THE DATA PROTECTION (BAILIWICK OF GUERNSEY) LAW, 2017

The States are asked to decide:-

Whether they are of the opinion to approve the draft Projet de Loi entitled "The Data Protection (Bailiwick of Guernsey) Law, 2017", and to authorise the Bailiff to present a most humble petition to Her Majesty praying for Her Royal Sanction thereto.

This proposition has been submitted to Her Majesty's Procureur for advice on any legal or constitutional implications in accordance with Rule 4(1) of the Rules of Procedure of the States of Deliberation and their Committees.

EXPLANATORY MEMORANDUM

The Law repeals and replaces the current Data Protection (Bailiwick of Guernsey) Law, 2001 with provisions to 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 and consistent with the General Data Protection Regulation (Regulation (EU) 2016/679). The associated Law Enforcement Directive (Directive (EU) 2016/680) will be implemented by an Ordinance to be made under the Law.

The Law imposes duties primarily on controllers (persons who determine the means and purposes of processing) and processors (persons processing the personal data), in relation to the processing of personal data (information relating to identified or identifiable living individuals). It also confers rights on data subjects (the living individuals to whom the personal data relates), and imposes corresponding duties on controllers. The Law also establishes the Data Protection Authority, confers a wide range of functions on it and authorises it to determine complaints, conduct inquiries and order sanctions (including administrative fines).

PROJET DE LOI

ENTITLED

The Data Protection (Bailiwick of Guernsey) Law, 2017

ARRANGEMENT OF SECTIONS

PART X
TRANSFERS TO UNAUTHORISED JURISDICTIONS

PART XI
THE DATA PROTECTION AUTHORITY

PART XII
ENFORCEMENT BY THE AUTHORITY

PART XIII
CIVIL PROCEEDINGS FOR BREACH OF STATUTORY DUTY

PROJET DE LOI

ENTITLED

The Data Protection (Bailiwick of Guernsey) Law, 2017

THE STATES, in pursuance of their Resolution of the 26th April, 2017[a], have approved the following provisions which, subject to the Sanction of Her Most Excellent Majesty in Council, shall have force of law in the Bailiwick of Guernsey.

PART I

PRELIMINARY

Object of this Law.

1. The object of this Law 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 GDPR and the Law Enforcement Directive, and

(b) make other provisions considered appropriate in relation to the processing of personal data.

---

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

Application.

2. (1) This Law applies in relation to the processing of personal data only where conditions A and B are satisfied.

(2) Condition A is that –

(a) the processing is wholly or partly by automated means, or

(b) if the processing is other than by automated means, the personal data forms or is intended to form part of a filing system.

(3) Condition B is that –

(a) the processing is in the context of a controller or processor established in the Bailiwick, or

(b) the personal data is that of a Bailiwick resident, and it is processed in the context of –

(i) the offering of goods or services (whether or not for payment) to the resident, or

(ii) the monitoring of the resident's behaviour in the Bailiwick.

(4) Schedule 1 has effect.

(5) In this section, "**Bailiwick resident**" means an individual who is ordinarily resident in the Bailiwick.

Extent.

3. Subject to section 2, this Law –

(a) applies regardless of where the processing takes place, and

(b) has extra-territorial application unless the context requires otherwise.

Exception for personal, family or household affairs.

4. Nothing in this Law applies to the processing of personal data by an individual solely for the purpose of the individual's personal, family or household affairs (including recreational purposes).

Other enactments.

5. So far as it is possible to do so, an enactment must be read and given effect in a way which is consistent with this Law.

PART II

DUTIES AND PRINCIPLES OF PROCESSING

Duty to comply with data protection principles.

6. (1) A controller must –

(a) ensure that the processing of all personal data in relation to which the person is the controller complies

with the data protection principles in subsection (2)(a) to (f), and

(b) comply with the principle in subsection (2)(g).

(2) The data protection principles are –

(a) **Lawfulness, Fairness and Transparency:**
Personal data must be processed lawfully, fairly and in a transparent manner in relation to the data subject,

(b) **Purpose Limitation:**
Personal data:

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

(ii) once collected, must not be further processed in a manner incompatible with the purpose for which it was collected,

(c) **Minimisation:**
Personal data processed must be adequate, relevant and limited to what is necessary in relation to the purpose for which it is processed,

(d) **Accuracy:**
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 purpose for which it is processed) is erased or corrected without delay,

(e) **Storage Limitation:**

Personal data must not be kept in a form that permits identification of the data subject any longer than is necessary for the purpose for which it is processed (but may be stored longer to the extent necessary for a historical or scientific purpose),

(f) **Integrity and Confidentiality:**

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, and

(g) **Accountability**:

The controller is responsible for, and must be able to demonstrate, compliance with the data protection principles in paragraphs (a) to (f).

Lawfulness of processing.

7. For the purposes of the data protection principle of Lawfulness, Fairness and Transparency, processing of personal data is lawful only if, and to the extent that –

(a) in the case of special category data, at least one condition in Part II or III of Schedule 2 is satisfied, and

(b) in any other case, at least one condition in Part I or II of Schedule 2 is satisfied.

Fairness of processing.

8. (1) For the purposes of the data protection principle of Lawfulness, Fairness and Transparency –

(a) subject to paragraphs (b) and (c), whether or not personal data is processed fairly must be determined having regard to the method by which it is obtained, including whether any person from whom it is obtained is deceived or misled as to the purpose or purposes for which it is to be processed,

(b) personal data must be regarded as obtained fairly if it consists of information obtained from a person who –

(i) is authorised by or under any enactment to supply it, or

(ii) is required to supply it by or under any enactment or any international agreement imposing an international obligation on the Bailiwick, and

(c) the processing of personal data containing an identifier of a prescribed kind or description must be regarded as unfair unless the processing complies with any conditions prescribed in relation to identifiers of that kind or description.

(2) In subsection (1)(c), "**prescribed**" means prescribed by an Ordinance made under this Law.

Compatibility of further processing.

9. (1) This section applies for the purposes of the data protection principle of Purpose Limitation, in relation to the requirement in section 6(2)(b)(ii) that personal data, once collected, must not be further processed in a manner incompatible with the purpose for which it was collected.

(2) Subject to subsection (3), whether or not personal data is further processed in a manner incompatible with the purpose for which it was collected must be determined having regard to the proportionality factors.

(3) Further processing of personal data is deemed to be compatible with any purpose for which the data was collected, where –

(a) the explicit consent of the data subject is obtained for the further processing,

(b) the further processing is for a historical or scientific purpose, or

(c) the further processing is specifically authorised or required by an enactment.

Consent to processing.

10. (1) For the purposes of this Law, consent given by a data subject means any specific, informed and unambiguous indication of the data subject's wishes by which the data subject, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to the data subject.

(2) A data subject's consent to the processing of personal data is not valid for the purposes of this Law except where the following conditions are satisfied –

(a) it is clearly demonstrable that the data subject has given the consent,

(b) the data subject has freely given the consent,

(c) before the consent is given, the data subject is informed that the data subject has the right to withdraw consent at any time,

(d) if the consent is given in writing in the context of other matters (not involving consent to processing of the personal data), the request for consent is -

(i) presented in a manner which is clearly distinguishable from the other matters,

(ii) in an intelligible and easily accessible form, and

(iii) in clear and plain language,

(e) if the consent is given in the context of the performance of a contract (including by provision of a service) –

(i) the consent was necessary for the performance of the contract, or

(ii) if it was not so necessary, the data subject was given the option of refusing consent without prejudice to the performance of the contract, and advised of this option, and

(f) if consent is given in the context of the offer of information society services directly to a child under 13 years of age, the consent is given or authorised by a person who has parental responsibility for the child.

(3) A person determining whether the conditions in subsection (2)(a) to (e) are satisfied in the context of consent given by a child must have regard to the age of the child.

(4) For the avoidance of doubt, a data subject's consent is not freely given if it is given on the basis of false, deceptive or misleading information or conduct, knowingly or recklessly provided or perpetrated by –

(a) the controller,

(b) the processor,

(c) any other person who seeks the consent or to whom the consent is given.

(5) A data subject may withdraw the data subject's consent to processing at any time, and the consent is treated as revoked from that time.

(6) Where consent to processing is sought or given, the controller must –

(a) provide a procedure for withdrawal that is at least as simple as the procedure for giving consent, and

(b) make reasonable efforts to verify that the person giving or authorising the consent is who that person claims to be, particularly where that person claims to be the person authorised to give or authorise consent for a child under 13 years of age.

(7) Consent to the processing of criminal data is not valid for the purposes of this Law unless –

(a) the controller to whom the data subject has given consent –

(i) is a person authorised or required by any enactment to process the criminal data of any person at the application or request of, or otherwise with the consent of, the data subject, or

(ii) is a person authorised or required by any enactment to apply to or request any person to process that criminal data, or

(b) otherwise provided by an Ordinance made under this Law.

(8) Nothing in this section affects the general law of contract, including rules on validity, formation or effect of a contract in relation to a child.

Anonymisation.

11. (1) Where personal data is anonymised –

(a) nothing in this Law requires the controller to maintain, acquire or process additional information solely in order to comply with this Law, but

(b) the controller must take reasonable steps to notify the data subject of the anonymisation.

(2) Part III of this Law does not apply to anonymised data unless the data subject provides additional information to enable the anonymised data to be identified with that data subject.

(3) In this section, "**anonymised**", in relation to personal data, means the personal data is manipulated or treated in such a manner that the controller is not capable of identifying the data subject.

PART III

DATA SUBJECT RIGHTS

Data subject rights and corresponding duties of controllers

Right to information for personal data collected from data subject.

12. (1) This section applies where personal data is collected from the data subject by –

(a) the controller, or

(b) a processor acting on the controller's behalf.

(2) Where this section applies, the data subject has a right to be given the following information in accordance with subsection (3) –

(a) the information specified in Schedule 3, and

(b) a statement as to –

(i) whether the provision of the personal data by the data subject is a statutory or contractual requirement, or a requirement necessary to be met in order to enter into a contract, and

(ii) whether the data subject is obliged to provide the personal data, and the possible consequences of failure to provide that personal data.

(3) The controller must give the data subject that information before or at the time the personal data is collected from the data subject.

(4) For the avoidance of doubt, the controller may give the data subject that information wholly or partly using standardised icons, but any icon presented electronically must be machine-readable.

Right to information for indirectly collected personal data.

13. (1) Where personal data processed in the context of a controller has not been collected from the data subject by either the controller or a processor acting on the controller's behalf, the data subject has a right to be given the information specified in Schedule 3 in accordance with subsection (2).

(2) The controller must give the data subject that information –

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

(b) in any case, before or at the earliest occurrence of any 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,

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

(iii) the expiry of one month following the processing of the personal data.

(3) For the avoidance of doubt, the controller may give the data subject that information wholly or partly using standardised icons, but any icon presented electronically must be machine-readable.

(4) Nothing in subsection (1) or (2) requires the controller to give the data subject any information where –

(a) the data subject already has the information,

(b) the provision of the information is impossible or would involve a disproportionate effort,

(c) the provision of the information is likely to prejudice the objectives of that processing,

(d) the information or the personal data must be kept confidential or secret in order to perform or comply with any duty imposed by law on the controller, or

(e) the collection of the personal data in the context of the controller, or the disclosure of the personal data to the controller, is required or authorised by the provisions of an enactment other than this Law.

(5) Where subsection (4)(b) applies, the controller must take appropriate measures to protect the significant interests of the data subject, for example by publishing a notice (without making public any personal data) or taking any other equivalent step to inform the data subject in an equally effective manner.

Right to data portability.

14. (1) This section applies where –

(a) a data subject has provided personal data relating to the data subject ("**relevant personal data**") to a controller ("**the first controller**"), directly or through a processor,

(b) the processing of the relevant personal data is based wholly or partly on the data subject's consent to processing or on the processing being necessary –

(i) for the conclusion or performance of a contract –

(A) to which the data subject is a party, or

(B) made between the first controller and a third party in the interest of the data subject, or

(ii) to take steps at the request of the data subject prior to entering into such a contract,

(c) the processing of the relevant personal data is not in the context of a public authority exercising or performing –

(i) a function that is of a public nature, or

(ii) a task carried out in the public interest, and

(d) the processing of the relevant personal data is carried out by automated means.

(2) The data subject has a right –

(a) to be given the relevant personal data in accordance with subsection (3)(a), and

(b) where the relevant personal data is given to the data subject, to transmit that personal data to another controller without hindrance from the first controller.

(3) On request by the data subject, the first controller must –

(a) give the data subject the relevant personal data in a structured, commonly used and machine-readable format, suitable for transmission to another controller, and

(b) transmit that personal data directly to another controller specified by the data subject unless this is not technically feasible.

(4) Nothing in this section affects or limits section 21.

Right of access.

15. (1) An individual has a right to be given the following information in accordance with subsections (2) to (4) –

(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) the information specified in Schedule 3,

(ii) one copy of the personal data, and

(iii) further copies of the personal data.

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

(3) For the avoidance of doubt, the controller must give the individual that information free of any charge, except in the case of the further copies specified in subsection (1)(b)(iii), for which the controller may require the payment of a reasonable charge for administrative costs.

(4) Where an individual makes a request under this section to a controller which is a credit reference agency, the request is to be regarded as limited to a request concerning personal data relevant to the individual's financial standing, unless the request shows a contrary intention.

(5) In subsection (4), "**credit reference agency**" means a person carrying on business comprising the furnishing of persons with information relevant to the financial standing of individuals, being information collected for that purpose.

Exception to right of portability or access involving disclosure of another individual's personal data.

16. (1) This section applies where a controller cannot comply with a request made by an individual ("**the requestor**") under section 14 or 15 without disclosing information relating to another individual ("**the other individual**") who is identified or identifiable from that information.

(2) Despite any provision to the contrary in section 14 or 15, if it is reasonable to do so in order to protect the significant interests of the other individual, the controller must –

(a) in the case of a request to be given that information, refuse to give that information to the requestor, and

(b) in the case of a request for transmission of that information to another controller, refuse to so transmit that information.

(3) In determining whether it reasonable in accordance with subsection (2) to refuse to give that information to the requestor or transmit that information to another controller, the controller must take into account the following matters –

(a) whether the controller has taken any steps to seek the other individual's consent to the disclosure of that information,

(b) whether the other individual has expressly refused consent for the disclosure of that information,

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

(d) the nature of that information, including whether it is special category data,

(e) the requestor and the other individual (including whether either is a child), and any significant interests of each at stake in the disclosure or non-disclosure of that information,

(f) the context in which that information has been collected or otherwise processed, and in particular the relationship between each data subject and the controller,

(g) the reasonable expectations of each data subject in relation to the disclosure of that information, including-

(i) whether the requestor had provided that information to the controller, directly or through a processor, and

(ii) whether the controller owes the other individual a duty of confidentiality,

(h) the persons to which, and the circumstances in which, the disclosure is to be made,

(i) if storage of that information is or may be involved following disclosure, the period for which that information is or may be stored,

(j) the existence of appropriate safeguards for the protection of that information, once disclosed, and

(k) the possible consequences for each data subject of disclosure of that information.

(4) If the controller determines that it is reasonable in accordance with subsection (2) to refuse to give that information to the requestor or transmit that information to another controller, the controller, taking into account the matters specified in subsection (3), may instead provide the requestor or (as the case may be) the other controller only with access to view or review that information.

(5) Subsections (2), (3) and (4) do not apply where –

(a) the other individual has given explicit consent for the disclosure of that information, or

(b) those provisions are disapplied by regulations.

(6) In this section, "**data subject**" means both the requestor and the other individual.

Right to object to processing for direct marketing purposes.

17. (1) This section applies where personal data is processed for direct marketing purposes.

(2) The data subject has a right to require the controller to cease the processing in accordance with subsection (4).

(3) The controller must give the data subject notice of the processing and the data subject right conferred by subsection (2) –

(a) before or at the time of the controller's first communication with the data subject,

(b) explicitly, and

(c) separately from any other matters notified to the data subject.

(4) If the data subject objects to the processing by a written request to the controller to cease the processing, the controller must cease the processing.

(5) Where the processing of that personal data is in the context of information society services, the request under subsection (4) may be made –

(a) by automated means, and

(b) by stating technical specifications, if appropriate.

Right to object to processing on grounds of public interest.

18. (1) This section applies where the lawfulness of the processing of personal data is based exclusively on either or both the conditions in paragraphs 4 and 5 of Schedule 2.

(2) The data subject has a right to require the controller to cease the processing in accordance with subsections (4) to (6).

(3) The controller must give the data subject notice of the processing and the data subject right conferred by subsection (2) –

(a) before or at the time of the controller's first communication with the data subject,

(b) explicitly, and

(c) separately from any other matters notified to the data subject.

(4) The data subject may object to the processing by a written request to the controller to cease the processing, stating any significant interests of the data subject sought to be protected.

(5) Where the processing of that personal data is in the context of information society services, the written request under subsection (4) may be made –

(a) by automated means, and

(b) by stating technical specifications, if appropriate.

(6) On receipt of a request made in accordance with subsection (4), the controller must cease the processing unless the public interest in the objective of that processing outweighs the data subject's significant interests.

Right to object to processing for historical or scientific purposes.

19. (1) This section applies where the lawfulness of the processing of personal data is based solely on the processing being necessary for a historical or scientific purpose.

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

(3) The data subject may object to the processing by a written request to the controller to cease the processing, stating any significant interests of the data subject sought to be protected.

