Directive),

(h) prevent the unauthorised reading, copying, modification or deletion of personal data during transfers of personal data or during transportation of data media (referred to as "transport control" in the Law Enforcement Directive),

(i) ensure that installed systems may, in the case of interruption, be restored (referred to as "recovery" in the Law Enforcement Directive), and

(j) ensure that the functions of the system perform, that the appearance of faults in the functions is reported (referred to as "reliability" in the Law Enforcement Directive) and that stored personal data cannot be corrupted by means of a malfunctioning of the system (referred to as "integrity" in the Law Enforcement Directive).

Notification and records required in case of personal data breach.

34. (1) Where a processor becomes aware of a personal data breach, the processor must –

(a) give the controller notice of it as soon as practicable, and

(b) where oral notice is given under paragraph (a), follow up the oral notice with a written notice to the controller at the first available opportunity.

(2) Where a controller becomes aware of a personal data breach, the controller must give the Authority written notice of it –

(a) as soon as practicable, and

(b) in any event, no later than 72 hours after becoming so aware, unless this is not practicable.

(3) Subject to subsection (4), a notice under subsection (2) 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 where 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, and

(e) if the notice is given more than 72 hours after the controller becomes aware of the personal data breach, an explanation of the reasons for the delay.

(4) If it is impracticable to give the Authority all of the information in subsection (3) at the same time as the notice is given, the controller may provide the information in phases as soon as practicable.

(5) Subsection (2) does not apply where the personal data breach is unlikely to result in any risk to the significant interests of the data subject.

(6) Where a controller ("**Controller A**") has received the personal data that is the subject of a personal data breach from another controller ("**Controller B**") in an authorised jurisdiction, or has transmitted that personal data to another controller ("**Controller C**") in an authorised jurisdiction, Controller A must give Controller B or (as the case may be) Controller C notice of the matters specified in subsection (3)(a) to (d) as soon as practicable.

(7) In any case, a controller must keep a written record of each personal data breach of which the controller is aware, including –

(a) the facts relating to the breach,

(b) the effects of the breach,

(c) the remedial action taken, and

(d) any steps taken by the controller to comply with this section, including whether the controller gave a notice to the Authority under subsection (2), and if so, a copy of the notice.

Data subject to be notified if high risk to significant interests.

35. (1) Where a controller becomes aware of a personal data breach that is likely to pose a high risk to the significant interests of a data subject, the controller must give the data subject written notice of the breach as soon as practicable.

(2) The notice must include –

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

(b) the name and contact details of the data protection officer or other source where more information can be obtained,

(c) a description of the likely consequences of the breach, and

(d) a description of the measures taken or proposed to be taken by the controller to address the breach, including, where appropriate, measures to mitigate its possible adverse effects.

(3) Subsection (1) does not apply where –

(a) the controller has established and carried out appropriate technical and organisational measures to protect personal data, and those measures were applied to the personal data affected by the breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption,

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

(c) performing that duty would involve disproportionate effort.

(4) Where the exception in subsection (3)(c) applies, the controller must publish a notice (without making public any personal data) or take any other

step equivalent to publication in order to inform the data subject in an equally effective manner.

(5) Unless a controller has taken steps to notify the data subject in accordance with subsections (1) and (2) or subsection (4), the Authority may by written notice to the controller require the controller to take steps specified by the Authority to so notify the data subject if the Authority is of the opinion that the controller is obliged to take those steps under subsections (1) and (2) or subsection (4).

PART VI

DATA PROTECTION IMPACT ASSESSMENTS AND PRIOR CONSULTATION

Impact assessment required for high-risk processing.

36. (1) A controller must not cause or permit any high-risk processing before carrying out an assessment of the impact of the proposed processing operations on the protection of personal data.

(2) The assessment must include –

(a) a general description of the proposed processing operations (including the means of processing),

(b) an assessment of the risks posed to the significant interests of data subjects by the processing, and

(c) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and demonstrate

compliance with this Ordinance, taking into account the significant interests of data subjects and any other individuals concerned.

(3) A single data protection impact assessment may address a set of similar processing operations that present similar risks.

(4) Subsection (1) does not apply to –

(a) any processing specifically required or authorised by high-risk legislation within the meaning of section 38, if an assessment including the information required by subsection (2) of this section has been given to the Authority prior to the high-risk legislation being made or enacted, or

(b) any other prescribed kind or description of processing.

(5) In this section and sections 37 and 38, "**high-risk processing**" –

(a) means any processing of personal data that is likely to pose a high risk to the significant interests of data subjects,

(b) is deemed to include any processing of a kind declared to be high-risk processing in a list maintained and published by the Authority, and

(c) is deemed to exclude any processing of a kind declared not to be high-risk processing in a list maintained and published by the Authority.

Prior consultation required for high-risk processing.

37. (1) This section applies to processing that would form part of a new filing system to be created –

(a) where a data protection impact assessment indicates that the processing is likely to be high-risk processing in the absence of measures taken by the controller to mitigate risks to the significant interests of data subjects,

(b) where the type of processing involved is likely to be high-risk processing, or

(c) in other prescribed circumstances.

(2) Before commencing the processing, the controller must consult the Authority by written request.

(3) A request must include the following information–

(a) where applicable, the respective responsibilities of the controller, joint controllers and processors involved in the proposed processing, for example for processing within a group of undertakings,

(b) a copy of the data protection impact assessment (if any),

(c) the contact details of any data protection officer, and

(d) any other information required by the Authority.

(4) Where the Authority is of the opinion that the proposed processing would be in breach of an operative provision, for example where the controller has insufficiently identified or mitigated the risk, the Authority –

(a) must give written notice of its opinion to the controller and, where applicable to the processor, and

(b) may exercise any power conferred on the Authority by the Law or this Ordinance in relation to a breach or potential breach of an operative provision.

(5) The Authority must give the notice required by subsection (4)(a) –

(a) as soon as practicable, and

(b) in any event within six weeks of the designated date.

(6) The Authority may extend the time allowed for the notice in subsection (5)(b) by a further month taking into account the complexity of the proposed processing, but in this case, the Authority must inform the controller and,

where applicable, the processor, of the extension and the reasons for it within six weeks of the designated date.

(7) In this section, "**designated date**" means the later of –

(a) the date on which the Authority receives the request made by the controller, or

(b) if the Authority has requested information from the controller or processor within the six-week period following the date specified in paragraph (a), the date on which the Authority receives the information requested.

Prior consultation required for high-risk legislation.

38. (1) Where a public committee or any other public authority of the Bailiwick authorised to make or recommend the enactment of legislation proposes to make or recommend the enactment of high-risk legislation, the committee or other public authority must consult the Authority unless consultation with the Authority has already taken place.

(2) Failure to comply with subsection (1) does not invalidate any high-risk legislation made or enacted.

(3) In this section, "**high-risk legislation**" means a Law, an Ordinance or subordinate legislation (excluding an Ordinance or subordinate legislation made under the Law, or any subordinate legislation made under this Ordinance) that requires or authorises the processing of personal data for a law enforcement purpose in circumstances where that processing is likely to be high-risk

processing despite any safeguards in the legislation concerned for the protection of the significant interests of data subjects.

PART VII

DATA PROTECTION OFFICERS

Mandatory designation of data protection officer.

39. (1) Subject to subsections (2) and (3), a controller must designate an individual as a data protection officer.

(2) A group of competent authorities that are controllers may designate a single data protection officer for those competent authorities if –

(a) it is appropriate to do so, having regard to the organisational structure and size of those competent authorities, and

(b) in any case –

(i) the data protection officer is easily accessible from each competent authority in the group, and

(ii) the data protection officer allocates an appropriate and adequate proportion of the officer's time to the performance of the officer's functions under this Ordinance in relation to each competent authority in the group.

(3) Subsection (1) does not apply to a court or tribunal acting in its

judicial capacity.

Requirements for designation.

40. (1) A designating entity may designate an individual as a data protection officer under section 39 whether or not the individual is an employee of the designating entity.

(2) An individual must not be designated as a data protection officer under section 39 unless –

(a) the designating entity considers that the individual possesses the appropriate professional skills, knowledge and abilities to adequately perform the functions of a data protection officer under this Ordinance, and

(b) the individual satisfies any prescribed requirements.

(3) In this section and sections 41 and 42, "**designating entity**", in relation to a data protection officer –

(a) means the controller or group of competent authorities that designates or wishes to designate a data protection officer, and

(b) in the case of a group of competent authorities, includes each competent authority within the group.

Functions of data protection officers.

41. (1) A data protection officer must –

(a) inform and advise the officer's designating entity and its employees who carry out processing operations ("**relevant employees**") of their duties under this Ordinance and any other enactments relating to data protection,

(b) monitor the designating entity's compliance with –

(i) this Ordinance,

(ii) any other enactments relating to data protection,

(iii) the policies of the designating entity in relation to data protection, including in relation to the assignment of responsibilities, awareness-raising and training of relevant employees, and

(iv) any data protection audits required by or under the Law or this Ordinance,

(c) where requested, provide advice to the designating entity and relevant employees relating to data protection impact assessments and monitor the carrying out of such assessments,

(d) act as the contact point for the Authority on issues relating to processing, including any prior consultation required by section 37 and any other consultation with the Authority with regard to any other matter, and

(e) cooperate with the Authority in the exercise or performance of any of the Authority's functions under the Law or this Ordinance.

(2) In performing any function under this Ordinance, a data protection officer must have due regard to the risk associated with processing operations, taking into account the nature, scope, context and purpose of the processing concerned.

(3) Where a data protection officer is required to be designated under section 39, the controller must take reasonable steps to ensure that the officer carries out the officer's functions in accordance with this section.

Further duties in relation to data protection officers.

42. (1) Upon the designation of a data protection officer, the designating entity must –

(a) give written notice to the Authority of the name and contact details of the officer, and

(b) publish a notice stating –

(i) the fact that a data protection officer has been designated, and

(ii) the contact details of the officer.

(2) The designating entity must ensure that the data protection officer is involved, appropriately and in a timely manner, in all issues which relate to the protection of personal data within and by the designating entity.

(3) The designating entity must support the data protection officer in the performance of the officer's functions under this Ordinance by ensuring that –

(a) the officer reports directly to the highest tier of management of the designating entity,

(b) the officer does not receive any instructions regarding the performance of those functions, other than to perform those functions in a professional and competent manner and to the best of the officer's abilities,

(c) the officer is provided the resources necessary -

(i) to perform those functions,

(ii) to gain access to personal data and processing operations, and

(iii) to maintain the officer's expert knowledge,

(d) the officer is not dismissed or penalised for performing those functions, other than for failing to perform those functions in a professional and competent manner and to the best of the officer's abilities,

(e) data subjects are allowed to contact the officer directly with regard to any issues related to the processing of their personal data or the exercise of their rights under this Ordinance, and

(f) any other tasks and duties assigned to the officer do not result in a conflict of interest in relation to the performance of the officer's functions.

(4) Despite subsection (2), a controller may wholly or partly restrict the involvement of a data protection officer in an issue which relates to the protection of personal data for any appropriate reasons, for example where the controller considers the restriction necessary –

(a) to avoid obstructing an official or legal inquiry, investigation or procedure within or outside the Bailiwick,

(b) to avoid prejudicing the prevention, detection, investigation or prosecution of a criminal offence within or outside the Bailiwick,

(c) to avoid prejudicing any proceedings relating to a criminal offence within or outside the Bailiwick, or

(d) to protect public security or the security of the British Islands.

PART VIII

TRANSFERS TO OTHER JURISDICTIONS

Prohibition of transfers to other jurisdictions.

43. (1) Except where all four conditions in subsections (2) to (5) are satisfied, a controller must not cause or permit the transfer of personal data to a person in an unauthorised jurisdiction –

(a) for processing, or

(b) in circumstances where the controller knew or should have known that the personal data will be processed after the transfer.

(2) The condition in this subsection is satisfied if the transfer is necessary for a law enforcement purpose.

(3) The condition in this subsection is satisfied if the transfer meets the requirements of section 44(1) or 45(1).

(4) The condition in this subsection is satisfied if –

(a) the intended recipient is a relevant authority or a relevant international organisation, or

(b) the transfer meets the requirements of section 46(1).

(5) The condition in this subsection applies where the personal data was originally transmitted or otherwise made available to the controller or another competent authority by a person in an authorised jurisdiction (other than the Bailiwick), and is satisfied if –

(a) a relevant authority of the authorised jurisdiction has authorised the transfer in accordance with the law of the authorised jurisdiction, or

(b) the authorisation mentioned in paragraph (a) cannot be obtained in good time and the transfer was necessary to prevent an immediate and serious threat to public security or the national security or other essential interests of any country.

(6) Where a transfer is made without the authorisation mentioned in subsection (5)(a), the controller must, as soon as practicable, inform the relevant authority that would otherwise have been responsible for deciding whether to authorise the transfer.

(7) In this section and sections 44 to 47 –

"**the controller**" means the controller causing or permitting the transfer of personal data,

"**recipient**", includes the controller or processor of the personal data following its transfer, and

"**relevant international organisation**" means an international organisation that carries out functions for a law enforcement purpose.

Transfers on the basis of available safeguards.