(4) On receipt of a request made in accordance with subsection (3), the controller must cease the processing unless –

(a) the controller is a public authority,

(b) the historical or scientific purpose for which the personal data is processed relates to an objective that is in the public interest, and

(c) the public interest in the objective outweighs the data subject's significant interests.

Right to rectification.

20. (1) This section applies where a data subject disputes the accuracy or completeness of personal data.

(2) The data subject has a right to require the controller to rectify or change the personal data in accordance with subsections (3) to (6).

(3) The data subject may make a written request to the controller to rectify or change the personal data, stating the inaccuracy or explaining why the personal data is incomplete.

(4) On receipt of a request made in accordance with subsection (3), 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 (5) or (6).

(5) 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.

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

(7) Nothing in this section affects or limits section 21.

Right to erasure.

21. (1) This section applies where a data subject disputes the accuracy or completeness of personal data in any of the following circumstances –

(a) the personal data is no longer necessary for the purposes for which it was collected or otherwise processed,

(b) the lawfulness of the processing of the personal data is based solely on the data subject's consent to the processing, and the data subject has withdrawn that consent,

(c) the data subject objects to the processing and the controller is required to cease processing the personal data in accordance with section 17, 18 or 19,

(d) the personal data has been unlawfully processed,

(e) the personal data is required to be erased in order to perform or comply with any duty imposed by law on the controller, or

(f) the personal data was collected in the context of an offer of information society services directly to a child under 13 years of age.

(2) The data subject has a right to require the controller to erase the personal data in accordance with subsections (3) to (6).

(3) The data subject may make a written request to the controller to erase the personal data, stating the inaccuracy or explaining why the personal data is incomplete.

(4) On receipt of a request made in accordance with subsection (3), the controller must erase that personal data.

(5) Where the controller has made the personal data public and is required under subsection (4) to erase that personal data, the controller, taking into account available technology and the cost of implementation, must take reasonable steps, including technical measures, to inform other controllers that are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or duplicate of, that personal data.

(6) Subsection (4) does not apply where the lawfulness of the processing of the personal data for which the erasure is requested is based on any condition in paragraph 3, 5, 6, 8, 9, 10, 11, 12 or 13 of Schedule 2.

Right to restriction of processing.

22. (1) This section applies where –

(a) a data subject disputes the accuracy or completeness of personal data, and the data subject wishes to obtain a restriction of processing for a period enabling the controller to verify the accuracy or completeness of the personal data,

(b) the processing is unlawful but the data subject opposes the erasure of the personal data and wishes to obtain a restriction of processing instead,

(c) the controller no longer needs the personal data for the purposes of the processing, but the data subject requires the personal data –

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

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

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

(d) the data subject has objected to the processing under section 18 or 19, but the controller has not ceased the processing pending determination of whether the public interest in the objective for which the personal data is processed outweighs the data subject's significant interests.

(2) The data subject has a right to obtain a restriction of processing in accordance with subsections (3) and (4).

(3) The data subject may make a written request to the controller for a restriction of processing of the personal data in a manner and for a period of time specified in the request, stating any significant interests of the data subject sought to be protected.

(4) On receipt of a request made in accordance with subsection (3), the controller must carry out the restriction of processing in the manner and for the period of time specified in the request, except to the extent that –

(a) that personal data is stored,

(b) the data subject gives explicit consent to processing of that personal data in any other manner, or

(c) the continued processing of the personal data contrary to the restriction requested by the data subject is necessary –

(i) for a purpose specified in paragraph 3 or 12 of Schedule 2,

(ii) for the protection of the significant interests of a third party, or

(iii) for reasons of public interest that outweigh the significant interests of the data subject.

Right to be notified of rectification, erasure and restrictions.

23. (1) This section applies where any rectification or erasure of personal data or restriction of processing is carried out in accordance with section 20, 21 or 22.

(2) The data subject has a right to the notifications required by subsections (3) and (4).

(3) If the controller has disclosed the personal data to another person –

(a) the controller must notify the other person of the rectification, erasure or restriction of processing, unless such notification is impracticable or involves disproportionate effort, and

(b) the controller must notify the data subject of the identity and contact details of the other person if the data subject requests these.

(4) Before lifting or otherwise ceasing a restriction of processing carried out under section 22, the controller must notify the data subject who requested and obtained the restriction.

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

24. (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 explicit consent to the automated processing,

(b) the automated processing is necessary to protect the vital interests of the data subject or any other individual who is a third party,

(c) the automated processing is necessary –

(i) for the conclusion or performance of a contract –

(A) to which the data subject is a party, or

(B) made between the controller and a third party in the interest of the data subject, or

(ii) to take steps at the request of the data subject prior to entering into such a contract, or

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

(3) Where a controller causes or permits a data subject to be subjected to an automatic decision under subsection (2), the controller must take reasonable steps to –

(a) allow the data subject to –

(i) express the data subject's views on the decision, or

(ii) appeal or seek a review of the decision,

(b) allow the data subject to request and obtain human intervention by or on behalf of the controller in that decision,

(c) ensure that the data subject's views are considered in making or reviewing that decision, and

(d) put in place any other appropriate safeguards for the significant interests of data subjects.

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

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

(b) the automated processing of that special category data is necessary to protect the vital interests of the data subject or any other individual who is a third party, and

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

(ii) the controller cannot reasonably be expected to obtain the explicit consent of the data subject, or

(c) 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.

(5) 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.

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

Further provisions relating to controller's duties and data subject rights

Application and effect of sections 27 to 29.

26. (1) Sections 27 to 29 apply where an individual has made a request to the controller to give the individual any information or to take any action under any of sections 14 to 22 (other than section 16).

(2) Sections 14 to 22 (other than section 16) are subject to sections 27 to 29.

(3) In sections 27 to 29 –

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

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

Compliance with request to exercise data subject right.

27. (1) Subject to the following provisions of this section, sections 28 and 29 and any other exception or exemption provided by sections 14 to 22 or any other provision of this Law, the controller must 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 notify the requestor of –

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

(b) the right to complain to the Authority under section 67, and

(c) a complainant's rights of appeal under sections 82 and 83.

(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 Law in respect of any information or action requested is paid to the controller.

Requirement to verify identity.

28. (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.

29. (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 Law 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 to show that it is.

PART IV

DUTIES OF CONTROLLERS AND PROCESSORS

Duty of controllers to give information or take action

Requirements to give information or take action under this Law.

30. (1) Where any provision of this Law 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 Law 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, or

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

(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.

31. (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 Law, 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 Law,

(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.

(3) A controller's compliance or non-compliance with applicable provisions of an approved code or approved mechanism in respect of the processing may be taken into account in determining whether or not the controller is in breach of subsection (1).

Data protection measures by design and default.

32. (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 Law 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) A controller's compliance or non-compliance with applicable provisions of an approved code or approved mechanism in respect of the processing may be taken into account in determining whether or not the controller is in breach of subsection (1).

(5) Nothing in this section limits the controller's duties under section 31(1).

Joint controllers.

33. (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 Law, in particular their duties under Part III.

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

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

(b) may designate a contact point for data subjects.

(3) Joint controllers must publish, or notify data subjects of, the essence of the matters specified in subsection (2)(a) and (b).

(4) 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 Law.

(5) Subsections (1), (2) and (3) 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.

34. (1) A controller must not cause or permit a processor to process personal data unless conditions A and B are satisfied.

(2) Condition A 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 Law, and

(b) to safeguard data subject rights.

(3) Condition B 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 35 and 36.

(4) A processor's compliance or non-compliance with applicable provisions of an approved code or approved mechanism in respect of the processing may be taken into account in determining whether or not there are sufficient guarantees by the processor of the matters specified in subsection (2).

(5) An agreement for the purposes of satisfying condition B may be based on standard data protection clauses.

Duties of processors in relation to controllers.

35. (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,

(f) take reasonable steps to assist the controller to comply with the controller's duties under Parts VI and VII, and

(g) make available to the controller all information necessary to –

(i) demonstrate compliance with this section and sections 34 and 36, and

(ii) facilitate any lawful audits or inspections, including –

(A) inspections conducted by the controller or an auditor authorised by the controller, and

(B) any data protection audit required by or under this Law.

(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 Law or any other enactment.

(3) Where a controller or processor ("**the authorising person**") gives any person ("**the authorised person**") 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.

(4) For the avoidance of doubt, subsection (3) applies whether or not the authorised person is an employee of the authorising person.

(5) A processor's compliance or non-compliance with applicable provisions of an approved code or approved mechanism in respect of the processing may be taken into account in determining whether or not the processor is in breach of subsection (1)(e) or (f).

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

36. (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) Where a primary processor engages a secondary processor to process personal data –

(a) sections 34 and 35 have effect as if, for the purposes of those provisions –

(i) the primary processor were the controller, and

(ii) the secondary processor were the processor,

and

(b) the secondary processor must carry out the duties of a processor under sections 34 and 35 and any other applicable provision of this Law.

(4) For the avoidance of doubt, where a primary processor engages a secondary processor to process personal data, and the secondary processor fails to carry out the secondary processor's duties as a processor under this Law, the primary processor remains fully liable for any breach of a processor's duties under this Law.

(5) In subsection (3)(b), "**this Law**" includes any legally binding agreement made between the primary processor and the secondary processor for the purposes of section 34(3), as given effect by subsection (3)(a) of this section.

(6) In subsection (4), "**this Law**" includes any legally binding agreement made between the controller and the primary processor for the purposes of section 34(3).

(7) 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.

Duties of controllers and processors to keep records, make returns and cooperate with Authority.

37. (1) A controller or processor must –

(a) maintain any prescribed records for the prescribed periods of time, in the prescribed manner and form,

(b) on request by an authorised officer, produce for inspection or provide any such records,

(c) make any prescribed returns of information to the Authority –

(i) in the prescribed manner and form, and

(ii) at the prescribed intervals and time.

(2) For the avoidance of doubt, the duty of a controller in subsection (1) may be discharged by a controller's representative.

(3) A controller and a processor must –

(a) cooperate with the Authority in the exercise or performance of any of the Authority's functions under this Law, and

(b) without limiting the generality of paragraph (a) –

(i) comply with any information notice given to the controller or processor under paragraph 1 of Schedule 7,

(ii) facilitate and assist or (where required) carry out any data protection audit required by or under this Law, and comply with any

requirement made by an authorised officer in relation to any such audit,

(iii) grant an authorised officer –

(A) entry to any premises which the officer is entitled to enter, and

(B) access to anything which the officer is entitled to access,

under powers granted to authorised officers in Schedule 7, and

(iv) if an enforcement order is made against the controller or processor concerned, comply with section 73(5).

PART V

ADMINISTRATIVE DUTIES

Controllers to designate Bailiwick representatives in certain cases.

38. (1) This section applies where a controller -

(a) is established in the Bailiwick, but

(b) is not a Guernsey, Alderney or Sark person.

(2) A controller to which this section applies must –

(a) designate in writing a Guernsey, Alderney or Sark person as the representative of the controller in the Bailiwick,

(b) notify the Authority of the name and contact details of the representative, and

(c) authorise the representative to receive on behalf of the controller notices and other communications from the Authority and any other competent supervisory authority in respect of any issue relating to the processing of personal data.

(3) Nothing in this section limits or affects the exercise of any rights or powers conferred by this Law against a controller or a processor.

Controllers and processors to be registered.

39. (1) A controller or processor established in the Bailiwick must not cause or permit personal data to be processed unless the controller or (as the case may be) processor is –

(a) registered in accordance with Schedule 4, or

(b) exempt from registration by regulations made by the Committee.

(2) Schedule 4 has effect.

(3) A person who fails to comply with or contravenes subsection (1) is guilty of an offence.

Registered controllers and registered processors to pay prescribed levies.

40. (1) The Committee may by regulations require registered controllers, registered processors, or both, to pay a levy to the Authority in order to pay for the remuneration, salaries, fees, allowances and other emoluments, costs and expenses of –

(a) the establishment of the Authority, and

(b) the Authority's operations, including any capital costs and the exercise or performance of any functions of the Authority.

(2) The regulations must specify –

(a) the amount of the levy or the basis on which the amount of the levy is to be calculated or ascertained,

(b) the periods in respect of which, and the times at which, the levy must be paid, or a means for ascertaining those periods and times, and

(c) the manner and form in which the levy must be paid.

(3) The regulations may –

(a) impose duties on the Authority, registered controllers, or registered processors in connection with the assessment, collection or payment of the levy, including a duty for registered controllers and registered processors to provide information of a specified kind or description to the Authority,

(b) confer powers on the Authority in connection with the assessment, collection or payment of the levy, including a power to waive or reduce the levy in prescribed circumstances,

(c) exempt any person from paying the levy, and

(d) provide for the payment of interest and penalties in the case of late payment or non-payment of the levy.

(4) A person required by regulations made under this section to pay a levy must do so in accordance with the regulations.

(5) The Authority may recover any levy due and payable by any person to the Authority as a civil debt owed by the person to the Authority.

(6) In this section, a reference to any levy includes a reference to any interest or penalty required under the regulations to be paid in the case of late payment or non-payment of the levy.

PART VI

SECURITY OF PERSONAL DATA

Duty to take reasonable steps to ensure security.

41. (1) A controller or processor must take reasonable steps to ensure a level of security appropriate to the personal 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.

(5) A controller's or processor's compliance or non-compliance with any applicable provisions of an approved code or mechanism in force in respect of the processing may be taken into account in determining whether or not the controller or processor is in breach of subsection (1).

Notification and records required in case of personal data breach.

42. (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) Where 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) 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.

43. (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) For the purposes of subsection (3)(a), a controller's compliance or non-compliance with applicable provisions of an approved code or approved mechanism in respect of the processing may be taken into account in determining whether or not the controller has established and carried out appropriate technical and organisational measures to protect personal data.

(5) 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.

(6) Unless a controller has taken steps to notify the data subject in accordance with subsections (1) and (2) or subsection (5), 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 (5).

PART VII

DATA PROTECTION IMPACT ASSESSMENTS AND PRIOR CONSULTATION

Impact assessment required for high-risk processing.

44. (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 systematic description of the proposed processing operations (including the means of processing), the purposes of the processing and the objectives pursued by the controller in carrying out or determining the purposes or means of the processing,

(b) an assessment of the necessity (including proportionality) of the processing in relation to those objectives,

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

(d) an assessment of compliance or non-compliance with applicable provisions of an approved code or approved mechanism in respect of the processing, and

(e) 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 Law, 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) In carrying out a data protection impact assessment, the controller must consult –

(a) the data protection officer (if any), and

(b) where appropriate and practicable, the data subjects or their representatives, unless this prejudices the objectives or the security of the processing operations.

(5) The controller must review, and where appropriate, revise the data protection impact assessment where –

(a) there is a change in the risks posed to the significant interests of data subjects by the processing operations, or

(b) the controller otherwise considers it necessary.

(6) A review under subsection (5) must include a review of –

(a) whether the processing operations being carried out accord with those described in the data protection impact assessment, and

(b) whether the measures established and carried out to address the risks of processing accord with those envisaged in the data protection impact assessment.

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

(a) any processing specifically required or authorised by high-risk legislation within the meaning of section 46, 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.

(8) In this section and sections 45 and 46, "**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.

45. (1) This section applies where a data protection impact assessment indicates that any processing is likely to be high-risk processing in the absence of measures taken by the controller to mitigate the risks to the significant interests of data subjects.

(2) Before commencing the processing, the controller must consult the Authority by giving it a 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,

(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 this Law 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 eight weeks of the designated date.

(6) The Authority may extend the time allowed for the notice in subsection (5)(b) by a further six weeks 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 eight weeks of the designated date.

(7) In this section, "**designated date**" means the latter 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 eight-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.

46. (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 this Law) that requires or authorises the processing of personal data 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 VIII

DATA PROTECTION OFFICERS

Mandatory designation of a data protection officer.

47. (1) This section applies where –

(a) processing is carried out in the context of a public authority, or

(b) processing operations are carried out as part of a core activity of a controller or processor and, by virtue of their nature, scope or purpose, those operations require or involve –

(i) large-scale and systematic monitoring of data subjects, or

(ii) large-scale processing of special category data.

(2) Where this section applies, the controller and the processor must jointly designate an individual as a data protection officer in accordance with section 49.

(3) A group of undertakings may designate a single data protection officer for the group if –

(a) in the case of a group of public authorities (other than the States), it is appropriate to do so, having regard to their organisational structure and size, and

(b) in any case –

(i) the data protection officer is easily accessible from each undertaking forming part of 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 Law in relation to each undertaking in the group.

Voluntary or prescribed designation of data protection officers.

48. Where a data protection officer is not required to be designated under section 47 –

(a) a controller, a processor, or any association or other body representing controllers or processors of any kind or description may designate an individual as a data protection officer for the controller, the processor or the body concerned in accordance with section 49, and

(b) the States of Deliberation may by Ordinance require a controller, a processor, or any association or other body representing controllers or processors of any kind or description to designate an individual as a data protection officer for the controller, the processor or the body concerned in accordance with section 49.

Requirements for designation.

49. (1) A designating entity may designate an individual as a data protection officer whether or not the individual is a staff member of the designating entity.

(2) An individual must not be designated as a data protection officer 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 Law, and

(b) the individual satisfies any prescribed requirements.

(3) In this section and sections 50 and 51, "**designating entity**", in relation to a data protection officer –

(a) means the controller, processor, group of undertakings, or other body that designates or wishes to designate a data protection officer, and

(b) in the case of a group of undertakings, includes each undertaking within the group.

Functions of data protection officers.

50. (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 Law and any other enactments relating to data protection,

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

(i) this Law,

(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 this Law,

(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 45 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 this Law.

(2) In performing any function under this Law, 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 47(2) or 48(b), the controller and the processor 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.

51. (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 Law 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 Law, 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.

PART IX

CODES OF CONDUCT AND CERTIFICATION MECHANISMS

Authority may approve code of conduct.

52. (1) The Authority may, by publishing the code, approve a code of conduct prepared by any person representing a category of controllers or processors for the purposes of –

(a) encouraging or facilitating compliance with this Law, or

(b) allowing controllers or processors that are not otherwise subject to this Law to demonstrate that they have appropriate safeguards for the protection of personal data, for the purposes of personal data transfers authorised by section 59(1)(j).

(2) A code may include provisions relating to any or all of the following –

(a) fair and transparent processing,

(b) legitimate interests pursued by controllers in specific contexts,

(c) the collection of personal data,

(d) the pseudonymisation of personal data,

(e) the information to be provided to the public and to data subjects,

(f) the exercise of data subject rights,

(g) the protection of children, including the information to be provided to them and the manner in which the consent of the person who has parental responsibility for them is to be obtained,

(h) any steps or measures required to be established, taken or carried out by controllers or processors under this Law,

(i) the notification of personal data breaches to competent supervisory authorities and the communication of such personal data breaches to data subjects,

(j) the transfer of personal data to a person outside the Bailiwick or in an unauthorised jurisdiction, or to international organisations,

(k) out-of-court proceedings and other dispute resolution procedures for resolving disputes between controllers and data subjects with regard to processing, without prejudice to the rights of data subjects under this Law, or

(l) any other matter relating to compliance with this Law or safeguards for the protection of personal data.

(3) The Authority must not approve a code unless –

(a) the code provides for a body accredited by the Authority (or a competent supervisory authority) to monitor compliance with the code by controllers and processors who purport to apply the code,

(b) the code requires any controller or processor that purports to apply the code but is not subject to this Law to enter into legally binding and enforceable commitments to apply provisions of the code,

(c) where the code relates to processing operations carried out in a Member State of the European Union, the European Commission has stated that the code has general validity within the European Union, and

(d) the Authority is of the opinion that –

(i) the contents of the code are compatible with the GDPR, and

(ii) the code provides appropriate safeguards for the protection of personal data.

(4) Subsection (3)(a) does not apply to any code relating to processing operations carried out by public authorities.

(5) In determining whether or not to approve a code, the Authority must take into account –

(a) the particular circumstances of the processing sectors to which the code relates, and

(b) the needs of any micro, small or medium-sized undertakings that are controllers or processors to which the code applies.

(6) The Authority must keep a register of codes approved under this section.

(7) In this section and section 53, "**code**" or "**code of conduct**", includes an amendment to or extension of a code of conduct.

Accreditation and duties of monitoring body.

53. (1) For the purposes of section 52(3)(a), the Authority may accredit a body to monitor compliance with a code only if the Authority is of the opinion that the body has –

(a) adequate expertise and independence in relation to the subject-matter of the code,

(b) established procedures which allow that body –

(i) to assess the eligibility of controllers and processors concerned to apply the code,

(ii) to monitor their compliance with the provisions of the code, and

(iii) to periodically review their application of the code,

(c) established procedures and structures –

(i) to handle complaints about infringements of the code or the manner in which the code has been, or is being, applied by a controller or processor, and

(ii) to publish those procedures and structures or otherwise make them available to data subjects, and

(d) no conflict of interest, for example in connection with the body's discharge or performance of its other tasks and duties.

(2) In cases of infringement of the code by any controller or processor that purports to apply the code, the accredited monitoring body must –

(a) take appropriate action including suspension or exclusion from the code where appropriate, and

(b) notify the Authority of any action taken by the body and the reasons for the action.

(3) The Authority may suspend or revoke an accreditation if –

(a) the conditions for accreditation are not, or no longer, satisfied, or

(b) the accredited body breaches subsection (2).

(4) The Authority may publish further criteria to be applied by it in determining whether or not to accredit a body for the purposes of subsection (1).

Regulations may provide for certification mechanisms.

54. (1) The Committee may make regulations to provide for the establishment, approval, use and application of mechanisms, seals and marks to certify –

(a) that particular processing operations carried out by controllers or processors comply with this Law, or

(b) the existence of appropriate safeguards for the protection of personal data provided by controllers or processors that are not otherwise subject to this Law, for the purposes of personal data transfers authorised by section 59(1)(j).

(2) Regulations under subsection (1) –

(a) must not require any certification mechanism, seal or mark to be used or applied on a mandatory basis,

(b) may confer powers or impose duties on the Authority, and

(c) may provide for the withdrawal or suspension of any certificate, seal or mark.

(3) In this section, "**use**", in relation to a certification mechanism includes following the mechanism.

PART X

TRANSFERS TO UNAUTHORISED JURISDICTIONS

Prohibition of transfers to unauthorised jurisdictions.

55. (1) Except as otherwise authorised by section 56, 57 or 59, a controller or processor must not transfer personal data to a person in an unauthorised jurisdiction–

(a) for processing, or

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

(2) In sections 56 and 57, "**further controller or processor**", in relation to any transfer of personal data –

(a) means the controller or processor of the personal data following its transfer, and

(b) includes the recipient of the personal data.

Transfers on the basis of available safeguards.

56. (1) A controller or processor may transfer personal data to a person in an unauthorised jurisdiction where the controller or processor is satisfied that –

(a) one or more of the safeguards specified in subsection (2) are in place in relation to the personal data, and

(b) there is a mechanism for data subjects to enforce their data subject rights and obtain effective legal remedies against the further controller or processor.

(2) Subsection (1)(a) refers to the following safeguards –

(a) where both the transferor of the personal data and the further controller or processor are public authorities, a legally binding and enforceable agreement between the transferor and the further controller or processor,

(b) binding corporate rules approved –

(i) by the Authority under section 58, or

(ii) by another competent supervisory authority under any provision of law equivalent or similar to Article 47 of the GDPR,

(c) standard data protection clauses,

(d) an approved code combined with binding and enforceable commitments of the further controller or processor to apply any relevant safeguards in the code, including as regards data subject rights, or

(e) an approved mechanism combined with binding and enforceable commitments of the further controller or

processor to apply the relevant safeguards in the mechanism, including as regards data subject rights.

Transfers on the basis of specific authorisation by Authority.

57. (1) A controller or processor may transfer personal data to a person in an unauthorised jurisdiction if the Authority has specifically authorised the transfer.

(2) The Authority may authorise a transfer for the purposes of subsection (1) only where it is satisfied that –

(a) one or more of the safeguards specified in subsection (3) or section 56(2) are in place in relation to the personal data, and

(b) there is a mechanism for data subjects to enforce their data subject rights and obtain effective legal remedies against the further controller or processor.

(3) Subsection (2)(a) refers to the following safeguards –

(a) contractual clauses between the transferor of the personal data and the further controller or processor, or

(b) where both the transferor and the further controller or processor are public authorities, provisions in administrative arrangements between those public authorities which include enforceable and effective data subject rights.

(4) In determining whether to authorise a transfer under this section, the Authority must take into account any opinions or decisions of the European Data Protection Board (established under Article 68 of the GDPR) issued or adopted under Article 64, 65 or 66 of the GDPR.

Approval of binding corporate rules.

58. For the purposes of section 56(2)(b)(i), the Authority must approve binding corporate rules for a group of undertakings, or a group of enterprises engaged jointly in a business, if those rules –

(a) are legally binding on, apply to and are to be enforced and implemented by, every member of the group concerned, including their employees,

(b) expressly confer enforceable rights on data subjects with regard to the processing of their personal data, and

(c) specify the matters required to be specified by Schedule 5 in a manner that provides appropriate safeguards for the protection of personal data and protection of the significant interests of data subjects.

Other authorised transfers.

59. (1) A controller or processor may transfer personal data to a person in an unauthorised jurisdiction where –

(a) required to do so by an order or a judgment of a court or tribunal having the force of law in the Bailiwick,

(b) required to do so by a decision of a public authority of the Bailiwick based on an international agreement imposing an international obligation on the Bailiwick,

(c) required to do so by –

(i) an order or a judgment of a court or tribunal of a country other than the Bailiwick, or

(ii) a decision of a public authority of any country other than the Bailiwick,

having the force of law in the Bailiwick, and based on an international agreement imposing an international obligation on the Bailiwick,

(d) the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision in respect of the unauthorised jurisdiction,

(e) the transfer is necessary –

(i) for the conclusion or performance of a contract –

(A) to which the data subject is a party, or

(B) made between the controller and a third party in the interest of the data subject, or

(ii) to take steps at the request of the data subject prior to entering into such a contract,

(f) the transfer is necessary –

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

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

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

(g) the transfer is necessary to protect the vital interests of the data subject or of another individual, and-

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

(ii) the controller cannot reasonably be expected to obtain the explicit consent of the data subject,

(h) the personal data transferred is personal data in a public register,

(i) the transfer is made from a register to which any member of the public has access who satisfies conditions specified by law for such access, where the transfer is made to or at the request of a person who satisfies those conditions,

(j) the transfer in question satisfies the following conditions–

(i) the transfer is not repetitive,

(ii) the transfer concerns only a limited number of data subjects,

(iii) the transfer is necessary for the purposes of compelling legitimate interests pursued by the controller that outweighs the significant interests of the data subject, and

(iv) the controller has assessed all the circumstances surrounding the data transfer and has on the basis of that assessment provided appropriate safeguards for the protection of personal data, or

(k) authorised to do so by regulations made for reasons of public interest.

(2) Nothing in subsection (1)(d) or (e) authorises the transfer of personal data by a public authority acting in the exercise or performance of a function that is of a public nature.

(3) Nothing in subsection (1)(h) authorises the transfer of the entire personal data or an entire category of personal data contained in the register.

(4) Where a transfer is authorised under subsection (1)(j), the controller –

(a) must notify the Authority of the transfer as soon as practicable, and

(b) must inform the data subject of the transfer and the compelling legitimate interests pursued (in addition to any other matters required to be notified to the data subject under this Law).

PART XI

THE DATA PROTECTION AUTHORITY

Establishment and constitution of the Authority.

60. (1) This subsection establishes a body to be called the Data Protection Authority.

(2) The Authority –

(a) is a body corporate with perpetual succession and a common seal, and

(b) is capable of suing and being sued in its own name.

(3) Schedule 6 has effect.

General functions of the Authority.

61. (1) The Authority has the following functions –

(a) to administer and enforce this Law,

(b) to monitor and report to the States of Deliberation on –

(i) whether the object of this Law is being attained, and

(ii) whether any amendment is required to be made to this Law or any other action is required to be taken, in order to attain the object of this Law,

(c) to promote public awareness of risks, rules, safeguards and rights in relation to processing, especially in relation to children,

(d) to promote the awareness of controllers and processors of their duties under this Law,

(e) on request, to provide reports and other information to the Committee or the States on any matter connected with the protection of personal data,

(f) on request, to provide information to any data subject concerning the exercise of their rights under this Law and, if appropriate, cooperate with competent supervisory authorities to this end,

(g) to cooperate with, including share information and provide mutual assistance to, other competent supervisory authorities with a view to ensuring that this Law is applied and enforced in a manner equivalent to the GDPR and the Law Enforcement Directive,

(h) to monitor relevant developments, insofar as they have an impact on the protection of personal data, in particular the development of information and communication technologies and commercial practices,

(i) to encourage the drawing up of codes of conduct,

(j) to keep confidential records of alleged breaches of this Law and of the exercise of any of its powers under Part XII, and

(k) any other function conferred or imposed on it by this Law or any other enactment.

(2) The Authority may impose a fee or charge for the performance of its functions in response to a request made by any person, where the fee or charge is authorised by –

(a) regulations made by the Committee, or

(b) any other provision of this Law.

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

(a) the fee or charge payable, or

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

(4) If a request made to the Authority to perform a task associated with any function of the Authority is manifestly unfounded, the Authority may refuse to perform the task.

(5) If a request made to the Authority to perform a task associated with any function of the Authority is frivolous, vexatious, unnecessarily repetitive or otherwise excessive, the Authority may –

(a) refuse to perform the task, or

(b) in exceptional circumstances, perform the task but charge the requestor a reasonable fee for the administrative costs of so doing.

(6) For the avoidance of doubt, if any question is raised in any proceedings under this Law as to whether or not a request is manifestly unfounded or frivolous, vexatious, unnecessarily repetitive or otherwise excessive within the meaning of subsection (4) or (5), the Authority bears the burden of proof to show that it is.

(7) Subject to subsection (5)(b), nothing in this section authorises the Authority to impose a fee or charge on any data subject or data protection officer for the performance of any of the Authority's functions in relation to the data subject or data protection officer.

Authority to be independent.

62. In exercising or performing its functions, the Authority must –

(a) act independently and in a manner free from direct or indirect external influence, and

(b) neither seek nor take instructions from any person.

Power to issue opinions and guidance.

63. (1) On its own initiative or on request by any person, the Authority may publish –

(a) opinions or guidance on any issue related to the protection of personal data, including compliance with any provision of this Law, and

(b) guidance about how the Authority proposes to exercise or perform any of its functions under this Law.

(2) An opinion or guidance published under subsection (1) is not legally binding, but may be taken into account in any proceedings under this Law.

Power to issue public statements.

64. (1) This section applies to any of the following matters –

(a) a notification of a personal data breach made to the Authority,

(b) a complaint, investigation or inquiry,

(c) a determination made under section 71(1),

(d) a recommendation or determination made under section 72(1), or

(e) any sanction imposed under section 73, including any order made under that section.

(2) Where the Authority considers that because of the gravity of the matter or other exceptional circumstances, it would be in the public interest to do

so, the Authority may issue a public statement about any aspect of a matter to which this section applies.

(3) Without limiting the generality of subsection (2), a public statement may include all or any of the following –

(a) details of any personal data breach,

(b) information describing or identifying any data subject whose personal data is or has been the subject of a personal data breach,

(c) information about the nature or progress of any complaint, investigation or inquiry, or

(d) information about the outcome of any complaint, investigation or inquiry.

(4) Before issuing a public statement, the Authority must so far as practicable –

(a) consult any data subject whose personal data is to be included in the statement or who is otherwise likely to be identified or identifiable from the statement, and

(b) give written notice of the contents of the statement to any controller and any processor that is likely to be identified or identifiable from the statement.

Authority to take steps to develop and facilitate international cooperation.

65. The Authority must so far as practicable take steps to –

(a) develop international cooperation mechanisms to facilitate the effective enforcement of legislation for the protection of personal data, including making agreements with the European Commission or any competent supervisory authority if appropriate,

(b) provide international mutual assistance in the enforcement of legislation for the protection of personal data, including through notification, complaint referral, investigative assistance and information exchange, subject to appropriate safeguards for the protection of personal data and the significant interests of data subjects,

(c) engage relevant stakeholders in discussion and activities aimed at furthering international cooperation in the enforcement of legislation for the protection of personal data, and

(d) promote the exchange and documentation of personal data protection legislation and practice, including on jurisdictional conflicts.

Further provisions relating to international cooperation and mutual assistance.

66. (1) For the purposes of this Law, the Authority is to be regarded as –

(a) the designated authority in the Bailiwick for the purposes of Article 13 of the Convention, and

(b) the competent supervisory authority of the Bailiwick under the GDPR and the Law Enforcement Directive.

(2) The Committee may by regulations make provision as to the functions to be exercised or performed by the Authority as if it were the designated authority and the competent supervisory authority mentioned in subsection (1).

(3) The Committee may by regulations make provision as to cooperation by the Authority with the European Commission or any competent supervisory authority in connection with the performance of their respective duties including –

(a) the exchange of information with the European Commission or any competent supervisory authority, and

(b) the exercise or performance within the Bailiwick at the request of a competent supervisory authority of functions conferred on the Authority by those regulations.

(4) The Committee may make regulations to give effect to –

(a) any agreement made under section 65 between the Authority and the European Commission or any competent supervisory authority, or

(b) any international obligations of the Bailiwick.

(5) Regulations made under this section may do all or any of the following –

(a) regulate or restrict the functions conferred on the Authority by section 65,

(b) confer additional powers and functions on the Authority, and

(c) create and impose duties on controllers, processors and recipients of personal data.

PART XII

ENFORCEMENT BY THE AUTHORITY

Right to make a complaint.

67. An individual may make a complaint in writing to the Authority in a form approved by the Authority if the individual considers that –

(a) a controller or processor has breached or is likely to breach an operative provision, and

(b) the breach involves or affects or is likely to involve or affect –

(i) any personal data relating to the individual, or

(ii) any data subject right of the individual.

Investigation of complaints.

68. (1) Upon receiving a complaint, the Authority must –

(a) promptly give the complainant a written acknowledgment of receipt of the complaint, and

(b) as soon as practicable and in any event within two months of receiving the complaint, determine whether or not to investigate it.

(2) The Authority must investigate the complaint unless –

(a) the complaint is manifestly unfounded,

(b) the complaint is frivolous, vexatious, unnecessarily repetitive or otherwise excessive, or

(c) the Authority determines that it is inappropriate to investigate the complaint, having regard to any other action that may be or is taken by the Authority under –

(i) section 65, or

(ii) any regulations made under section 66.

(3) Where a complaint is investigated, the Authority must give the complainant and the controller or processor concerned –

(a) as soon as practicable, and in any event within two months of receiving the complaint, written notice that the complaint is being investigated, and

(b) at least once within three months of giving the notice under paragraph (a), written notice of the progress and, where applicable, the outcome of the investigation.