44. (1) The requirements of this subsection are met if the controller is satisfied that appropriate safeguards exist for the protection of personal data –

(a) in a legally binding instrument, or

(b) otherwise in all the circumstances surrounding the transfer.

(2) Where a transfer takes place in reliance on meeting the requirements of subsection (1), the controller must record the transfer in writing and keep the record for a prescribed period.

(3) A record required to be kept by subsection (2) must include –

(a) the date and time of the transfer,

(b) the name of and any other pertinent information about the recipient,

(c) the justification for the transfer, and

(d) a description of the personal data transferred.

(4) The controller must notify the Authority of the categories of

data transferred in reliance on meeting the requirement in subsection (1)(b).

(5) Without limiting the generality of subsection (1)(a), an example of a legally binding instrument within the meaning of that provision is a legally binding and enforceable agreement between the controller and the recipient.

Transfers on the basis of special circumstances.

45. (1) The requirements of this subsection are met if the transfer is necessary –

(a) to protect the vital interests of the data subject or any other individual,

(b) to safeguard the legitimate interests of the data subject,

(c) to prevent an immediate and serious threat to the public security or national security of any country,

(d) in individual cases for any law enforcement purpose, or

(e) in individual cases –

(i) for the purpose of, or in connection with, any legal proceedings (including prospective legal proceedings) relating to a law enforcement purpose,

(ii) for the purpose of obtaining legal advice in relation to a law enforcement purpose, or

(iii) otherwise for the purposes of establishing, exercising or defending legal rights relating to a law enforcement purpose.

(2) Neither subsection (1)(d) nor (e) applies if the controller determines in any specific case that the significant interests of the data subject overrides the public interest in the transfer.

(3) Where a transfer takes place in reliance on meeting the requirements of subsection (1), the controller must record the transfer in writing and keep the record for a prescribed period.

(4) A record required to be kept by subsection (3) must include–

(a) the date and time of the transfer,

(b) the name of and any other pertinent information about the recipient,

(c) the justification for the transfer, and

(d) a description of the personal data transferred.

(5) The controller must notify the Authority of the categories of data transferred in reliance on meeting the requirements of subsection (1).

Transfers of personal data to persons other than relevant authorities.

46. (1) The requirements of this subsection are met if –

(a) the transfer is strictly necessary in a specific case for the performance of a function conferred or imposed by law on the controller for a law enforcement purpose,

(b) the controller has determined that no significant interests of the data subject override the public interest necessitating the transfer,

(c) the transferring controller considers that the transfer of the personal data to a relevant authority or to a relevant international organisation would be ineffective or inappropriate, and

(d) the controller informs the recipient of the specific purpose for which the personal data may, so far as is necessary, be processed.

(2) Without limiting the generality of subsection (1)(c), an example of where the transfer of the personal data to a relevant authority or to a relevant international organisation would be ineffective or inappropriate is where the transfer could not be made in sufficient time to enable its purpose to be fulfilled.

(3) Where personal data is transferred to a person in an unauthorised jurisdiction, other than a relevant authority of the unauthorised jurisdiction or a relevant international organisation, in reliance on meeting the requirements of subsection (1), the controller must –

(a) inform a relevant authority of the unauthorised jurisdiction of the transfer as soon as practicable, unless this would be ineffective or inappropriate, and

(b) record the transfer in writing and keep the record for a prescribed period.

(4) A record required to be kept by subsection (3)(b) must include–

(a) the date and time of the transfer,

(b) the name of and any other pertinent information about the recipient,

(c) the justification for the transfer, and

(d) a description of the personal data transferred.

(5) The controller must notify the Authority of the categories of data transferred in reliance on meeting the requirements of subsection (1).

(6) This section does not limit or affect the operation of any international agreement in force between the Bailiwick and any other country in the field of judicial co-operation in criminal matters and police co-operation.

Subsequent transfers

47. (1) Where personal data is transferred to any person in an unauthorised jurisdiction as permitted by section 43, the transferring controller must

make it a condition of the transfer that the data is not to be further transferred to any other person in an unauthorised jurisdiction without the authorisation of –

(a) the transferring controller, or

(b) another competent authority of the Bailiwick or an authorised jurisdiction.

(2) A competent authority must not give an authorisation unless the further transfer is necessary for a law enforcement purpose.

(3) In determining whether or not to give an authorisation, the competent authority must take into account —

(a) the seriousness of the circumstances leading to the request for authorisation,

(b) the purpose for which the personal data was originally transferred,

(c) the standards for the protection of personal data that apply in the unauthorised jurisdiction to which the personal data would be further transferred, and

(d) any other relevant matters.

(4) Subsections (5) and (6) apply in any case where the personal data was originally transmitted or otherwise made available to the controller or

another competent authority by a relevant authority of an authorised jurisdiction other than the Bailiwick.

(5) A competent authority must not give an authorisation unless –

(a) the relevant transmitting authority has given permission for the further transfer in accordance with the law of the authorised jurisdiction concerned, or

(b) the transfer –

(i) is necessary to prevent an immediate and serious threat to the public security, national security or other essential interests of any country, and

(b) the permission mentioned in paragraph (a) cannot be obtained in good time.

(6) Where a transfer is made without the permission mentioned in subsection (5)(a), the controller must inform the relevant transmitting authority as soon as practicable.

(7) In this section –

"**authorisation**" means an authorisation given for the purposes of subsection (1),

"**further transfer**" means the further transfer mentioned in

subsection (1), for which an authorisation is required, and

"**relevant transmitting authority**" means the relevant authority mentioned in subsection (4).

PART IX

GENERAL AND MISCELLANEOUS

General exceptions and exemptions.

48. Schedule 3 has effect.

General provisions as to regulations.

49. (1) Regulations under this Ordinance -

(a) may be amended or repealed by subsequent regulations hereunder,

(b) may contain such consequential, incidental, supplemental and transitional provision as may appear to the Committee to be necessary or expedient, and

(c) must be laid before a meeting of the States of Deliberation as soon as possible and, if at that or the next meeting the States of Deliberation resolve to annul them, cease to have effect, but without prejudice to anything done under them or to the making of new regulations.

(2) Any power conferred by this Ordinance to make regulations

may be exercised -

(a) in relation to all cases to which the power extends, or in relation to all those cases subject to specified exceptions, or in relation to any specified cases or classes of cases,

(b) so as to make, as respects the cases in relation to which it is exercised -

(i) the full provision to which the power extends, or any lesser provision (whether by way of exception or otherwise),

(ii) the same provision for all cases, or different provision for different cases or classes of cases, or different provision for the same case or class of case for different purposes,

(iii) any such provision either unconditionally or subject to any conditions specified in the regulations.