(4) If the Authority determines not to investigate a complaint, the Authority must give the complainant written notice of its determination and the reasons for it within two months of receiving the complaint.

(5) A notice under subsection (4) must include information as to the complainant's right of appeal under section 82.

(6) Despite subsections (3) and (4), where the Authority is of the opinion that giving a notice required by either of those subsections within the time specified for the notice to be given is likely to seriously prejudice an investigation, the Authority may delay giving the notice.

(7) If the Authority delays giving a notice under subsection (6), the Authority must give the notice, including an update as to the progress and,

where applicable, the outcome of the investigation, as soon as it becomes possible to do so without seriously prejudicing the investigation.

Inquiries.

69. (1) The Authority may conduct an inquiry on its own initiative into the application of this Law, including into whether a controller or processor has breached or is likely to breach an operative provision.

(2) An inquiry may be conducted –

(a) on the basis of a request made or information provided by any person, or

(b) on any other basis.

(3) An inquiry may be conducted together with, or in addition to and separately from, an investigation under section 68.

(4) Where the Authority decides to conduct an inquiry into whether a controller or processor has breached or is likely to breach an operative provision, the Authority must give the controller or processor concerned –

(a) as soon as practicable, and in any event within two months of commencing the inquiry, written notice of the nature of the inquiry, and

(b) at least once within three months of giving the notice under paragraph (a), written notice of the progress and, if possible, the outcome of the inquiry.

(5) Despite subsection (4), where the Authority is of the opinion that giving a notice required by that subsection within the time specified for the notice to be given is likely to seriously prejudice the inquiry, the Authority may delay giving the notice.

(6) If the Authority delays giving a notice under subsection (5), the Authority must give the notice, including an update as to the progress and, where applicable, the outcome of the inquiry, as soon as it becomes possible to do so without seriously prejudicing the inquiry.

(7) Nothing in this section limits –

(a) an individual's right to make a complaint under section 67, or

(b) the duties of the Authority under section 68.

Powers of the Authority.

70. Schedule 7 has effect.

Determinations on completion of investigation.

71. (1) On completing an investigation, the Authority must determine–

(a) whether or not the controller or processor concerned has breached or is likely to breach an operative provision, and

(b) if the Authority makes a breach determination against the controller or processor, which sanction to impose against that controller or processor.

(2) As soon as practicable after making a determination under subsection (1), the Authority must give the controller or processor concerned and the complainant written notice of –

(a) the determination and the reasons for it, and

(b) their respective rights of appeal under sections 83 and 84.

Recommendations and determinations on completion of inquiry.

72. (1) On completing an inquiry, the Authority may do either or both of the following –

(a) make a recommendation to the Committee, the States of Deliberation or any of the States, for any action to be taken to ensure that the object of this Law is attained, or

(b) make a determination –

(i) that a controller or processor has breached or is likely to breach an operative provision, and

(ii) if the Authority makes a breach determination against the controller or processor, as to which

sanction to impose against that controller or processor.

(2) As soon as practicable after making a determination under subsection (1)(b), the Authority must give the controller or processor concerned written notice of –

(a) the determination and the reasons for it, and

(b) the right of appeal under section 84.

Sanctions following breach determination.

73. (1) If the Authority makes a breach determination, the Authority may by written notice to the person concerned impose all or any of the following sanctions against that person –

(a) a reprimand,

(b) a warning that any proposed processing or other act or omission is likely to breach an operative provision, and

(c) an order under subsection (2).

(2) For the purposes of subsection (1)(c), the Authority may make an order against the person concerned requiring that person to do all or any of the following –

(a) bring specified processing operations into compliance with a specified operative provision, or take any other

specified action required to comply with any operative provision,

(b) notify a data subject of any personal data breach,

(c) comply with a request made by a data subject to exercise a data subject right,

(d) rectify or erase any personal data in accordance with any provision of this Law,

(e) restrict or limit any processing operation, which may include –

(i) restricting the processing operation in accordance with any provision of this Law,

(ii) ceasing the processing operation, or

(iii) suspending any transfer of personal data to a person in an unauthorised jurisdiction,

(f) notify any other person to whom personal data has been disclosed of a rectification, erasure or temporary restriction on processing, in accordance with any provision of this Law, and

(g) in any case where the person concerned has breached an operative provision, pay a civil penalty by way of an

administrative fine ordered by the Authority in accordance with section 74.

(3) Nothing in subsection (2)(d), (e) or (f) limits subsection (2)(c).

(4) An order under subsection (2)(a) to (f) may, in relation to each requirement in the order, specify –

(a) the time at which, or by which, the requirement must be complied with, and

(b) the period during which the requirement must be complied with (including the occurrence of any action or event upon which compliance with the requirement may cease).

(5) The person concerned must comply with an order under subsection (2) within the time specified in it for compliance.

(6) A person who fails to comply with an order under subsection (2) within the time specified in it for compliance is guilty of an offence.

(7) Subsection (6) does not apply in respect of a failure to comply with an order to pay a civil penalty by way of an administrative fine under subsection (2)(g).

(8) The Authority may revoke or amend an order under subsection (2) by giving written notice to the person concerned.

Specific provisions concerning administrative fines.

74. (1) For the purposes of section 73(2)(g), the Authority may order the person concerned to pay to the States of Guernsey (whether directly or through the Authority) an administrative fine for any of the following matters –

(a) failure to make reasonable efforts to verify that a person giving consent to the processing of the personal data of a child under 13 years of age in the context of the offer of information society services directly to the child is a person duly authorised to give consent to that processing under section 10(2)(f),

(b) failure to take reasonable steps to inform the data subject of anonymisation, in breach of section 11(1)(b),

(c) breach of any duty imposed on the person concerned by any provision of Part IV (except section 31), V, VI, VII (except section 46) or VIII,

(d) where the person concerned is an accredited monitoring body, breach of the duty imposed on the body by section 53(2),

(e) breach of any duty imposed on the person concerned by section 6(1), including (for the avoidance of doubt) a breach of the data protection principle relating to lawfulness of processing,

(f) breach of any duty imposed on the person concerned under Part III,

(g) transfer of personal data to a person in an unauthorised jurisdiction in breach of section 55, or

(h) breach of any provision of any Ordinance or regulations made under any Part of this Law imposing a duty on a controller or processor in respect of the processing of personal data.

(2) In determining whether or not to order an administrative fine and, if ordered, the amount of the administrative fine, the Authority must have regard to –

(a) the nature, gravity and duration of the breach of the operative provision 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,

(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) compliance or non-compliance with applicable provisions of an approved code or approved mechanism in respect of the processing concerned, and

(j) any other aggravating or mitigating factor applicable to the circumstances of the case, such as financial benefits gained, or losses avoided, directly or indirectly, from the breach.

(3) In ordering any administrative fine, the Authority must take into account the need for administrative fines to be effective and proportionate and have a deterrent effect.

(4) An order imposing an administrative fine –

(a) must specify –

(i) the date by which the fine must be paid, and

(ii) the reasons for the amount of the fine, including any aggravating or mitigating factors that the Authority has taken into account, and

(b) may provide for the fine to be paid by instalments –

(i) of any specified number and amounts, and

(ii) at any specified times and intervals.

(5) An administrative fine imposed on an unincorporated body by order of the Authority must be paid from the funds of the body.

(6) The Authority may publish the amount of an administrative fine ordered by the Authority and the name of the person concerned.

(7) The Authority may recover an administrative fine as a civil debt owed and due to the Authority by the person concerned.

(8) Any administrative fine paid to or recovered by the Authority must be paid to the general revenue account of the States of Guernsey as soon as practicable.

(9) Nothing in this section authorises the Authority to order any of the following persons to pay an administrative fine –

(a) the States,

(b) a public committee,

(c) a holder of a public office,

(d) a court or tribunal,

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

(f) 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, or

(g) a parish Douzaine of the Island of Guernsey or the Douzaine of the Island of Sark.

Limits on administrative fines.

75. (1) An administrative fine issued against a person for any matter specified in section 74(1)(a) to (d) must not exceed –

(a) £5,000,000, or

(b) any higher or lower limit prescribed by Ordinance made by the States of Deliberation in place of the limit in paragraph (a).

(2) An administrative fine issued against a person for any other matter specified in section 74(1) must not exceed –

(a) £10,000,000, or

(b) any higher or lower limit prescribed by Ordinance made by the States of Deliberation in place of the limit in paragraph (a).

(3) An administrative fine issued against a person must not exceed £300,000, unless the amount of the fine is less than 10% of the total global

annual turnover or total global gross income in the preceding financial year of that person.

(4) An administrative fine issued against a person must not exceed 10% of the total global annual turnover or total global gross income of that person during the period of the breach in question, up to a maximum period of 3 years.

(5) Where a person breaches several operative provisions in relation to the same processing operations, or associated or otherwise linked processing operations, the total aggregate of the administrative fines issued against the controller or processor in respect of those processing operations must not exceed the limit specified for the gravest breach under subsection (1) or (as the case may be) subsection (2).

(6) The Committee may by regulations prescribe the manner in which the total global annual turnover or total global gross income of a person is to be calculated for the purposes of subsection (3) or (4).

Procedure to be followed before making breach determination or order.

76. (1) This section applies where the Authority, otherwise than with the agreement of the person concerned, proposes to make –

(a) a breach determination, or

(b) an enforcement order.

(2) Before making the determination or order, the Authority must give the person concerned notice in writing stating –

(a) that the Authority is proposing to make the determination or order,

(b) the terms of, and the reasons for, the proposed determination or order,

(c) that the person concerned may, within a period of 28 days beginning on the date of the notice or any longer period that may be specified in the notice, make written or oral representations to the Authority in respect of the proposed determination or order in a manner specified in the notice, and

(d) the right of appeal of the person concerned under section 84 if the Authority were to make the proposed determination or order.

(3) The Authority must consider any representations made in response to a notice under subsection (2) before giving further consideration to the proposed determination or order.

(4) The Authority may reduce the period of 28 days mentioned in subsection (2)(c) where the Authority considers it necessary to do so–

(a) in the interests of data subjects, any class or description of data subjects, or the public, or

(b) where there are reasonable grounds for suspecting –

(i) that, if that period of notice were given, information relevant to or relating to the proposed determination or order would be concealed, falsified, tampered with or destroyed, or

(ii) that the giving of that period of notice is likely to seriously prejudice -

(A) any criminal, regulatory or disciplinary investigation, or any prosecution, in the Bailiwick or elsewhere,

(B) co-operation or relations with investigatory, prosecuting, regulatory or disciplinary authorities, in the Bailiwick or elsewhere, or

(C) the performance by the Authority of its functions.

(5) The Authority may dispense with the requirements of subsections (2) and (3) altogether if it is of the opinion that the determination or order needs to be made immediately or without notice because of the interests or grounds mentioned in subsection (4).

(6) For the avoidance of doubt, a notice of a proposed administrative fine must state the amount of the proposed fine.

Exclusion of courts and tribunals acting in a judicial capacity.

77. Nothing in this Law authorises the Authority –

(a) to investigate, inquire into or determine any matter, or

(b) exercise any of its other powers,

in relation to processing operations carried out by, or any other act or omission of, a court or tribunal acting in its judicial capacity.

PART XIII

CIVIL PROCEEDINGS FOR BREACH OF STATUTORY DUTY

Interpretation of this Part.

78. In this Part, unless the context requires otherwise –

"**action**" means an action under section 79(2),

"**breach of duty**" means a breach of the duty created by section 79(1), and

"**controller or processor**" excludes any controller or processor that is a public authority of any country other than the Bailiwick.

Civil action against a controller or processor for breach of duty.

79. (1) A controller or processor has a duty not to breach an operative provision.

(2) Where a controller or processor breaches the duty in subsection (1), and the breach causes damage to another person ("**the injured party**"), the breach is actionable in court by the injured party against the controller or processor in the same manner and by the same remedies and other means as if the controller or processor had committed the tort of breach of statutory duty against the injured party.

(3) A court in which an action is brought may grant any order, relief and remedy that the court may grant in the case of the tort of breach of statutory duty, including, for the avoidance of doubt, in the Royal Court –

(a) an award of damages (including punitive or exemplary damages) in respect of the breach of duty,

(b) an injunction or interim injunction to restrain any actual or anticipated breach of duty, and

(c) a declaration that the controller or processor has committed a breach of duty, or that a particular act, omission or course of conduct on the part of the controller or processor would result in a breach of duty.

(4) Despite any rule of law to the contrary, a court in which an action is brought may grant an order, relief or remedy of a kind mentioned in subsection (3) in respect of any distress, inconvenience or other adverse effect suffered by an injured party even if it does not result from any physical or financial loss or damage.

(5) This section replaces any action for the tort of breach of statutory duty that may lie against a controller or processor in relation to the breach or anticipated breach of an operative provision.

(6) Except as otherwise provided by subsection (5), nothing in this section affects or limits any other administrative, civil or other action, right, remedy or relief that any person has or may have against a controller or processor.

Further provisions on liability.

80. (1) A defendant in any action is exempt from liability for breach of duty if the defendant proves that the defendant is not in any way responsible for the damage that is the subject of the action.

(2) A processor is exempt from liability for damages under any action unless the processor –

(a) has breached a provision of this Law specifically imposing a duty on processors, or

(b) has acted outside or contrary to lawful instructions given by the controller.

(3) For the avoidance of doubt –

(a) where both a controller and a processor, or more than one controller or one processor, are involved in the same processing that caused the damage that is the subject of the action, each controller and each processor

so involved is jointly and severally liable for the damage concerned, and

(b) where a controller or a processor ("**A**") has, in accordance with paragraph (a), paid full compensation for any damage, A is entitled to reimbursement from each of the other controllers and processors ("**B**") involved in that processing, for that part of the compensation corresponding to the responsibility of B for the damage concerned, subject to subsections (1) and (2).

PART XIV

APPEALS AND OTHER PROCEEDINGS

Interpretation of this Part.

81. In this Part –

"**complainant**" means a person who makes a complaint, and

"**the Court**", in relation to any appeal, means –

(a) where the appellant –

(i) is an Alderney person, or –

(ii) is neither a Guernsey person nor a Sark person, but has the appellant's principal or prospective principal place of business in Alderney,

the Court of Alderney,

(b) where the appellant –

(i) is a Sark person, or

(ii) is neither a Guernsey person nor an Alderney person, but has the appellant's principal or prospective principal place of business in Sark,

the Court of the Seneschal, and

(c) in any other case, the Royal Court.

Complainant may appeal failure to notify investigation or progress.

82. (1) A complainant may appeal to the Court against any failure of the Authority to give the complainant –

(a) written notice that the complaint is either being investigated or not being investigated, within the two-month period specified by section 68(3)(a) or (4), or

(b) if the complaint is being investigated, written notice of the progress and, where applicable, the outcome of the investigation within the three-month period specified by section 68(3)(b).

(2) The grounds of an appeal under this section are that the Authority failed to comply with a requirement to give written notice in accordance with section 68(3) or (4), but for the avoidance of doubt any such requirement is subject to the exception in section 68(6).

(3) An appeal under this section must be made within the period of 28 days immediately following –

(a) in an appeal under subsection (1)(a), the date on which the two-month period mentioned in that provision expires, and

(b) in an appeal under subsection (1)(b), the date on which the three-month period mentioned in that provision expires.

(4) An appeal under this section is made by summons served on the Authority stating the grounds and material facts on which the appellant relies.

(5) Where an appeal is made under this section, the Authority may apply to the Court by summons served on the appellant for an order to dismiss the appeal for want of prosecution; and on hearing the application the Court may –

(a) dismiss the appeal or dismiss the application (in either case on such terms and conditions as the Court may direct), or

(b) make such other order as the Court considers just.

(6) The provisions of subsection (5) are without prejudice to the inherent powers of the Court or to the provisions of rule 52 of the Royal Court Civil Rules, 2007[b], rule 51 of the Court of Alderney Civil Rules, 2005[c] or any similar civil rule of the Court of the Seneschal.

(7) Upon determining an appeal under this section, the Court may–

(a) dismiss the appeal, or

(b) uphold the appeal and order the Authority to give the appellant the written acknowledgment or notice sought in the appeal,

and make any other order it considers just.

(8) An appeal from a decision of the Royal Court under this section lies to the Court of Appeal on a question of law.

Complainant may appeal determinations.

83. (1) A complainant may appeal to the Court against a determination of the Authority –

(a) under section 68(1)(b) not to investigate the complaint, or

---

[b] Order of the Royal Court No. IV of 2007, as amended by Order of the Royal Court No. II of 2008 and No. IV of 2009.

[c] As amended by the Court of Alderney Civil (Amendment) Rules, 2015.

(b) under section 71(1)(a) that a controller or processor has not breached or is not likely to breach an operative provision, in connection with the complaint.

(2) The grounds of an appeal under this section are that –

(a) the determination was *ultra vires* or there was some other error of law,

(b) the determination was unreasonable,

(c) the determination was made in bad faith,

(d) there was a lack of proportionality, or

(e) there was a material error as to the facts or as to the procedure.

(3) An appeal under this section must be made within the period of 28 days immediately following the date on which the complainant receives written notice of the determination from the Authority.

(4) An appeal under this section is made by summons served on the Authority stating the grounds and material facts on which the appellant relies.

(5) Where an appeal is made under this section, the Authority may apply to the Court by summons served on the appellant for an order to dismiss the appeal for want of prosecution; and on hearing the application the Court may –

(a) dismiss the appeal or dismiss the application (in either case on such terms and conditions as the Court may direct), or

(b) make such other order as the Court considers just.

(6) The provisions of subsection (5) are without prejudice to the inherent powers of the Court or to the provisions of rule 52 of the Royal Court Civil Rules, 2007, rule 51 of the Court of Alderney Civil Rules, 2005 or any similar civil rule of the Court of the Seneschal.

(7) Upon determining an appeal under this section, the Court may –

(a) confirm the determination, or

(b) annul the determination and remit the matter back to the Authority for reconsideration,

and make any other order it considers just.

(8) An appeal from a decision of the Royal Court under this section lies to the Court of Appeal on a question of law.

Sanctioned person may appeal breach determination or enforcement order.

84. (1) The person concerned may appeal to the Court against –

(a) a breach determination made by the Authority, or

(b) an enforcement order.

(2) The grounds of an appeal under this section are that –

(a) the determination or order was *ultra vires* or there was some other error of law,

(b) the determination or order was unreasonable,

(c) the determination or order was made in bad faith,

(d) there was a lack of proportionality, or

(e) there was a material error as to the facts or as to the procedure.

(3) An appeal must be made within the period of 28 days immediately following the date on which the person concerned receives written notice of the determination or order from the Authority.

(4) An appeal is made by summons served on the Authority stating the grounds and material facts on which the appellant relies.

(5) Where an appeal is made, the Authority may apply to the Court by summons served on the appellant for an order to dismiss the appeal for want of prosecution; and on hearing the application the Court may –

(a) dismiss the appeal or dismiss the application (in either case on such terms and conditions as the Court may direct), or

(b) make such other order as the Court considers just.

(6) The provisions of subsection (5) are without prejudice to the inherent powers of the Court or to the provisions of rule 52 of the Royal Court Civil Rules, 2007, rule 51 of the Court of Alderney Civil Rules, 2005 or any similar civil rule of the Court of the Seneschal.

(7) On the application of the appellant, the Court may, on such terms as the Court thinks just, suspend or modify the effect of the determination or order appealed pending the determination of the appeal.

(8) Upon determining an appeal under this section, the Court may –

(a) confirm the determination or order, with or without modification, or

(b) annul the determination or order and –

(i) remit the matter back to the Authority for reconsideration, or

(ii) make, in its place, any determination or order that the Authority is authorised to make under this Law,

and make any other order it considers just.

(9) An appeal from a decision of the Royal Court under this section lies to the Court of Appeal on a question of law.

Authority may bring civil proceedings in respect of breach or anticipated breach.

85. (1) On request by a data subject or on its own initiative, the Authority may bring proceedings before the Court in respect of any breach or anticipated breach of an operative provision by a controller or a processor.

(2) Where proceedings are brought under subsection (1) and the Court is satisfied that an operative provision has been or is likely to be breached by the controller or processor, the Court may make any order, relief and remedy it considers just under the circumstances, including, for the avoidance of doubt, in the case of the Royal Court –

(a) an award of compensation to any person who suffers damage as a result of the breach,

(b) an injunction or interim injunction to restrain any actual or anticipated breach of an operative provision, and

(c) a declaration that the controller or processor has committed a breach of an operative provision, or that a particular act, omission or course of conduct on the part of the controller or processor would result in a breach of an operative provision.

(3) Despite any rule of law to the contrary, a court in which an action is brought under this section may grant an order, relief or remedy of a kind mentioned in subsection (2) in respect of any distress, inconvenience or other adverse effect suffered by a person even if it does not result from any physical or financial loss or damage.

Suspension of court proceedings.

86. (1) This section applies where –

(a) any proceedings ("**Court A's proceedings**") relating to processing in the context of a controller or processor are pending before any court ("**Court A**") under or in relation to this Law (including an action or appeal under this Law, or an appeal against any determination made under this Law), and

(b) proceedings ("**Court B's proceedings**") are pending in any other court or tribunal ("**Court B**"), whether in the Bailiwick or elsewhere, concerning the same subject matter and processing in the context of the same controller or processor.

(2) Where this section applies, Court A –

(a) must contact Court B to confirm the existence and nature of Court B's proceedings,

(b) may suspend Court A's proceedings until Court B's proceedings have been completed and determined, and

(c) may decline to hear and determine Court A's proceedings if –

(i) Court A's proceedings are proceedings at first instance, and

(ii) Court B had been seized of Court B's proceedings before Court A was seized of Court A's proceedings.

PART XV

OFFENCES AND CRIMINAL PROCEEDINGS

Unlawful obtaining or disclosure of personal data.

87. (1) A person is guilty of an offence who knowingly or recklessly –

(a) obtains or discloses personal data without the consent of the controller,

(b) procures the disclosure of personal data to another person without the consent of the controller, or

(c) after any personal data is obtained or disclosed without the consent of the controller, retains that personal data without the consent of the person who would otherwise have been the controller of the data.

(2) Subsection (1) does not apply to a person who shows –

(a) that the obtaining, disclosing, procuring or retaining was required or authorised by law,

(b) that the person acted in the reasonable belief that the obtaining, disclosing, procuring or retaining was required or authorised by law,

(c) that the person acted in the reasonable belief that the person would have had the consent of the controller if the controller had known of the obtaining, disclosing, procuring or retaining and the circumstances of it,

(d) that the person acted –

(i) for the purpose of journalism or an artistic, literary or academic purpose,

(ii) with a view to the publication by any person of any journalistic, artistic, literary or academic material, and

(iii) in the reasonable belief that in the particular circumstances the obtaining, disclosing, procuring or (as the case may be) retaining was justified as being in the public interest,

(e) that the obtaining, disclosing, procuring or retaining was necessary for a law enforcement purpose, or

(f) that in the particular circumstances the obtaining, disclosing, procuring or (as the case may be) retaining was justified as being in the public interest.

(3) A person who sells personal data is guilty of an offence if the person has obtained the data in contravention of subsection (1).

(4) A person who offers to sell personal data is guilty of an offence if –

(a) the person has obtained the data in contravention of subsection (1), or

(b) the person subsequently obtains the data in contravention of that subsection.

(5) For the purposes of subsection (4), an advertisement indicating that personal data is or may be for sale is an offer to sell the data.

(6) For the purposes of this section, a reference to personal data includes information extracted from personal data.

Obstruction, etc. or provision of false, deceptive or misleading information.

88. (1) A person is guilty of an offence if the person –

(a) intentionally obstructs,

(b) without reasonable excuse, fails to comply with any requirement made by, or

(c) removes, tampers or otherwise interferes with any thing secured against interference by,

an Authority official acting in the exercise or performance of any function under this Law.

(2) A person is guilty of an offence if –

(a) for the purposes of or in connection with an application made under this Law,

(b) in purported compliance with any condition of a registration or an approval under this Law,

(c) for the purposes of, or in connection with, obtaining consent to processing,

(d) in purported compliance with any requirement imposed by, or otherwise for the purposes of, this Law, or

(e) otherwise than as mentioned in paragraphs (a) to (d) but in circumstances in which the person intends, or could reasonably be expected to know, that the information would or might be used by an Authority

official acting in the exercise or performance of a function under this Law,

that person does any of the following –

(i) makes a statement which that person knows or has reasonable cause to believe to be false, deceptive or misleading in a material particular,

(ii) recklessly makes a statement, dishonestly or otherwise, which is false, deceptive or misleading in a material particular,

(iii) produces or furnishes, or causes or permits to be produced or furnished, any information which that person knows or has reasonable cause to believe to be false, deceptive or misleading in a material particular, or

(iv) recklessly produces or furnishes or recklessly causes or permits to be produced or furnished, dishonestly or otherwise, any information which is false, deceptive or misleading in a material particular.

(3) For the avoidance of doubt, in this section, "**requirement**" includes any requirement made in the exercise of a power conferred by Schedule 7.

Impersonation of Authority officials.

89. A person is guilty of an offence if, with intent to deceive, the person –

(a) impersonates an Authority official,

(b) makes any statement or does any act calculated to falsely suggest that the person is an Authority official, or

(c) makes any statement or does any act calculated to falsely suggest that the person has powers as an Authority official that exceed the powers that the person actually has.

Duty of confidentiality.

90. (1) This section applies where a designated official acquires any information from which a person (whether or not an individual) ("**the identifiable person**") is identified or identifiable –

(a) in the exercise or performance of any function under this Law, or otherwise under or for the purposes of this Law, or

(b) directly or indirectly from any person who acquired the information in the exercise or performance of any function conferred or imposed on that person under this Law, or otherwise under or for the purposes of this Law.

(2) Except as authorised by section 91, the designated official must not, without the consent of the identifiable person –

(a) use the information, or

(b) disclose the information.

(3) Where the designated official is an individual, the individual's duty in subsection (2) survives the expiry or termination of that individual's office, employment, appointment or designation as a designated official.

(4) A person who fails to comply with or contravenes subsection (2) is guilty of an offence.

(5) In this section and section 91, "**designated official**" means –

(a) an Authority official,

(b) an agent of the Authority or the Commissioner, or

(c) a data protection officer.

Exceptions to confidentiality.

91. (1) A designated official may use, or disclose to another person, the information mentioned in section 90(1) where –

(a) at the time of use or disclosure, the information is or has already been made public (other than through an act or omission of the official),

(b) the information used or disclosed is in the form of a summary or collection so framed as not to enable information relating to any identifiable person to be ascertained from it,

(c) the use or disclosure is necessary for the purpose of –

(i) exercising or performing any function conferred or imposed on the official by this Law,

(ii) enabling or assisting any other person to exercise or perform functions conferred or imposed by this Law,

(iii) enabling or assisting a competent supervisory authority to exercise or perform functions conferred or imposed by or under a comparable foreign enactment, or

(iv) seeking advice from a qualified person on any matter requiring the exercise of professional skills, for a purpose mentioned in subparagraph (i), (ii) or (iii),

(d) the use or disclosure is necessary for the purposes of any legal proceedings, including any proceedings arising out of this Law or a comparable foreign enactment,

(e) the use or disclosure is necessary to enable or assist the pursuit of a law enforcement purpose,

(f) the use or disclosure is necessary for the purposes of enabling or assisting the instigation, defence, or conduct of disciplinary proceedings against any person in relation to–

(i) a breach of a provision of this Law, or

(ii) compliance with this Law resulting in a breach of the person's professional or other duties,

(g) the use or disclosure is necessary for the purposes of complying with an order of a court or tribunal, or

(h) the use or disclosure is necessary for the purposes of discharging any international obligations of the Bailiwick.

(2) In subsection (1), "**comparable foreign enactment**" means any enactment in any country other than the Bailiwick that is similar or comparable in purpose or effect to this Law.

Criminal liability of directors and other officers.

92. (1) Where an offence under this Law is committed by a body corporate, limited partnership with legal personality or foundation and is proved to

have been committed with the consent or connivance of, or to be attributable to any neglect on the part of –

(a) in the case of a body corporate, any director, controller, manager, secretary or other similar officer,

(b) in the case of a limited partnership with legal personality, any general partner,

(c) in the case of a foundation, any foundation official, or

(d) any person purporting to act in a capacity described in paragraph (a), (b) or (c),

that person as well as the body corporate, limited partnership or foundation is guilty of the offence and may be proceeded against and punished accordingly.

(2) Where the affairs of a body corporate are managed by its members, subsection (1) applies to a member in connection with the member's functions of management as if the member were a director.

Criminal proceedings against unincorporated bodies.

93. (1) Where an offence under this Law is committed by an unincorporated body and is proved to have been committed with the consent or connivance of, or to be attributable to any neglect on the part of –

(a) in the case of a partnership (not being a limited partnership with legal personality, or a limited liability

partnership incorporated under the Limited Liability Partnerships (Guernsey) Law, 2013[d]), any partner,

(b) in the case of any other unincorporated body, any officer of that body who is bound to fulfil any duty of which the offence is a breach or, if there is no such officer, any member of the committee or other similar governing body, or

(c) any person purporting to act in a capacity described in paragraph (a) or (b),

that person as well as the unincorporated body is guilty of the offence and may be proceeded against and punished accordingly.

(2) Where an offence under this Law is alleged to have been committed by an unincorporated body, proceedings for the offence must, without prejudice to subsection (1), be brought in the name of the body and not in the name of any of its members.

(3) A fine imposed on an unincorporated body on its conviction for an offence under this Law must be paid from the funds of the body.

Penalties and court orders for offences.

94. (1) A person guilty of an offence under section 90 is liable –

---

d Order in Council No. VI of 2014; as amended by Order in Council No. VI of 2017; Ordinance No. XII of 2015; and No. IX of 2016.

(a) on summary conviction, to a fine not exceeding level 5 on the uniform scale, and

(b) on conviction on indictment, to a fine.

(2) A person guilty of an offence under any other provision of this Law is liable –

(a) on summary conviction, to imprisonment for a term not exceeding 12 months, or to a fine not exceeding level 5 on the uniform scale, or to both, and

(b) on conviction on indictment, to imprisonment for a term not exceeding two years, or a fine, or to both.

(3) Subject to subsection (4), the court by or before which a person is convicted of an offence under this Law may order any document used in connection with the processing of personal data and appearing to the court to be connected with the commission of the offence to be forfeited, destroyed or erased.

(4) The court must not make an order under subsection (3) in relation to any document where a person (other than the offender) claiming to be the owner of or otherwise interested in the document applies to be heard by the court, unless an opportunity is given to that person to show cause why the order should not be made.

Penalties for offences tried before the Court of Alderney or the Court of the Seneschal.

95. In relation to offences under this Law tried before the Court of Alderney or the Court of the Seneschal, the penalties stipulated by this Law in relation to summary conviction for an offence are applicable notwithstanding the provisions of section 13 of the Government of Alderney Law, 2004[e] or section 11 of the Reform (Sark) Law, 2008[f].

PART XVI

GENERAL AND MISCELLANEOUS

General exceptions and exemptions.

96. Schedule 8 has effect.

Representation of data subjects.

97. Any person may, by agreement with a data protection organisation, authorise the organisation on the person's behalf, to –

(a) make a complaint under section 67 and represent the person in any proceedings arising from the complaint, or

(b) bring an action under section 79 and represent the person in any proceedings arising from the action,

---

[e] Order in Council No. III of 2005; as amended by Order in Council No. XXII of 2010; No. XI of 2012; No. V of 2014; Alderney Ordinance No. IX of 2016.

[f] Order in Council No. V of 2008; as amended by Order in Council No. VI of 2008; No. XXVII of 2008; No. XIV of 2010; No. XII of 2011; No. XI of 2014; Sark Ordinance Nos. II and VI of 2015.

including, if agreed with that person, receiving all or any part of any damages awarded to that person when the action is determined.

Avoidance of certain contractual terms relating to health records.

98. (1) Any term or condition of a contract is void in so far as it purports to require an individual to supply or produce to any other person –

(a) a health record, or

(b) a copy or part of any health record.

(2) In subsection (1), "**health record**", in relation to any individual, means any health data –

(a) made or compiled by or on behalf of a health professional in connection with the care of that individual, and

(b) obtained or to be obtained by the individual in the exercise of a data subject right.

Proceedings concerning unincorporated bodies.

99. Subject to section 93, where a breach of an operative provision is alleged to have been committed by an unincorporated body, any complaint, investigation, action, order or notice, or other proceedings, for or otherwise in relation to the breach must be brought, issued or (as the case may be) served in the name of the body and not in the name of any of its members.

Protection from self-incrimination.

100. (1) A statement made by a person in response to a requirement imposed by or under this Law ("**the statement concerned**") –

(a) may be used in evidence against the person in proceedings other than criminal proceedings, and

(b) may not be used in evidence against the person in criminal proceedings except –

(i) where evidence relating to the statement concerned is adduced, or a question relating to the statement concerned is asked, in the proceedings by or on behalf of that person, or

(ii) in proceedings for –

(A) an offence under section 88(2),

(B) perjury,

(C) perverting the course of justice, or

(D) any other offence where, in giving evidence the person makes a statement inconsistent with the statement concerned, in which case it is admissible only to the extent necessary to establish the inconsistency.

(2) Despite subsection (1)(b), information disclosed by any person in compliance with any request under section 14 or 15 is not admissible against the person in proceedings for any offence under this Law.

Exclusion of liability.

101. (1) Subject to subsection (2), an Authority official is not liable in damages or personally liable in any civil proceedings in respect of anything done or omitted to be done after the commencement of this Law in the discharge or purported discharge of the functions of the Authority official under this Law, unless the thing was done or omitted to be done in bad faith.

(2) Subsection (1) does not apply so as to prevent an award of damages in respect of the act or omission on the ground that it was unlawful as a result of section 6(1) of the Human Rights (Bailiwick of Guernsey) Law, 2000[g].

Service of documents.

102. (1) Any document to be given or served under or for the purposes of this Law may be given or served –

(a) on an individual, by being delivered to the individual, or by being left at, or sent by post or transmitted to, the individual' s usual or last known place of abode,

(b) on a company, by being left at, or sent by post or transmitted to, its registered office,

---

[g] Order in Council No. XIV of 2000; as amended by Order in Council No. I of 2005; Ordinance No. XXXVII of 2001; No. XXXIII of 2003; No. XX of 2015; No. IX of 2016; and G.S.I. No. 27 of 2006.

(c) on an overseas company, by being left at, or sent by post or transmitted to, its principal or last known principal place of business in the Bailiwick or, if there is no such place, its registered or principal office or last known registered or principal office elsewhere,

(d) on an unincorporated body, by being given to or served on any partner, member, manager or authorised officer thereof in accordance with paragraph (a), or by being left at, or sent by post or transmitted to, the body's principal or last known principal place of business in the Bailiwick or, if there is no such place, its principal or last known principal place of business elsewhere, or

(e) on an Authority official, by being left at, or sent by post or transmitted to, the offices of the Authority or any other prescribed office.