(3) Without prejudice to the generality of the other provisions of this Ordinance, regulations under this Ordinance –

(a) may, subject to subsection (4), make provision in relation to the creation, trial (summarily or on indictment) and punishment of offences,

(b) may empower the Authority, any public committee, any other body or authority (including, without limitation, any court of the Bailiwick), or any other person to issue codes or guidance in relation to any matter for which regulations may be made under this Ordinance, and

(c) may repeal, replace, amend, extend, adapt, modify or disapply any rule of custom or law.

(4) Regulations under this Ordinance may not –

(a) provide for offences to be triable only on indictment, or

(b) authorise the imposition –

(i) on summary conviction, of imprisonment for a term exceeding 12 months, or a fine exceeding level 5 on the uniform scale, or

(ii) on conviction on indictment, of imprisonment for a term exceeding two years.

(5) Before making any regulations under this Ordinance, the Committee must consult –

(a) the Authority,

(b) in the case of regulations having effect in Alderney, the Policy and Finance Committee of the States of Alderney, and

(c) in the case of regulations having effect in Sark, the Policy and Performance Committee of the Chief Pleas of Sark,

in relation to the terms of the proposed regulations; but a failure to comply with this subsection does not invalidate any regulations made under this Ordinance.

Interpretation.

50. (1) In this Ordinance, unless the context requires otherwise –

"**authorised jurisdiction**" means –

(a) the Bailiwick,

(b) a Member State of the European Union,

(c) any country, any sector within a country, or any international organisation that the Commission has determined ensures an adequate level of protection within the meaning of Article 36 of the Law Enforcement Directive (or the equivalent article of the former Directive), and for which the determination is still in force, or

(d) a designated jurisdiction,

"**competent authority**" means –

(a) any of the following persons, when exercising or performing a function conferred or imposed on the person by law or by a States Resolution for a law enforcement purpose –

(i) the States,

(ii) a public committee,

(iii) a holder of a public office,

(iv) a statutory body,

(v) a court or tribunal of the Bailiwick,

(vi) any person hearing or determining an appeal, or conducting a public inquiry, under any enactment,

(vii) the salaried police force of the Island of Guernsey or any police force which may be established by the States of Alderney or Chief Pleas of Sark,

(viii) a parish Douzaine of the Island of Guernsey or the Douzaine of the Island of Sark, or

(ix) any person exercising or performing functions or holding any office similar or comparable to any of the persons described in subparagraphs (i) to (viii) in respect of any country other than the Bailiwick, or

(b) any other person that exercises or performs any function that is of a public nature in respect of the Bailiwick or any other country, when exercising or performing a function that is of a public nature in respect of the Bailiwick or any other country for a law enforcement purpose, or

(c) any other prescribed person,

"**the complaints and appeals information**" means –

(a) information as to the existence of –

(i) the right to complain to the Authority under section 67 of the Law, and

(ii) a complainant's rights of appeal under sections 82 and 83 of the Law, and

(b) the contact details of the Authority,

"**criminal proceeds enactment**" means –

(a) any of the following enactments, including any Ordinance or subordinate legislation made under any of them –

(i) the Criminal Justice (Proceeds of Crime) (Bailiwick of Guernsey) Law, 1999[c],

(ii) the Drug Trafficking (Bailiwick of Guernsey) Law, 2000[d],

(iii) the Terrorism and Crime (Bailiwick of Guernsey) Law, 2002[e],

---

c Ordres en Conseil Vol. XXXIX, p. 137; amended by Order in Council No. I of 2000; No. II of 2005; No. XV of 2007; No. XIII of 2010; No. XI of 2011; Recueil d'Ordonnances Tome XXVIII, p. 266; Ordinance No. XII of 2002; No. XXXIII of 2003; No. XLVII of 2007; No. XXXVII of 2008; Nos. XVI and XXXIV of 2010; No. XVII of 2014; No. IX of 2016; No. XVIII of 2017; G.S.I. No. 56 of 1999; G.S.I. Nos. 4 and 27 of 2002; G.S.I. No. 33 of 2007; G.S.I. Nos. 48 and 73 of 2008; G.S.I. No. 12 of 2010; G.S.I. No. 14 of 2013; G.S.I. No. 45 of 2016.

d Order in Council No. VII of 2000; as amended by No. I of 2000; No. II of 2005; Nos. XVI and XVII of 2007; No. XVII of 2008; No. XIII of 2010; Ordinance No. XXXIII of 2003; No. XXXVIII of 2008; Nos. XV and XXV of 2010; No. XVI of 2014; and No. IX of 2016.

e Order in Council No. XVI of 2002; as amended by No. I of 2000; No. VII of 2005; No. XIII of 2006; No. XIII of 2010; No. XI of 2011; No. XIV of 2012; Ordinance No. XXXIII of 2003; No. XLVI of 2007; Nos. XIII, XX and XXXVII of 2010; Nos. XXIX and LIV of 2014; No. IX of 2016; G.S.I. No. 16 of 2003; No. 41 of 2005; No. 5 of 2017.

(iv) the Criminal Justice (Fraud Investigation) (Bailiwick of Guernsey) Law, 1991[f],

(v) the Criminal Justice (International Cooperation) (Bailiwick of Guernsey) Law, 2001[g],

(vi) the Forfeiture of Money etc. in Civil Proceedings (Bailiwick of Guernsey) Law, 2007[h],

(vii) the Disclosure (Bailiwick of Guernsey) Law, 2007[i],

(viii) the Beneficial Ownership of Legal Persons (Guernsey) Law, 2017[j], or

(ix) the Beneficial Ownership of Legal Persons (Alderney) Law, 2017[k], or

---

[f] Ordres en Conseil Vol. XXXIII, p. 81; as amended by Order in Council No. I of 2000; No. II of 2003; No. XIII of 2010; Ordinance No. XXXIII of 2003; and No. VII of 2009.

[g] Order in Council No. VII of 2001; as amended by No. I of 2000; No. IX of 2008; Ordinance No. XXXVIII of 2010 and No. XXIX of 2013.

[h] Order in Council No. XVII of 2008; as amended by No. XIII of 2010; No. XVI of 2012; Ordinance No. XXX of 2008; No. VII of 2009; No. XX of 2015; No. IX of 2016.

[i] Order in Council No. XVI of 2007; as amended by No. XXXIX of 2008; Ordinance No. VII of 2009; Nos. XIV, XIX and XXXVII of 2010; Nos. XVI and LIII of 2014; No. XXXIX of 2015; No. IX of 2016.

[j] Order in Council No. VI of 2017; as amended by Ordinance No. XXVIII of 2017.