(2) In subsection (1) –

(a) the expression "**by post**" means by recorded delivery service or ordinary letter post, and

(b) the expression "**transmitted**" means transmitted by electronic communication, facsimile transmission or other similar means which produce or enable the production of a document containing the text of the

communication; in which event the document is to be regarded as served when it is received.

(3) If a person notifies the Authority of an address for service within the Bailiwick for the purposes of this Law, any document to be given to or served on the person may be given or served by being left at, or sent by post or transmitted to, that address.

(4) If service of a document cannot, after reasonable enquiry, be effected by the Authority in accordance with this section, the document may be served –

(a) by being published in such manner and for such period as the Authority thinks fit, or

(b) by being published in La Gazette Officielle on two occasions falling in successive weeks,

and a document served under this subsection is sufficient if addressed to the person for whom it is intended.

(5) Subsections (1) to (4) are without prejudice to any other lawful method of service.

(6) Despite subsections (1) to (5) and (8) and any other enactment or rule of law in relation to the service of documents, no document to be given to or served on the Authority under or for the purposes of this Law is to be regarded as having been given or served until it is received.

(7) If a person upon whom a document is to be served under this Law is person under legal disability, the document must be served on the person's guardian; and if there is no guardian, the party wishing to effect service may apply to the court for the appointment of a person to act as guardian for the purposes of this Law.

(8) A document sent by post is, unless the contrary is shown, deemed for the purposes of this Law to have been received –

(a) in the case of a document sent to an address in the United Kingdom, the Channel Islands or the Isle of Man, on the third day after the day of posting,

(b) in the case of a document sent elsewhere, on the seventh day after the day of posting,

excluding in each case any day which is not a working day.

(9) Service of a document sent by post is to be proved by showing the date of posting, the address thereon and the fact of prepayment.

(10) In this section –

"**document**" excludes a summons, and

"**working day**" means any day other than a Saturday, a Sunday or a non-business day within the meaning of section 1(1) of the Bills of Exchange (Guernsey) Law, 1958[h].

(11) The provisions of this section are subject to any contrary provision in this Law.

Ordinances for law enforcement purposes.

103. (1) The States of Deliberation may by Ordinance make such provision as they think fit relating to –

(a) the processing of personal data for a law enforcement purpose, or

(b) personal data which is or was processed for a law enforcement purpose.

(2) Without limiting the generality of subsection (1), the States of Deliberation may by Ordinance make provision to protect the rights of individuals in relation to their personal data in a manner equivalent to the Law Enforcement Directive.

Ordinances relating to electronic communications.

104. (1) The States of Deliberation may by Ordinance make such provision as they think fit relating to respect for private life and protection of personal data in relation to electronic communications.

---

h Ordres en Conseil Vol. XVII, p. 384 as amended by Ordres en Conseil Vol. XXIV, p. 84, Vol. XXXIV, p. 504 and Vol. XXXV (1), p. 367.

(2) Without limiting the generality of subsection (1), the States of Deliberation may by Ordinance –

(a) make provision to protect the rights of individuals in relation to their personal data in a manner equivalent to any Community provision relating to respect for private life and protection of personal data in relation to electronic communications, and

(b) repeal or amend all or any part of –

(i) the European Communities (Implementation of Privacy Directive) (Guernsey) Ordinance, 2004[i],

(ii) the European Communities (Implementation of Council Directive on Privacy and Electronic Communications) (Sark) Ordinance, 2004, and

(iii) the European Communities (Implementation of Council Directive on Privacy and Electronic Communications) (Alderney) Ordinance, 2009[j].

---

[i] Ordinance No. XXIV of 2004; as amended by Ordinance No. II of 2010; No. XIII of 2012; and No. IX of 2016.

[j] Alderney Ordinance No. VIII of 2009; as amended by Alderney Ordinance No. III of 2010; and Alderney Ordinance No. XIII of 2012.

Ordinance relating to identifiers or personal data.

105. (1) The States of Deliberation may by Ordinance make any provision they think fit for any or all of the following purposes –

(a) requiring or authorising any identifier or personal data to be processed in a specified manner or in specified circumstances, or

(b) prohibiting or restricting any identifier or personal data from being processed in a specified manner or in specified circumstances.

(2) Without limiting the generality of subsection (1), an Ordinance made under subsection (1) may include provisions relating to –

(a) the processing of personal data in the context of employment or in the context of the provision of medical, health or social care or treatment,

(b) safeguards for the significant interests of data subjects,

(c) the transparency of processing,

(d) the transfer of identifiers or personal data within a group of undertakings or within a group of enterprises engaged jointly in a business, or

(e) the monitoring of the application of the Ordinance or this Law.

(3) In subsection (2)(a) "**in the context of employment**" includes in the context of –

(a) recruitment,

(b) the performance of a contract of employment, including the discharge of duties laid down by law,

(c) management, planning and organisation of work, including business continuity,

(d) equality and diversity in the workplace,

(e) health and safety at work,

(f) protection of the property of employers or customers,

(g) the exercise and enjoyment, on an individual or collective basis, of rights and benefits related to employment, and

(h) the termination of an employment relationship.

Power to amend this Law.

106. (1) The States of Deliberation may by Ordinance amend this Law where it appears to be necessary or expedient to do so in order 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 GDPR or the Law Enforcement Directive,

(b) implement any other Community provision or any provision of the Convention or any other international agreement (whether or not applicable in or binding on the Bailiwick) relating to the processing or protection of personal data,

(c) enable the Authority and the Commissioner to effectively and efficiently exercise or perform their functions,

(d) ensure the effective, efficient and fair conduct of investigations and inquiries by the Authority,

(e) maintain or enhance the reputation or standing of the Bailiwick, in relation to the processing or protection of personal data,

(f) make provision relating to any matter of a kind for which regulations may be made under any provision of this Law,

(g) ensure the effective enforcement of this Law, or

(h) provide for any other matters necessary or expedient for giving full effect to this Law and for its due administration.

(2) Without limiting subsection (1), the States of Deliberation may by Ordinance amend all or any part of Schedule 2.

(3) In subsection (1)(b), "**implement**" in relation to any provision, includes to enforce or enact the provision, and to secure the administration, execution, recognition, exercise or enjoyment of the provision, in or under the law of the Bailiwick.

Power to make transitional, savings and consequential provisions by Ordinance.

107. (1) The States of Deliberation may by Ordinance make any transitional, savings or consequential provisions they think fit in connection with the commencement of any provision of this Law.

(2) Without limiting subsection (1), an Ordinance under that subsection may –

(a) repeal, revoke or amend any provision of any enactment that is inconsistent with any provision of this Law, and

(b) make any other consequential amendments to any enactment that the States of Deliberation think fit.

(3) This section does not affect or limit any other provision of this Law empowering the States of Deliberation to make an Ordinance.

(4) In this section and section 108, "**enactment**" –

(a) includes this Law, but

(b) excludes an Act of Parliament that applies or extends to the Bailiwick.

General provisions as to Ordinances.

108. (1) An Ordinance under this Law –

(a) may be amended or repealed by a subsequent Ordinance, and

(b) may contain such consequential, incidental, supplementary, transitional and savings provisions as may appear to be necessary or expedient (including, without limitation, provision making consequential amendments to any enactment).

(2) Any power to make an Ordinance under this Law may be exercised –

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

(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, or

(iii) any such provision either unconditionally or subject to any prescribed conditions.

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

(a) exempt from all or any part of this Law, or conversely apply all or any part of this Law (with or without modifications) to –

(i) the processing of personal data in any specified manner or circumstances, or

(ii) personal data of any specified kind or description,

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

(c) empower the Authority, any public committee, any other body or authority (including, without limitation, any court of the Bailiwick), or any other person to –

(i) make subordinate legislation, or

(ii) issue codes or guidance,

in relation to any matter for which an Ordinance may be made under this Law,

(d) provide that no liability shall be incurred by any person in respect of anything done or omitted to be done in the discharge or purported discharge of any of the person's functions unless the thing is done or omitted to be done in bad faith,

(e) make provision under the powers conferred by this Law despite the provisions of any enactment for the time being in force,

(f) repeal, replace, amend, extend, adapt, modify or disapply any rule of custom or law, and

(g) without prejudice to the generality of the foregoing, make any such provision of any such extent as might be made by Projet de Loi, but may not provide that a person is to be guilty of an offence as a result of any retrospective effect of the Ordinance.

(4) An 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 recommending that the States of Deliberation agree to make an Ordinance under this Law, the Committee must consult –

(a) the Authority,

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

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

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

General provisions as to regulations.

109. (1) Regulations under this Law -

(a) may be amended or repealed by subsequent regulations made under this Law,

(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 Law 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 Law, regulations under this Law –

(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 Law, and

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

(4) Regulations under this Law 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 Law, the Committee must consult –

(a) the Authority,

(b) in the case of regulations having effect in Alderney, the Policy & 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 Law.

Expressions with special meanings.

110. Schedule 9 has effect.

Interpretation of this Law.

111. (1) In this Law, unless the context requires otherwise –

"**adequacy decision**", in respect of any country, sector within a country or international organisation, means a decision made by the European Commission that the relevant country, sector or international organisation ensures an adequate level of protection within the meaning of Article 45(2) of the GDPR,

"**administrative fine**" means a fine ordered by the Authority under sections 73(2)(g) and 74,

"**Alderney person**" means –

(a) an individual ordinarily resident in Alderney,

(b) a company incorporated under the Companies (Alderney) Law, 1994[k], or

(c) a public authority of Alderney,

"**approved code**" means –

(a) a code of conduct, or an amendment or extension to such a code, approved under section 52, or

(b) any other code of conduct, or an amendment or extension to such a code, approved by a competent supervisory authority of an authorised jurisdiction.

"**approved mechanism**" means –

(a) a certification mechanism approved in accordance with regulations made under section 54, or

(b) any other certification mechanism approved by a competent supervisory authority of an authorised jurisdiction,

"**authorised jurisdiction**" means –

(a) the Bailiwick,

---

k Ordres en Conseil Vol. XXXV(2), p. 777; there are amendments not relevant to this Law.

(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 45(2) of the GDPR (or the equivalent article of the former Directive), and for which the determination is still in force, or

(d) a designated jurisdiction,

"**authorised officer**" means –

(a) the Commissioner, or

(b) in relation to any function of an authorised officer –

(i) any other employee of the Authority, or

(ii) any other individual,

authorised by the Authority or the Commissioner to exercise or perform the function,

"**the Authority**" mean the Data Protection Authority established by Part XI,

"**Authority official**" or "**official**" means –

(a) the Authority or any member of it,

(b) the Commissioner or any other employee of the Authority, or

(c) any authorised officer, where the officer is neither a member nor an employee of the Authority,

"**automated processing**" includes profiling,

"**the Bailiwick**" –

(a) means the Bailiwick of Guernsey, including the territorial waters adjacent to it, and

(b) includes any part of the Bailiwick of Guernsey,

"**bankrupt**", in relation to any individual, means –

(a) that the individual has been declared by the Royal Court to be insolvent or that a Commissioner or Committee of Creditors has been appointed by the Royal Court to supervise or secure the individual's estate,

(b) that the individual's affairs have been declared in a state of "désastre" by the individual's arresting creditors at a meeting held before a Commissioner of the Royal Court,

(c) that a preliminary vesting order has been made against the individual in respect of any of the individual's real property in the Bailiwick, or

(d) that a composition or arrangement with creditors has been entered into in respect of the individual whereby the individual's creditors will receive less than 100p in the pound or that possession or control has been taken of any of the individual's property or affairs by or on behalf of creditors,

and includes analogous procedures and declarations in any country other than the Bailiwick,

"**binding corporate rules**" means personal data protection policies which are adhered to by a controller or processor established in an authorised jurisdiction for transfers or a set of transfers of personal data to a controller or processor in one or more unauthorised jurisdictions within a group of undertakings, or group of enterprises engaged jointly in a business,

"**biometric data**" means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of an individual, which allows or confirms the unique identification of that individual, such as facial images or dactyloscopic data,

"**body corporate**" means a body corporate, of whatever description, incorporated with or without limited liability in any part of the world,

"**breach**" or "**likely to breach**", in relation to any operative provision or duty: see paragraph 7 of Schedule 9,

"**breach determination**", in relation to a controller or processor, means a determination by the Authority under section 71(1)(a) or 72(1)(b)(i) that the controller or processor has breached or is likely to breach an operative provision,

"**business**" –

(a) includes any activity, trade or profession, whether or not carried on for profit, and

(b) for the avoidance of doubt, includes an activity, trade or profession carried out by a non-profit organisation or charity,

"**by law**" includes by –

(a) any enactment,

(b) any judgment or decision of a court or tribunal having legal and binding effect,

(c) any rule of law (including a rule of common law),

(d) professional privileges and duties, or

(e) customary law,

"**category**" –

(a) in relation to personal data, processing, data subject or other persons, means a kind or description of the personal data, processing or (as the case may be) data subject or other person, and

(b) in relation to personal data, includes whether the personal data is special category data,

"**child**" means an individual under 18 years of age,

"**the Commissioner**" means the individual appointed as the Commissioner by the Authority under paragraph 5 of Schedule 6,

"**the Committee**" means the States of Guernsey Committee for Home Affairs,

"**Community provision**" has the meaning given by section 3(1) of the European Communities (Implementation) (Bailiwick of Guernsey) Law, 1994[1],

"**competent supervisory authority**" –

(a) means any public authority of an authorised jurisdiction that exercises or performs functions

---

1 Ordres en Conseil Vol. XXXV(1), p. 65.

equivalent or similar to the Authority's functions under this Law, and

(b) includes the European Data Supervisory Board,

"**complaint**" means a complaint under section 67,

"**consent**": see section 10,

"**controller**" –

(a) means a person that, alone or jointly with others, determines the purposes and means of the processing of any personal data, and

(b) for the avoidance of doubt, includes a processor or any other person, where the processor or other person determines the purposes and means of processing personal data,

"**controller's representative**" means a person designated to be the representative of a controller in the Bailiwick under section 38,

"**controlling undertaking**", in relation to a group of undertakings, means the undertaking which can exert a dominant influence over the other undertakings in the group, by virtue, for example, of –

(a) ownership, financial participation or the rules which govern the group,

(b) the power to have personal data protection rules implemented within the group, or

(c) control over the processing of personal data in undertakings affiliated to it, and

"**controlled undertaking**" has a corresponding meaning,

"**the Convention**" means the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data which was opened for signature on 28th January 1981[m], and includes any protocol to the Convention extended to the Bailiwick,

"**country**" includes territory,

"**criminal data**" means personal data relating to –

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

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

---

m European Treaty Series No. 108.

"**damage**" includes financial loss, distress, inconvenience and other adverse effects,

"**data protection impact assessment**" means an assessment carried out in accordance with section 44,

"**data protection officer**" means an individual designated as a data protection officer under section 47 or 48,

"**data protection organisation**" means –

(a) a non-profit organisation or charity, which has as one of its objects or purposes, the protection of personal data, data subject rights or any other significant interests of data subjects, or

(b) any other prescribed organisation,

"**data protection principle**" means a principle specified in section 6(2),

"**data subject**", in relation to personal data, means the identified or identifiable individual to whom the personal data relates,

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

"**designated jurisdiction**" means any of the following, where designated by an Ordinance made by the States of Deliberation –

(a) the United Kingdom,

(b) a country within the United Kingdom,

(c) any other country within the British Islands, or

(d) any sector within a country mentioned in paragraph (a), (b) or (c),

"**document**" includes any document in electronic form,

"**duty**" includes obligation,

"**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,

"**enforcement order**" –

(a) means an order made by the Authority under section 73(2), including an order to pay an administrative fine, and

(b) includes any amendment to such an order,

"**enterprise**" means any individual or other person engaged in business, irrespective of its legal form, including partnerships or associations regularly engaged in a business,

"**equipment**" includes any computer or other electronic equipment,

"**established in the Bailiwick**", in relation to any controller, processor or other person, includes a controller, processor or other person that –

(a) is a Guernsey person, Alderney person or Sark person,

(b) maintains in the Bailiwick –

(i) an office, branch or agency through which the person carries on an activity, or

(ii) a regular practice,

(c) causes or permits any processing equipment in the Bailiwick to be used for processing personal data otherwise than for the purposes of transit through the Bailiwick, or

(d) is engaging in effective and real processing activities through stable arrangements in the Bailiwick,

"**fairly**", in relation to processing: see section 8,

"**filing system**" means any structured set of personal data which is accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis,

"**former Directive**" means European Parliament and Council Directive 95/46/EC[n] of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data,

"**foundation**" means –

(a) a foundation created under the Foundations (Guernsey) Law, 2012[o], or

(b) an equivalent or similar body (however named) created or established under the law of any other jurisdiction,

"**foundation official**" means –

(a) in relation to a foundation created under the Foundations (Guernsey) Law, 2012, a foundation official within the meaning of that Law, and

(b) in relation to an equivalent or similar body created or established under the law of another jurisdiction, a

---

n O.J. L 281 of 23.11.1995, p. 31.

o Order in Council No. I of 2013; as amended by Ordinance No. IX of 2016; and No. VI of 2017.

person with functions corresponding to those of a foundation official described in paragraph (a),

"**function**" includes –

(a) any power or duty, and

(b) in relation to a public authority, any act or omission in furtherance of an objective conferred or imposed on the public authority by an enactment,

"**function that is of a public nature**", in relation to any person, includes a function conferred or imposed on the person by any enactment,

"**the GDPR**" means Regulation (EU) 2016/679[p] of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC,

"**general partner**" means –

(a) in relation to a limited partnership falling within paragraph (a) of the definition of "**limited partnership**" in this subsection, a general partner within the meaning of the Limited Partnerships (Guernsey) Law, 1995[q], and

---

[p] O.J. L 119 of 4.5.2016, p. 1.

[q] Ordres en Conseil Vol. XXXVI, p. 264; as amended by Ordres en Conseil Vol. XXXVI, p. 571; Vol. XLI, p. 158; Order in Council No. X of 2007; No. VIII of 2008;

(b) in relation to a limited partnership falling within paragraph (b) of the definition of "**limited partnership**" in this subsection, a person whose liability for, and functions in relation to, the partnership correspond to that of a general partner described in paragraph (a) of this definition,

"**genetic data**" means personal data relating to the inherited or acquired genetic characteristics of an individual which gives unique information about the physiology or the health of that individual, including as a result of an analysis of a biological sample from the individual,

"**group of undertakings**" –

(a) means any controlling undertaking and its controlled undertakings,

(b) includes the States or any other group of public authorities (excluding any court or tribunal acting in its judicial capacity),

"**Guernsey person**" means –

(a) an individual ordinarily resident in Guernsey,

Ordinance No. XXXIII of 2003; No. IX of 2016; G.S.I. No. 89 of 2008 and No. 51 of 2016.

(b) a company incorporated under the Companies (Guernsey) Law, 2008[r],

(c) a limited liability partnership incorporated under the Limited Liability Partnerships (Guernsey) Law, 2013,

(d) an arrangement which is registered as a limited partnership, and in respect of which there is a valid certificate of registration, under the Limited Partnerships (Guernsey) Law, 1995,

(e) a foundation created under the Foundations (Guernsey) Law, 2012, or

(f) a public authority of Guernsey or the Bailiwick of Guernsey,

"**health**" means physical or mental health,

"**health data**" means personal data relating to the health of an individual, including the provision of health care services, which reveals information about the individual's health status,

"**health professional**" means any person who may lawfully practise a profession or occupation referred to in paragraph (a) or (b) of the definition

---

[r] Order in Council No. VIII of 2008; there are amendments not relevant to this Law.

of "**health profession**" in section 4(1) of the Regulation of Health Professions (Enabling Provisions) (Guernsey) Law, 2012[s],

"**high risk**", in relation to the significant interests of data subjects: see paragraph 6 of Schedule 9,

"**historical or scientific purpose**", in relation to processing: see paragraph 5 of Schedule 9,

"**identifiable",** in relation to any individual: see paragraph 1 of Schedule 9,

"**identifier**", in relation to any individual –

(a) means a number or code –

(i) that is assigned to an individual by a controller or processor for the purposes of the operations of the controller or processor, and

(ii) that uniquely identifies that individual, for the purposes of that controller or processor, and

(b) for the avoidance of doubt –

(i) includes location data, and

---

s Order in Council No. IX of 2013; as amended by Ordinance No. IX of 2016.

(ii) includes a social security number or any other unique identification number or unique identification code issued to an individual by a public authority, but

(iii) excludes an individual's name used to identify that individual,

"**in the context of**": for processing in the context of a controller or processor, see paragraph 2 of Schedule 9,

"**individual**" means a living natural person,

"**information**" includes –

(a) personal data,

(b) a copy of personal data in any form,

(c) any notification or notice required under this Law,

(d) any record, and

(e) any document,

"**information notice**" has the meaning given by paragraph 1(8) of Schedule 7,

"**information society service**" means a service as defined in point (b) of Article 1(1) of Directive (EU) 2015/1535[t] of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services,

"**inquiry**" means an inquiry under section 69,

"**international organisation**" means an organisation and its subordinate bodies governed by public international law, or any other body which is set up by, or on the basis of, an agreement between two or more countries,

"**investigation**" means an investigation under section 68,

"**this Law**" includes any Ordinance or subordinate legislation made under this Law,

"**Law Enforcement Directive**" means Directive (EU) 2016/680[u] of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA,

---

t O.J. L 241 of 17.9.2015, p. 1.

u O.J. L 119 of 4.5.2016, p. 89.

"**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, or

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

"**lawfully**", in relation to processing, has the meaning given by section 7,

"**legal proceedings**" includes –

(a) any proceedings by a disciplinary or regulatory body under any enactment, and

(b) any appeal, or public inquiry, under any enactment,

"**limited partnership**" means –

(a) an arrangement which is registered as a limited partnership, and in respect of which there is a valid certificate of registration, under the Limited Partnerships (Guernsey) Law, 1995, or

(b) an arrangement entered into under the laws of a jurisdiction outside Guernsey between two or more persons, under which –

(i) one or more of them is, or are jointly and severally, liable without limitation for all debts and obligations to third parties incurred pursuant to the arrangement, and

(ii) the others have, by whatever means, contributed or agreed to contribute specified amounts pursuant to the arrangement and are not liable for those debts and obligations (unless they participate in controlling the business or are otherwise subjected to a greater liability by those laws in specified circumstances) beyond the amount contributed or agreed to be contributed,

whether with or without legal personality,

"**machine-readable format**" means a format that can easily and readily be processed by a computer, and "**machine-readable**" has a corresponding meaning,

"**member**" means a member of the Authority,

"**monitoring body**" means a body accredited by the Authority under section 53 to monitor compliance with an approved code,

"**necessary**", in relation to any purpose or aim of processing: see paragraph 3 of Schedule 9,

"**non profit organisation**" has the meaning given by section 4(1) of the Charities and Non Profit Organisations (Enabling Provisions) (Guernsey and Alderney) Law, 2009[v],

"**operative provision**" means any provision of Parts II to X of this Law,

"**organisational measures**" includes policies and procedures,

"**parental responsibility**" has the meaning given by section 5 of the Children (Guernsey and Alderney) Law, 2008[w],

"**person**" includes –

(a) an individual,

(b) a body corporate,

(c) any other legal person,

(d) an unincorporated body of persons, and

---

[v] Order in Council No. V of 2010; as amended by Ordinance No. IX of 2016.

[w] Order in Council No. XIV of 2009; as amended by Ordinance No. XI of 2009; No. XLVIII of 2009; Nos. IX and XX of 2016; and No. VI of 2017.

(e) for the avoidance of doubt, a public authority,

"**the person concerned**" –

(a) in relation to any breach determination or sanction, means the controller or processor against whom the determination is made or sanction imposed,

(b) for the avoidance of doubt, in relation to an enforcement order, means the controller or processor against whom the order is made, and

(c) in relation to an information notice, means the person to whom the information notice is given,

"**personal data**" means any information relating to an identified or identifiable individual,

"**personal data breach**" means a breach of security leading to –

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

(b) unauthorised disclosure of, or access to,

personal data transmitted, stored or otherwise processed,

"**police officer**" means –

(a) in relation to Guernsey, Herm and Jethou –

(i) a member of the salaried police force of the Island of Guernsey, or

(ii) within the limits of the officer's jurisdiction, a member of the special constabulary of the Island of Guernsey,

(b) in relation to Alderney –

(i) a member of the salaried police force of the Island of Guernsey,

(ii) a member of any police force which may be established by the States of Alderney, or

(iii) within the limits of their jurisdiction, a special constable appointed under section 47 of the Government of Alderney Law, 2004, and

(c) in relation to Sark -

(i) the Constable, the Vingtenier or the Assistant Constable of Sark,

(ii) a member of the salaried police force of the Island of Guernsey, or

(iii) within the limits of their jurisdiction, a special constable appointed by the Court of the Seneschal,

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

"**premises**" includes any place and any vehicle, vessel, aircraft, offshore installation, tent or moveable structure,

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

"**privileged items**" means –

(a) items subject to legal professional privilege, within the meaning given by section 24 of the Police Powers and Criminal Evidence (Bailiwick of Guernsey) Law, 2003[x], and

(b) any communication between a professional legal adviser and the adviser's client in connection with the giving of legal advice to the client with respect to the client's duties, liabilities or rights under this Law,

---

[x] Order in Council No. XXIII of 2003; there are amendments not relevant to this provision.

"**processing**" –

(a) means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, for example –

(i) collection, recording, organisation, structuring or storage,

(ii) adaptation or alteration,

(iii) retrieval, consultation or use,

(iv) disclosure by transmission, dissemination or otherwise making available,

(v) alignment or combination, or

(vi) restriction, erasure or destruction,

(b) includes any further or continued processing of personal data, falling within paragraph (a), and

(c) for the avoidance of doubt, includes profiling,

and "**process**" and any other cognate expression has a corresponding meaning,

"**processing equipment**" means any equipment used to process personal data,

"**processor**" –

(a) means an individual or other person that processes personal data on behalf of a controller, and

(b) includes a secondary processor within the meaning of section 36(1),

"**profiling**" means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to an individual, including aspects concerning that individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements,

"**progress**", in relation to any investigation or inquiry, includes whether further investigation or coordination with another competent supervisory authority is necessary,

"**proportionality factors**" has the meaning given by paragraph 4 of Schedule 9,

"**pseudonymisation**" means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, where that additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data is not attributed to an identified or identifiable individual, and "**pseudonymise**" has a corresponding meaning,

"**public authority**" means –

(a) the States,

(b) a public committee,

(c) a holder of a public office,

(d) a statutory body,

(e) a court or tribunal of the Bailiwick,

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

(g) 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,

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

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

(j) any other person that exercises or performs any function that is of a public nature in respect of the Bailiwick or any other country,

"**public committee**" means any authority, board, committee or council of the States (however named) constituted by or under a Resolution, a Law or an Ordinance approved by the States,

"**public office**" means any office, however created –

(a) to which functions are specifically assigned by an enactment, and

(b) the holder of which is remunerated out of funds provided by the States or any public committee,

"**public register**" means a register of information that is required to be published by or under any 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,

"**publication**" in relation to any information, means to make that information available to the public or any section of the public in any form or manner, whether free of charge or otherwise, and "**publish**" has a corresponding meaning,

"**recipient**", in relation to personal data –

(a) means any person to which the personal data is disclosed, but

(b) excludes any public authority receiving the personal data in the context of the exercise or performance of its functions in accordance with any enactment,

"**register**", in relation to any controller or processor, means register in accordance with Schedule 4,

"**regulations**" means regulations made by the Committee in accordance with section 109,

"**restriction of processing**" –

(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 specified in a request made under section 22(3),

"**Royal Court**" means the Royal Court sitting as an Ordinary Court, constituted by the Bailiff sitting unaccompanied by the Jurats; and for the purposes of any appeal, or any application for an order, under this Law the Court may appoint one or more assessors to assist it in the determination of any matter before it,

"**safeguard data subject rights**" –

(a) to allow and facilitate the exercise of data subject rights by data subjects, and

(b) to otherwise protect data subject rights,

"**safeguards**", in relation to the protection of personal data or the significant interests of individuals, may include –

(a) technical or organisational measures to ensure that the personal data is processed fairly,

(b) encryption or pseudonymisation of the personal data concerned, and

(c) duties imposed by law, such as duties of confidentiality or secrecy,

"**sanction**" means a sanction authorised by section 73,

"**Sark person**" means –

(a) an individual ordinarily resident in Sark, or

(b) a public authority of Sark,

"**significant interests**", in relation to any individual, means -

(a) any rights or freedoms conferred by law on the individual,

(b) the existence or extent of a duty imposed by law on the individual, or

(c) any other interests of the individual that can reasonably be regarded as significant under the circumstances,

"**special category data**" means –

(a) personal data revealing an individual's –

(i) racial or ethnic origin,

(ii) political opinion,

(iii) religious or philosophical belief, or

(iv) trade union membership,

(b) genetic data,

(c) biometric data,

(d) health data,

(e) personal data concerning an individual's sex life or sexual orientation, or

(f) criminal data,

"**standard data protection clauses**" means standard contractual clauses for data protection –

(a) approved or adopted by the European Commission for the purposes of Article 28 of the GDPR, or

(b) approved by the Authority for the purposes of this Law,

"**the States**" means –

(a) in respect of Guernsey, Herm and Jethou, the States of Guernsey,

(b) in respect of Alderney, the States of Alderney, and

(c) in respect of Sark, the Chief Pleas of Sark,

"**statutory body**" means any authority, board, commission or other body constituted by or under an enactment, other than a public committee,

"**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,

"**third party**", in relation to any processing of personal data, means a person other than–

(a) the data subject, controller or processor, or

(b) a person who, under the direct authority of the controller or processor, is authorised to process the personal data,

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

"**undertaking**" includes –

(a) any establishment, and

(b) any public committee or other public authority,

"**vital interests**", in relation to any individual, includes the life, health or safety of the individual, and

"**voting member**", in relation to the Authority, means the Chairman or any other voting member appointed by resolution of the States of Deliberation under paragraph 1(2) of Schedule 6.

(2) A reference in this Law to a provision or Part of this Law includes a reference to an Ordinance or any regulations made under the provision or Part of this Law.

(3) An expression used in this Law that is also used in the GDPR has the same meaning as in the GDPR unless –

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

(b) the context requires otherwise.

(4) The Interpretation (Guernsey) Law, 1948[y] applies to the interpretation of this Law throughout the Bailiwick.

(5) Any reference in this Law 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.

---

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

Index of defined expressions.

112. Schedule 10 sets out an index of the expressions defined or given meaning by a provision of this Law.

Repeals.

113. The following enactments are repealed –

(a) the Data Protection (Bailiwick of Guernsey) Law, 2001[z],

(b) the Data Protection (Bailiwick of Guernsey) (Amendment) Ordinance, 2010[aa],

(c) the Data Protection (Bailiwick of Guernsey) (Amendment) Ordinance, 2011[bb], and

(d) the Data Protection (Bailiwick of Guernsey) (Amendment) Ordinance, 2012[cc],

Citation.

114. This Law may be cited as the Data Protection (Bailiwick of Guernsey) Law, 2017.

---

[z] 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.

[aa] Ordinance No. II of 2010.

[bb] Ordinance No. XXXIV of 2011.

[cc] Ordinance No. XLIX of 2012.

Commencement.

115. (1) This Law shall come into force on a date appointed by the States of Deliberation by Ordinance.

(2) An Ordinance under subsection (1) may appoint different dates for different provisions of this Law and for different purposes.

SCHEDULE 1

APPLICATION TO THE CROWN, PUBLIC COMMITTEES AND THE POLICE

Section 2(4)

1. Application to the Crown and public committees.

(1) This Law binds the Crown and is applicable to public committees.

(2) Each public committee is to be regarded as a person separate from the other public committees.

(3) An individual in the service of the States is to be regarded as a servant of the public committee to which the individual's responsibilities or duties relate.

(4) Where any notice under this Law is served on a public committee by means of service on the chief officer, chief secretary, president or chairman, however designated, of the public committee, the chief officer, chief secretary, president or chairman, however designated, must ensure that the notice is complied with if the notice requires compliance.

(5) A public committee is not liable to prosecution under this Law.

2. Application to the Police.

(1) This Law applies to the Chief Officer of Police.

(2) For the purposes of this Law –

(a) every member of the salaried police force of Guernsey,

(b) every member of the special constabulary of Guernsey whilst acting as such, and

(c) every special constable appointed by the Court of Alderney whilst acting as such,

is to be regarded as a servant of the Chief Officer of Police.

(3) In this paragraph, "**Chief Officer of Police**" means the chief officer of the salaried police force of Guernsey.

SCHEDULE 2

CONDITIONS FOR PROCESSING TO BE LAWFUL

Sections 7, 18(1), 21(6), 22(4)(c) and 106(2)

The following are conditions for processing to be lawful –

Part I

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

2. The processing is necessary –

(a) for the conclusion or performance of a contract –

(i) to which the data subject is a party, or

(ii) made between the controller and a third party in the interest of the data subject, or

(b) to take steps at the request of the data subject prior to entering into such a contract.

3. The processing is necessary to protect the vital interests of the data subject or any other individual who is a third party.

4. The processing is necessary for the purposes of the legitimate interests of the controller or a third party, except where the processing is in the context of the exercise or performance by a public authority of a function or task described in paragraph 5.

5. The processing is necessary for the exercise or performance by a public authority of –

(a) a function that is of a public nature, or

(b) a task carried out in the public interest.

6. 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 law, otherwise than by an enactment or an order or a judgment of a court or tribunal having the force of law in the Bailiwick.

Part II

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

8. 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.

9. 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.

10. (a) The processing is necessary for a health or social care purpose and is undertaken by –

(i) a health professional, or

(ii) a person who in the circumstances owes a duty of confidentiality which is equivalent to that which would arise if the person were a health professional.

(b) In subparagraph (a) –

"**health or social care purpose**" includes the purpose of –

(i) preventative or occupational medicine,

(ii) the assessment of the working capacity of an employee or worker,

(iii) medical diagnosis,

(iv) the provision of medical, health or social care or treatment, or

(v) the management of medical, health or social care systems and services.

11. (a) The processing –

(i) is necessary for reasons of public health, for example –

(A) for protection against serious threats to public health, or

(B) to ensure high standards of quality and safety for health care, medicinal products or medical devices, and

(ii) is carried out with appropriate safeguards for the significant interests of data subjects.

(b) In subparagraph (a)(i)(B) –

"**medical device**" means –

(i) any medical device, within the meaning of Article 1(2)(a) of Council Directive 93/42/EEC[dd] of 14 June 1993 concerning medical devices, or

(ii) any accessory, within the meaning of Article 1(2)(b) of that Council Directive, and

"**medicinal product**" has the meaning given by section 133 of the Medicines (Human and Veterinary) (Bailiwick of Guernsey) Law, 2008[ee].