(b) any enactment, in any country outside the Bailiwick, that is similar or comparable in purpose or effect to an enactment mentioned in paragraph (a),

"**data protection impact assessment**" means an assessment carried out in accordance with section 36,

"**data protection officer**" means an individual designated as a data protection officer under section 39,

"**data protection principle**" means a principle specified in any of sections 5 to 10,

"**data subject right**" means a right conferred on a data subject by or under Part III,

"**enactment**" includes –

(a) an Act of Parliament that extends to the Bailiwick, and

(b) a Law, an Ordinance and any subordinate legislation and includes any provision or portion of a Law, an Ordinance or any subordinate legislation,

"**fairly**", in relation to processing, is to be construed in light of Recitals (26) and (42) of the Law Enforcement Directive,

---

k Order in Council No. VII of 2017; as amended by Alderney Ordinance No. X of 2017.

"**the former Commissioner**" means the Data Protection Commissioner under the Data Protection (Bailiwick of Guernsey) Law, 2001[1],

"**the Law**" means the Data Protection (Bailiwick of Guernsey) Law, 2017,

"**law enforcement purpose**" means the purpose of –

(a) prevention, investigation, detection or prosecution of a criminal offence within or outside the Bailiwick,

(b) the execution of criminal penalties within or outside the Bailiwick,

(c) safeguarding against or preventing threats to public security or the security of the British Islands, or

(d) exercising or performing any power or duty conferred or imposed on a public authority by a criminal proceeds enactment,

"**lawfully**", in relation to processing, has the meaning given by section 5(2) to (7),

"**operative provision**" means any provision of Parts II to VIII,

---

1 Order in Council No. V of 2002; as amended by Ordinance No. XXXIII of 2003; No. II of 2010; No. XXXIV of 2011; No. XLIX of 2012; No. XXIX of 2013; and No. IX of 2016.

"**prejudice**" includes hinder, seriously impair or prevent,

"**prescribed**", in relation to any provision of this Ordinance, means prescribed by regulations for the purposes of the provision,

"**proceedings relating to a criminal offence**" includes –

(a) any proceedings for the purpose of executing a criminal penalty,

(b) any proceedings under or for the purposes of a criminal proceeds enactment, and

(c) the exercise or performance of any power or duty conferred or imposed on a public authority by a criminal proceeds enactment,

"**public security**" includes –

(a) the health or safety of the population,

(b) the security of any infrastructure facility, information systems or communications network, which if prejudiced may endanger human life, and

(c) the economic or environmental security,

of the whole or any part of the British Islands or any country outside the British Islands,

"**recipient**", in relation to personal data, means any person to which the personal data is disclosed,

"**regulations**" means regulations made by the Committee in accordance with section 49,

"**relevant authority**" –

(a) means any person in a jurisdiction that has, in respect of that jurisdiction, functions comparable to those of a competent authority, and

(b) includes an authority competent for the purposes referred to in Article 1(1) of the Law Enforcement Directive,

"**restriction of processing**", in relation to personal data –

(a) means the marking of stored personal data with the aim of limiting its processing in the future, and

(b) includes restricting or otherwise limiting the processing of that personal data in a manner and for a period of time under section 14(5) or 15(5) or (6), and

"**restrict the processing**", in relation to personal data, has a corresponding meaning,

"**subordinate legislation**" means any regulation, rule, order, rule of court, resolution, scheme, byelaw or other instrument made under any statutory, customary or inherent power and having legislative effect, but does not include an Ordinance, and

"**unauthorised jurisdiction**" means any country, sector in a country or international organisation that is not an authorised jurisdiction.

(2) The Committee may by regulations amend the definition of "**criminal proceeds enactment**" in subsection (1).

(3) A reference in this Ordinance to a provision of the Law includes a reference to any Ordinance or regulations made under, or any Schedule given effect by, the provision.

(4) An expression used in this Ordinance that is also used in the Law Enforcement Directive has the same meaning as in that Directive unless –

(a) the expression is otherwise defined in this Ordinance, or

(b) the context requires otherwise.

(5) The Interpretation (Guernsey) Law, 1948[m] applies to the

---

[m] Ordres en Conseil Vol. XIII, p. 355.

interpretation of this Ordinance throughout the Bailiwick of Guernsey.

(6) Any reference in this Ordinance to an enactment or a Community provision is a reference thereto as from time to time amended, re-enacted (with or without modification), extended or applied.

Citation.

51. This Ordinance may be cited as the Data Protection (Law Enforcement and Related Matters) (Bailiwick of Guernsey) Ordinance, 2018.

Commencement.

52. This Ordinance shall come into force on the 25th May, 2018.

SCHEDULE 1

Section 3(1)

MODIFICATIONS TO THE LAW FOR COMPETENT AUTHORITIES PROCESSING FOR A LAW ENFORCEMENT PURPOSE

Provision of the Law	**Modifications**
Section 11(2)	For "Part III of this Law", substitute "Part III of the Law Enforcement Ordinance".
Section 73(2)	At the end of paragraph (e)(iii), immediately after the comma, insert "and". At the end of paragraph (f), for ", and", substitute a full stop. Omit paragraph (g).
Section 73(7) and (7A)	For these subsections, substitute the following subsection – "(7) In determining what, if any, order to make under subsection (2) in any case where a controller or processor has breached an operative provision, the Authority must have regard to – (a) the nature, gravity and duration of the breach concerned, taking into account – (i) the nature, scope and purpose of the processing concerned, (ii) the categories of personal data affected by the breach, (iii) the number of data subjects affected, and (iv) the level of any damage suffered by these data subjects, (b) the manner in which the breach became known to the Authority, in particular whether, and if so to what extent, the person concerned notified the breach to the Authority, (c) whether the breach was intentional or negligent, (d) the degree of responsibility of the person concerned, taking into account technical and organisational measures implemented by that person for the purposes of any provision of this Law, (e) any relevant previous breaches by the person concerned,

Provision of the Law	Modifications
	(f) the degree to which the person concerned has cooperated with the Authority to remedy the breach and mitigate its possible adverse effects, (g) any other action taken by the person concerned to mitigate any damage suffered by data subjects, (h) where an enforcement order has previously been issued to the person concerned with regard to the same subject-matter, the actions taken in compliance with the order, (i) any other aggravating or mitigating factor applicable to the circumstances of the case.".
Sections 74 and 75	Omit these sections.
Section 111(1)	In the definition of "**data subject right**", immediately after "Part III" insert "of the Law Enforcement Ordinance". In the definition of "**operative provision**", for "Parts II to X of this Law", substitute "Parts II to VIII of the Law Enforcement Ordinance". Insert the following definition in the appropriate alphabetical order – " "**Law Enforcement Ordinance**" means the Data Protection (Law Enforcement and Related Matters) (Bailiwick of Guernsey) Ordinance, 2018,".

SCHEDULE 2

Section 5(4)(b)

CONDITIONS FOR LAWFUL PROCESSING OF SPECIAL CATEGORY DATA

1. The information contained in the personal data has been made public as a result of steps deliberately taken by the data subject.

2. The processing is necessary for the controller to exercise any right or power, or perform or comply with any duty, conferred or imposed on the controller by an enactment or otherwise by law.

3. The processing is necessary in order to comply with an order or a judgment of a court or tribunal having the force of law in the Bailiwick.

4. The processing is necessary –

(a) for the purpose of, or in connection with –

(i) any legal proceedings (including prospective legal proceedings), or

(ii) the discharge of any functions of a court or tribunal acting in its judicial capacity,

(b) for the purpose of obtaining legal advice, or

(c) otherwise for the purposes of establishing, exercising or defending legal rights.

5. The processing is necessary for –

(a) the administration of justice, or

(b) the exercise of any function of the Crown, a Law Officer of the Crown, the States or a public committee.

6. The processing is necessary for a historical or scientific purpose.

7. The processing is –

(a) authorised by regulations made by the Committee for this purpose and carried out in accordance with those regulations, or

(b) authorised or required by any other enactment and carried out in accordance with the enactment.

8. The data subject has given consent to the processing of the personal data for the purpose for which it is processed.

9. The processing is necessary to protect the vital interests of the data subject or any other individual, and –

(a) the data subject is physically or legally incapable of giving consent, or

(b) the controller cannot reasonably be expected to obtain the consent of the data subject.

10. (1) The processing—

(a) is necessary for the purposes of preventing fraud or a particular kind of fraud, and

(b) consists of —

(i) the disclosure of personal data by a competent authority as a member of an anti-fraud organisation,

(ii) the disclosure of personal data by a competent authority in accordance with arrangements made by an anti-fraud organisation, or

(iii) the processing of personal data disclosed as described in sub-item (i) or (ii).

(2) In this paragraph, "**anti-fraud organisation**" means any unincorporated association, body corporate or other person which –

(a) enables or facilitates any sharing of information to prevent fraud or a particular kind of fraud, or

(b) has, as its purpose or one of its purposes, the sharing of information to prevent fraud or a particular kind of fraud.

SCHEDULE 3

Section 48

GENERAL EXCEPTIONS AND EXEMPTIONS

1. **Disclosure to relevant bodies to protect individuals from serious harm**.

(1) The disclosure of personal data to a relevant body is exempt from a provision of Part III that prohibits or restricts such a disclosure, to the extent that the disclosure is necessary for the purpose of protecting the data subject or any other individual from serious harm.

(2) In subparagraph (1), "**relevant body**" means a public authority or any other body, association or agency that has as an object or function, or as any part of its objects or functions, the protection of individuals from serious harm.

2. Disclosure required by law, etc.

The disclosure of personal data to any person is exempt from a provision of Part III that prohibits or restricts such a disclosure, to the extent that the disclosure is necessary –

(a) to comply with a duty imposed –

(i) by or under any enactment,

(ii) by any rule of law, or

(iii) by the order of a court or tribunal, or

(b) for the purpose of, or in connection with, any legal proceedings (including prospective legal proceedings),

(c) for the purpose of obtaining legal advice, or

(d) otherwise for the purposes of establishing, exercising or defending legal rights.

3. Privileged items.

Privileged items are exempt from a provision of Part III.

4. Armed forces.

Personal data is exempt from a designated provision to the extent that the application of the provision to the data would be likely to prejudice the combat effectiveness of any of the armed forces of the Crown.

5. Negotiations.

(1) A negotiation record is exempt from a designated provision to the extent that the application of the provision to the record would be likely to prejudice those negotiations.

(2) In subparagraph (1), "**negotiation record**" means a record of the intentions of the controller in relation to any negotiations with the data subject.

6. Self-incrimination.

(1) Personal data is exempt from a designated provision to the extent that the application of the provision to the data would be likely to expose

the controller to proceedings for an offence by revealing evidence of the commission of the offence.

(2) In subparagraph (1), "**offence**" excludes –

(a) an offence under the Law,

(b) perjury, or

(c) perverting the course of justice.

7. J**udicial independence and judicial proceedings**.

Personal data is exempt from a designated provision to the extent that the application of the provision to the data would be likely to prejudice judicial independence or the conduct of judicial proceedings.

8. Public information.

(1) Public information is exempt from –

(a) section 12 of this Ordinance, including any designated provision corresponding to a right or duty in that section of this Ordinance, and

(b) any other designated provision, to the extent that the application of the provision to the information would be likely to prejudice the purpose of requiring that information to be published.

(2) In subparagraph (1), "**public information**" includes –

(a) information which the controller is required to publish by law, and

(b) information held on a public register.

9. <u>Historical or scientific information</u>.

Personal data processed for a historical or scientific purpose is exempt from a designated provision to the extent that the application of the provision to the data would be likely to prejudice the historical or scientific purpose for which that data is processed.

10. <u>Tax and crime information</u>.

(1) The exemption in each of subparagraphs (2) and (3) apply to personal data processed for –

(a) a law enforcement purpose, or

(b) the assessment or collection within or outside the Bailiwick of any tax, duty, or other imposition of a similar nature, including any interest or penalty required to be paid as a result of late payment or non-payment of such a tax, duty or other imposition.

(2) Personal data is exempt from a designated provision (other than the lawfulness principle) to the extent that the application of the provision to the personal data would be likely to prejudice a purpose specified in subparagraph (1)(a) or (b).

(3) Personal data that consists of a classification applied to the data subject as part of a system of risk assessment which is operated by a public authority for a purpose specified in subparagraph (1)(a) or (b) is exempt from a designated provision (other than the lawfulness principle) to the extent that the application of the provision to that personal data would be likely to prejudice the operation of the system of risk assessment.

11. <u>Prejudice to international obligations, etc.</u>

Personal data is exempt from a designated provision (other than the lawfulness principle) to the extent that the application of the provision to the personal data would be likely to –

(a) breach an international obligation of the Bailiwick, or

(b) otherwise prejudice the ability of the Bailiwick to meet its international obligations.

12. <u>Protective functions</u>.

(1) This paragraph applies to personal data processed in the discharge of a protective function that –

(a) is conferred or imposed by an enactment on any person,

(b) is a function of the Crown, a Law Officer of the Crown, the States or a public committee, or

(c) is of a public nature and is exercised in the public interest.

(2) Personal data is exempt from a designated provision to the extent that the application of the provision to the personal data would be likely to prejudice the proper discharge of the protective function.

(3) In this paragraph, "**protective function**" means –

(a) the protection of members of the public against –

(i) financial loss due to dishonesty, malpractice or other seriously improper conduct by, or the unfitness or incompetence of, persons concerned in the provision of banking, insurance, investment, fiduciary, trustee services or other financial services or in the establishment or management of any body corporate, limited partnership with legal personality or foundation,

(ii) financial loss due to the conduct of a person that is bankrupt or otherwise insolvent,

(iii) dishonesty, malpractice or other seriously improper conduct by, or the unfitness or incompetence of, persons authorised to carry on any profession or other activity,

(iv) maladministration by any public authority,

(v) failure in the services provided by any public authority, or

(vi) a failure of a public authority to provide a service which it is a function of the public authority to provide,

(b) the protection of non-profit organisations or charities against misconduct or mismanagement (whether by trustees, directors or other persons) in their administration,

(c) the protection of the property of non-profit organisations or charities from loss or misapplication,

(d) the recovery of the property of non-profit organisations or charities,

(e) the securing of the health, safety and welfare of persons at work,

(f) the protection of persons other than those at work against risk to health or safety arising out of or in connection with the action of persons at work, or

(g) the protection of the reputation and standing of the Bailiwick.

(4) Any power or duty conferred or imposed on a person by a criminal proceeds enactment is deemed to be a protective function within the meaning of subparagraph (1).

13. <u>Regulatory purposes.</u>

(1) Personal data processed for a regulatory purpose is exempt from a designated provision to the extent to which the application of the provision to the data would be likely to prejudice the regulatory purpose.

(2) In this paragraph –

"**administrative offence**" means any offence, breach or other transgression (which may include a disciplinary offence) punishable by any measures under and in accordance with any enactment, other than by way of criminal proceedings, and

"**regulatory purpose**" means –

(a) prevention, investigation, detection, determination or punishment of an administrative offence,

(b) carrying out the measures imposed as punishment of an administrative offence, or

(c) determination by a public authority of an application for a registration, licence, approval or any other kind of authorisation or consent, in accordance with an enactment.

14. **<u>Disclosures prohibited or restricted by enactments.</u>**

(1) Personal data the disclosure of which is prohibited or restricted by an enactment is exempt from a designated provision.

(2) Without limiting the generality of subparagraph (1), examples of such enactments include –

(a) in relation to Guernsey, sections 17, 20A and 20B of the Adoption (Guernsey) Law, 1960[n], and

(b) in relation to Alderney, sections 17, 20A and 20B of the Adoption (Guernsey) Law, 1960, as extended to Alderney by the Alderney (Application of Legislation) (Adoption) Ordinance, 1974[o].

15. Court-directed exemptions.

(1) Personal data withheld by a court or tribunal is exempt from a designated provision.

(2) Personal data is withheld by a court or tribunal if –

(a) it is processed by a court or tribunal,

(b) it is supplied in a report or other evidence given to the court or tribunal in the course of any legal proceedings by or on behalf of –

---

[n] Ordres en Conseil, Vol. XVIII, p. 192; amended by Vol. XXI, p. 34; Vol. XXII, pp. 380 and 521; Vol. XXIII, p. 26; Vol. XXXI, p. 278; Vol. XXXVII, p. 130; Order in Council No. XII of 2000; No. III of 2001; Ordinance No. XXXIII of 2003; No. VII of 2010; No. IX of 2016.

[o] Recueil d'Ordonnances Tome XIX, p. 247; as amended by Ordinance No. XXXIII of 2003; No. IX of 2016.

(i) a probation officer,

(ii) a health professional,

(iii) an educational establishment,

(iv) a public committee, or

(v) any other person or body, and

(c) the court or tribunal directs that the personal data should be withheld from the data subject on the ground that it appears to be –

(i) impracticable to disclose the report or other evidence to the data subject having regard to the age and understanding of the data subject, or

(ii) undesirable to do so having regard to potential serious harm which might be suffered by the data subject as a result of such disclosure.

16. **Serious harm to data subjects or other individuals**.

(1) Any educational data, health data or social assistance data is exempt from a designated provision to the extent that the application of the provision to the data would be likely to cause serious harm to the data subject or any other individual.

(2) A non-health controller must not give a person any information (whether or not in response to a request), or take any action, in respect of any health data in accordance with a designated provision, unless the controller has first consulted the appropriate health professional on whether or not the exemption in subparagraph (1) applies in respect of the health data.

(3) Subparagraph (2) does not apply to the extent that the non-health controller is satisfied that –

(a) the health data has previously been seen by, or is already within the knowledge of, the data subject, or

(b) within the period of six months before the controller gives the person the information, or takes the action, the appropriate health professional has given the controller an opinion to the effect that the exemption in subparagraph (1) applies or does not apply in respect of the health data.

(4) In subparagraphs (2) and (3) –

"**appropriate health professional**" means –

(a) the health professional who is currently or was most recently responsible for the clinical care of the data subject in connection with the matters to which the health data relates,

(b) where there is more than one such health professional,

the health professional who is the most suitable to advise on the matters to which the health data relates, or

(c) where –

(i) there is no health professional available falling within item (a) or (b), or

(ii) the controller is the States of Guernsey Committee for Employment and Social Security and the health data is processed in connection with the exercise of the functions conferred on the committee by or under the Social Insurance (Guernsey) Law, 1978[p], the Health Service (Benefit) (Guernsey) Law, 1990[q] or any other of its functions in relation to social or health protection,

---

[p] Ordres en Conseil Vol. XXVI, p. 292; amended by Vol. XXVII, pp. 238, 307 and 392; Vol. XXIX, pp. 24, 148 and 422; Vol. XXXI, p. 278; Vol. XXXII, p. 59; Vol. XXXIV, p. 510; Vol. XXXV(1), p. 161; Vol. XXXVI, pp. 123 and 343; Vol. XXXVIII, p. 59; Vol. XXXIX, p. 107; Order in Council No. X of 2000, No. IX of 2001, No. XXIII of 2002, No. XXIV of 2003, No. XI of 2004, No. XVIII of 2007; Nos. VII and XLII of 2009; No. XVII of 2011; No. XXXVIII of 2012; No. XXX of 2013; No. IX of 2016.

[q] Ordres en Conseil Vol. XXXII, p. 192; as amended by Order in Council No. IX of 2003 and No. II of 2011; Recueil d'Ordonnances Tome XXVI, pp. 177 and 483; Ordinance Nos. XXII and XXVII of 2002; No. XXXIII of 2003; No. XLII of 2006; No. XLIII of 2007; No. XXII of 2015; No. IX of 2016; No. XXV of 2017. The Law is applied, with modifications to the Island of Alderney by Recueil d'Ordonnances Tome XXV, p. 204.

a health professional who has the necessary experience and qualifications to advise on the matters to which the health data relates, and

"**non-health controller**" means any controller who is not a health professional.

17. **Requests by persons with parental responsibility or court-appointed administrators.**

(1) This paragraph applies where a person falling within subparagraph (2) –

(a) is authorised by or under any enactment or rule of law to make a request under a provision of Part III on behalf of a data subject, and

(b) has made such a request.

(2) A person falls within this subparagraph if –

(a) the data subject is a child, and that person has parental responsibility for that data subject, or

(b) the data subject is incapable of managing the data subject's own affairs, and that person has been appointed by a court to manage those affairs (for example, as a curateur).

(3) Personal data relating to whether the data subject is or has been the subject of or may be at risk of child abuse is exempt from a

designated provision to the extent that the application of the provision to the personal data would not be in the best interests of the data subject.

(4) Health data or social assistance data relating to the data subject is exempt from a designated provision to the extent that the application of the provision to the health data would disclose information –

(a) provided by the data subject in the expectation that it would not be disclosed to the person making the request,

(b) obtained as a result of any examination or investigation to which the data subject consented in the expectation that the information would not be so disclosed, or

(c) which the data subject has expressly indicated should not be so disclosed.

(5) Neither subparagraph (4)(a) nor (4)(b) applies where the data subject has expressly indicated that the data subject no longer has the expectation mentioned in those subparagraphs.

(6) In subparagraph (3), "**child abuse**" includes –

(a) physical injury (other than accidental injury) to a child,

(b) physical or emotional neglect of a child,

(c) ill-treatment of a child, or

(d) sexual abuse of a child.

18. Public security, etc.

(1) Personal data is exempt from any provision of Parts II to VIII of this Ordinance to the extent that the application of the provision ("**exemptable provision**") to the data would be likely to prejudice public security or the security of the British Islands.

(2) Subject to subparagraph (4), a certificate signed by Her Majesty's Procureur certifying that exemption from one or more exemptable provisions specified in the certificate is or at any time was required for the purposes of subparagraph (1) in respect of any personal data is conclusive evidence of that fact.

(3) A certificate under subparagraph (2) –

(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.

(4) Any person directly affected by the issuing of a certificate under subparagraph (2) may appeal to the Royal Court against the certificate.

(5) If on an appeal under subparagraph (4), the Royal Court finds that, applying the principles applied by the court on an application for

judicial review, Her Majesty's Procureur did not have reasonable grounds for issuing the certificate, the court may –

(a) allow the appeal, and

(b) quash the certificate.

(6) Where in any proceedings under the Law it is claimed by a controller that a certificate under subparagraph (2) which identifies the personal data to which it applies by means of a general description applies to any personal data, any other party to the proceedings may appeal to the Royal Court on the ground that the certificate does not apply to the personal data in question.

(7) But, subject to any determination under subparagraph (8), the certificate is to be conclusively presumed so to apply.

(8) On an appeal under subparagraph (6), the Royal Court may determine that the certificate does not so apply.

(9) A document purporting to be a certificate under subparagraph (2) must be –

(a) received in evidence, and

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

(10) A document which purports to be certified by or on behalf of Her Majesty's Procureur as a true copy of a certificate issued by Her

Majesty's Procureur under subparagraph (2) must be regarded in any legal proceedings as evidence of the certificate.

(11) For the avoidance of doubt, no power conferred by a provision of Part XI or XII of the Law may be exercised in relation to personal data which by virtue of this paragraph is exempt from the provision concerned.

19. Committee may make further exceptions and exemptions.

(1) The Committee may by regulations –

(a) provide for modifications to, and further exceptions to or exemptions from, any designated provision, and

(b) amend this Schedule for the purpose specified in item (a).

(2) The modifications, exceptions and exemptions provided for by regulations under subparagraph (1) may be in addition to, or in substitution of, any modifications, exceptions or exemptions specified in this Schedule before those regulations are made.

Interpretation of this Schedule

20. Interpretation.

In this Schedule –

"**a provision of Part III**" means –

(a) any provision of Part III of this Ordinance, and

(b) any provision of sections 4 to 10 of this Ordinance corresponding to a right or duty in Part III of this Ordinance,

"**designated provision**" means –

(a) any provision of Part III of this Ordinance,

(b) any provision of sections 4 to 10 this Ordinance corresponding to a right or duty in Part III of this Ordinance, or

(c) section 35 of this Ordinance,

"**educational data**" means any personal data which –

(a) is processed by or on behalf of the proprietor of, or a teacher at, a school,

(b) relates to any person who is or has been a pupil at the school, and

(c) originates from or is supplied by or on behalf of –

(i) a teacher or other employee at the school,

(ii) an individual engaged by the proprietor of the school or working at a school under a contract for the provision of educational services,

(iii) the pupil to whom the data relates, or

(iv) a parent of that pupil,

"**the lawfulness principle**" means the principle in section 5(1) of this Ordinance that personal data must be processed lawfully,

"**proprietor**" in relation to a school in the Bailiwick, means the person or body of persons responsible for the management of the school,

"**school**" has the meaning given by section 1(1) of the Education (Guernsey) Law, 1970[r],

"**serious harm**", in relation to any individual –

(a) means serious harm to the physical or mental health or condition of the individual, and

(b) includes psychological or bodily injury, and

"**social assistance data**" means personal data –

---

[r] Ordres en Conseil Vol. XXII, p.318; Vol. XXVI, p. 107, Vol. XXVII, p. 347; Vol. XXVIII, p. 181; Vol. XXX, p. 179; Vol. XXXI, p. 168 and Vol. XXXII, p. 144.

(a) processed by the States of Guernsey Committee for Employment & Social Security or any other person in connection with the allocation of housing or other residential accommodation,

(b) processed by the States of Guernsey Committee for Employment & Social Security in connection with the payment of supplementary benefit under the Supplementary Benefit (Guernsey) Law, 1971[s], or

(c) processed by the States of Guernsey Committee for Health & Social Care in connection with the carrying out of its functions under the States Children Board and Public Assistance (Amendment) (Guernsey) Law, 1970[t].

---

[s] Ordres en Conseil Vol. XXIII, p. 26; amended by Vol. XXVI, p. 292; Vol. XXXI, p. 278; Vol. XXXIX, p. 107; Order in Council No. XIII of 2014; No. VII of 2015; Recueil d'Ordonnances Vol. XXVI, p. 177; Ordinance No. XXXIII of 2003; No. VII of 2010; No. IX of 2016.

[t] Ordres en Conseil Vol. XXII, p. 521; as amended by Vol. XXXII, p. 155; Ordinance No. VII of 2010). See also Order in Council No. XIV of 2009; Ordinance No. XXXIII of 2003; No. IX of 2016.