12. The processing is necessary –

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

---

dd O.J. L 169 of 12.7.1993, p. 1.

ee Order in Council No. V of 2009; as amended by Ordinance No. XXIV of 2009; and No. XLI of 2013.

(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.

13. 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.

14. The processing –

(a) is in the context of the legitimate activities of any person which –

(i) is not an individual,

(ii) is not established or conducted for profit, and

(iii) exists for political, philosophical, religious or trade-union purposes,

(b) is carried out with appropriate safeguards for the significant interests of data subjects,

(c) relates only to individuals who either are members of the body or association or have regular contact with it in connection with its purposes, and

(d) does not involve disclosure of the personal data to a third party without the consent of the data subject.

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

16. This condition is satisfied if the condition in subparagraph (a) is satisfied, subject to subparagraphs (b) and (c) –

(a) The personal data processed is of a category specified in the left-hand column of the table below, and the processing is necessary for the purpose of identifying or keeping under review the existence or absence of equality of opportunity or treatment between the groups of people specified in the right-hand column of that table in relation to each category of personal data, with a view to enabling such equality to be promoted or maintained:

Category of personal data	**Groups of people (in relation to a category of personal data)**
Personal data revealing racial or ethnic origin	People of different racial or ethnic origin
Personal data revealing religious or philosophical beliefs	People holding different religious or philosophical beliefs
Health data	People with different states of health
Personal data concerning an individual's sexual orientation	People of different sexual orientation

(b) Processing does not satisfy the condition in subparagraph (a) if it is carried out–

(i) in order to make a decision, or facilitate or allow a decision to be made, with respect to a particular data subject, or

(ii) in such a way that substantial damage is, or is likely to be, caused to any data subject.

(c) Processing does not satisfy the condition in subparagraph (a) if—

(i) a data subject has given notice in writing to the controller requiring the controller not to process the personal data, and has not given notice in writing withdrawing that requirement,

(ii) the notice gave the controller a reasonable period in which to stop processing such data, and

(iii) that period has ended.

17. 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.

Part III

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

19. The processing is necessary to protect the vital interests of the data subject or any other individual who is a third party, and –

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

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

SCHEDULE 3

INFORMATION TO BE GIVEN TO DATA SUBJECTS

Sections 12(2)(a), 13(1) and 15(1)(b)

1. The identity and contact details of the controller and, where applicable, any controller's representative.

2. The contact details of the data protection officer, where applicable.

3. Whether any of the personal data is special category data.

4. If any of the personal data has not been collected from the data subject by either of the controller or a processor acting on the controller's behalf –

(a) the source of the personal data, and

(b) if applicable, whether the personal data was obtained from a publicly available source.

5. The purposes and the legal basis of the processing.

6. Where the lawfulness of processing is based on the processing being necessary for the legitimate interests of the controller or a third party, the legitimate interests concerned.

7. The recipients or categories of recipients of the personal data, if any.

8. If the controller intends to transfer the personal data to a recipient in an authorised jurisdiction, other than a Member State of the European Union, a statement of which of the following applies to that authorised jurisdiction –

(a) an adequacy decision is in force in respect of the authorised jurisdiction, or

(b) the authorised jurisdiction is a designated jurisdiction.

9. If the controller intends to transfer the personal data to a recipient in an unauthorised jurisdiction, reference to the appropriate or suitable safeguards applying to the transfer and the means to obtain a copy of them or where they have been published or otherwise made available.

10. 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.

11. The data subject rights under sections 14 to 24.

12. Where the lawfulness of processing is based on the consent (explicit or otherwise) of the data subject, the existence of the right to withdraw consent at any time (without affecting the lawfulness of processing based on consent before its withdrawal).

13. The right to complain to the Authority under section 67, and the rights of appeal under sections 82 and 83.

14. Whether any decision would be made based on automated processing of the personal data, and in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

SCHEDULE 4

REGISTRATION OF BAILIWICK CONTROLLERS AND PROCESSORS

Sections 39 and 111(1)

1. Applications for registration.

(1) Any person established in the Bailiwick may apply to the Authority for registration as a controller or processor.

(2) An application –

(a) must be made in a form and manner required by the Authority or prescribed,

(b) must include the prescribed fee, and

(c) must include any information required by the Authority or prescribed.

2. Registration by the Authority.

Upon receipt of an application made in accordance with paragraph 1, the Authority must register the applicant as a controller or (as the case may be) processor.

3. Public register to be kept.

The Authority must –

(a) maintain a register of controllers and processors in any form and manner it considers appropriate, and

(b) publish any prescribed information on the register.

SCHEDULE 5

MATTERS TO BE SPECIFIED IN BINDING CORPORATE RULES

Section 58(c)

The following matters must to be specified in binding corporate rules in order for the Authority to approve those rules under section 58 for a group of undertakings or a group of enterprises engaged jointly in a business –

1. The structure and contact details of the group and each of its members.

2. The data transfers or set of transfers, including the categories of personal data, the category of processing and its purposes, the categories of data subjects affected and the identification of the unauthorised jurisdiction in question.

3. The legally binding nature of those rules, both internally and externally.

4. The application of the data protection principles, including the legal basis for processing (including processing of special category data) for the purposes of the data protection principle relating to lawfulness, fairness and transparency.

5. How the group members intend to comply with their duties under sections 31 and 41 and, in respect of onward transfers to bodies not bound by the binding corporate rules, section 55.

6. The data subject rights under sections 14 to 24, and how these rights may be exercised; the right to make a complaint under section 67; the rights of appeal under sections 82 and 83; the right to bring an action under section 79; and

how to obtain redress and, where appropriate, compensation for breach of the binding corporate rules.

7. The acceptance by the controller, processor or recipient of personal data of liability for any breaches of the binding corporate rules, subject to exemption from such liability only to the extent that the controller, processor or recipient concerned proves that it is not responsible for the event giving rise to the breach.

8. How the information on the binding corporate rules, in particular on the matters specified in paragraphs 4, 5, 6 and 7, is to be provided to the data subjects in addition to any other matters required to be notified to the data subject under this Law.

9. The tasks of –

(a) any data protection officer designated in relation to the group, or

(b) any other person in charge of monitoring compliance with the binding corporate rules within the group, as well as monitoring, training and complaint-handling.

10. The applicable complaint procedures.

11. The mechanisms within the group for verifying compliance with the binding corporate rules, including –

(a) data protection audits,

(b) mechanisms to ensure that corrective actions are taken where required to protect the rights of data subjects,

(c) communicating the results of such audits or actions to an officer or other person mentioned in paragraph 9 and to the board of the controlling undertaking of the group, and

(d) making those results available to the Authority on request.

12. The mechanisms for reporting and recording changes to the rules and reporting those changes to the Authority.

13. The mechanism for cooperating with the Authority to ensure compliance by members of the group, including by making the results of audits or corrective actions mentioned in paragraph 11(a) or (b) available to the Authority on request.

14. The mechanisms for reporting to the Authority any duties imposed by law –

(a) to which a member of the group is subject in any unauthorised jurisdiction, and

(b) which are likely to have a substantial adverse effect on the safeguards for data protection rights provided by the binding corporate rules.

15. The appropriate data protection training to individuals having permanent or regular access to personal data.

SCHEDULE 6

THE DATA PROTECTION AUTHORITY

Sections 60(3) and 111(1)

1. Constitution of the Authority.

(1) The Authority comprises –

(a) the Chairman,

(b) no fewer than four and no more than eight other voting members, with the exact number being determined by the Committee, and

(c) the Commissioner, as an *ex officio* and non-voting member.

(2) Subject to paragraph 2(5), the Chairman and the other voting members must be appointed by resolution of the States of Deliberation from individuals nominated by the Committee.

(3) In determining who to nominate for appointment, the Committee must have particular regard to the need to ensure that voting members of the Authority–

(a) have the qualifications, experience and skills necessary to exercise and perform the functions of a member, in particular relating to the protection of personal data,

(b) have a strong sense of integrity, and

(c) are able to maintain confidentiality.

(4) Before nominating an individual for appointment, the Committee may require the individual to provide, and to authorise the Committee to obtain, any information and references that the Committee reasonably requires to ascertain that individual's suitability for appointment as a voting member.

(5) Each voting member is to be appointed for a term of five years or any shorter period that the Committee thinks fit in a particular case.

(6) Each voting member may be reappointed in accordance with this paragraph, but must not be appointed as a voting member for more than three terms in aggregate (whether consecutive or not).

(7) An individual is ineligible to be a voting member if the individual –

(a) is now, or has ever been in the preceding 12 months, a member of the States of Deliberation, the States of Alderney or the Chief Pleas of Sark,

(b) is a person employed, whether on a full-time or part-time basis, by the States,

(c) is otherwise under the direction and control of the States, or

(d) is engaged in any employment, occupation (whether gainful or not) or business, or receives any benefits, that is incompatible with the functions of a member of the Authority.

2. <u>Removal or resignation of voting members</u>.

(1) The States of Deliberation may by Resolution remove a voting member from office before the expiration of the voting member's term of office only if the States of Deliberation is satisfied, based on a report and recommendation submitted by the Committee, that the voting member –

(a) is guilty of serious misconduct,

(b) has been convicted of a criminal offence,

(c) is bankrupt,

(d) is incapacitated by physical or mental illness,

(e) is otherwise unable or unfit to perform the voting member's duties, or

(f) is ineligible to be a voting member under paragraph 1(7).

(2) The Committee must not recommend a voting member to be removed from office on the ground specified in subparagraph (1)(a) unless a panel consisting of three or more individuals (none of whom is a member of the States of Deliberation, the Committee or the Authority) appointed by the Committee determines the voting member to be guilty of serious misconduct.

(3) A panel convened under subparagraph (2) may determine and adopt its own procedures to determine whether or not the voting member is guilty of serious misconduct.

(4) Any voting member may resign from office at any time by giving written notice to the Committee.

(5) If the individual who is the Chairman resigns from the Chairman's office, but not from office as a voting member of the Authority –

(a) this in itself does not affect that individual's continuance in office as a voting member,

(b) the Authority must elect another voting member to act as Chairman for the remainder of that member's term of office as a voting member, and

(c) the Committee must notify the States of that election at the next available sitting of the States.

3. <u>Emoluments and expenses of voting members</u>.

Each voting member of the Authority must be paid the fees, allowances and other emoluments and expenses determined by the Committee in consultation with the Authority; the Committee must publish those fees, allowances and other emoluments and expenses.

4. <u>Appointment of staff</u>.

(1) The Authority may appoint employees on terms and conditions it thinks fit for the exercise of its functions.

(2) The Authority may establish and maintain such schemes or make such other arrangements as it thinks fit for the payment of pensions and other benefits in respect of its employees.

(3) The Authority may take any steps it considers necessary and reasonable to protect and indemnify its current and former members and employees

against any costs, claims, liabilities and proceedings arising from or in consequence of anything done or omitted to be done in the discharge or purported discharge by them of their functions as members or (as the case may be) employees of the Authority.

(4) This paragraph is subject to paragraph 5.

5. <u>The Commissioner</u>.

(1) The Authority must appoint a Commissioner.

(2) The Commissioner –

(a) is the chief executive and an employee of the Authority,

(b) is responsible for managing the other employees of the Authority,

(c) is in charge of the day-to-day operations of the Authority, and

(d) has any other function conferred or imposed on the Commissioner by this Law or any other enactment.

(3) Subject to subparagraphs (4) to (8), the Commissioner holds office subject to terms and conditions determined by the Authority, for example regarding salary, allowances and other emoluments, expenses, and resignation.

(4) The Commissioner holds office for –

(a) a term of five years, or

(b) any shorter term specified in the terms and conditions of the Commissioner's appointment.

(5) The Commissioner may be reappointed by the Authority.

(6) The Authority may remove the Commissioner from office before the expiration of the Commissioner's term of office only if the Authority is satisfied that the Commissioner –

(a) is guilty of serious misconduct, based on a determination made by a panel convened by the Authority in consultation with the Committee and consisting of three or more individuals, none of whom is a member of the Authority or the Committee,

(b) has been convicted of a criminal offence,

(c) is bankrupt,

(d) is incapacitated by physical or mental illness, or

(e) is otherwise unable or unfit to perform the Commissioner's duties.

(7) A panel convened under subparagraph (6)(a) may determine and adopt its own procedures to determine whether or not the Commissioner is guilty of serious misconduct.

(8) Except with the approval of the Authority, the Commissioner must not engage in any other employment, occupation (whether gainful or not) or business, or receive any benefits other than the salary, allowances and other emoluments and expenses awarded by the Authority.

6. Commissioner may discharge Authority's functions (other than a reserved function).

(1) Subject to any policies, procedures and specific directions issued by the Authority, the Commissioner may exercise or perform, on behalf of the Authority and in its name, any function of the Authority under this Law other than a reserved function.

(2) A function exercised or performed by the Commissioner under subparagraph (1) is deemed for all purposes to have been exercised or performed by the Authority.

(3) Nothing in subparagraph (1) or (2) prevents the Authority from exercising or performing the function concerned.

7. Other resources.

The Authority may procure any accommodation, equipment, services or facilities it reasonably requires for the proper and effectual discharge of its functions.

8. Meetings.

(1) The Authority must meet –

(a) at least once every two months, or

(b) less frequently if resolved by the Authority, but no fewer than four times a year.

(2) If the Authority resolves to meet less frequently than once every two months, it must record the reason in its resolution.

(3) The person who presides at meetings is –

(a) the Chairman, if the Chairman is present, or

(b) if the Chairman is not present, the person elected to chair the meeting by, and from among, the other voting members present.

(4) At a meeting –

(a) a quorum is constituted by the nearest whole number of voting members above one half of the number of voting members for the time being in office,

(b) decisions are made by a majority vote,

(c) the Commissioner has no vote, but may participate in the Authority's proceedings,

(d) each voting member other than the person presiding has one vote, and

(e) the person presiding has no original vote, but in the event of equality in the votes of the other voting members present, the person presiding must exercise a casting vote.

9. Disclosure of interest.

(1) A voting member who has any direct or indirect personal interest in the outcome of the deliberations of the Authority in relation to any matter must disclose the nature of the interest at a meeting of the Authority and the disclosure must be recorded in the minutes of the Authority.

(2) For the purposes of this paragraph, a general notice given by a voting member to the effect that the voting member is a member, director or other office-holder, of any specified legal entity and is to be regarded as interested in any matter concerning that legal entity is a sufficient disclosure in relation to any such matter.

(3) A voting member need not attend in person at a meeting of the Authority in order to make any disclosure required under this paragraph if the voting member makes disclosure by a notice in writing delivered to the Chairman and that notice is brought to the attention of every meeting of the Authority at which deliberations of the kind mentioned in subparagraph (1) are to take place and before those deliberations commence.

10. <u>Transaction of business without meeting.</u>

The Authority may, if it thinks fit, transact any business by the circulation of papers to all members, and a resolution in writing approved in writing by a majority of its voting members is as valid and effectual as if passed at a meeting by the votes of the members approving the resolution.

11. <u>Records and minutes</u>.

The Authority must keep proper minutes of its proceedings, including records of any business transacted as permitted by paragraph 10.

12. <u>Financial and accounting provisions</u>.

(1) All expenditures of the Authority, including the fees, allowances and other emoluments and expenses of its members, must be paid from –

(a) any levies, fees, charges or other monies (other than administrative fines) paid to or received by the Authority under this Law, and

(b) where those monies are insufficient or unlikely to be sufficient to enable the Authority to properly and effectually discharge its

functions under this Law, an amount allocated by the States of Guernsey from its general revenue account (including from the proceeds of administrative fines).

(2) Where subparagraph (1)(b) requires the States of Guernsey to allocate an amount from its general revenue account to the Authority, the amount so allocated must be sufficient to enable the Authority to properly and effectually discharge its functions under this Law.

(3) The Authority must not borrow any money except with the prior consent of the States of Guernsey Policy & Resources Committee.

(4) The Authority must maintain proper financial accounts and proper records in relation to those accounts.

(5) The financial accounts of the Authority must be audited annually by auditors approved by the States of Guernsey Policy & Resources Committee.

(6) As soon as practicable after the end of each calendar year, the Authority must submit to the States of Guernsey Committee for Home Affairs a report containing –

(a) a statement of its financial accounts (giving a true and fair view of the state of affairs of the Authority),

(b) the auditor's report following the audit under subparagraph (5), and

(c) an annual report in accordance with paragraph 13.

(7) The States of Guernsey Committee for Home Affairs must in turn submit that report to the States of Deliberation.

13. <u>Annual report</u>.

An annual report of the Authority must include –

(a) a summary of the Authority's activities during the calendar year to which the report relates, including –

(i) the number of data protection complaints received,

(ii) the number of investigations and inquiries conducted by the Authority,

(iii) the number of investigations and inquiries resulting in a determination that an operative provision has been or is likely to be breached,

(iv) an anonymised summary of any sanctions imposed by the Authority under section 73, and

(v) where practicable and useful to promote the awareness of controllers, processors and the public, anonymised examples of data protection complaints and the outcome of the Authority's investigations into those, and

(b) the Authority's observations on whether the object of this Law is being attained, and if not, any amendment to this Law required to be made or any other actions required to be taken in order to better meet that object, and

(c) any other information required by the Committee or by Resolution of the States of Deliberation.

14. <u>Delegation of functions by the Authority.</u>

(1) The Authority may in writing delegate –

(a) any of its functions, other than a reserved function, to any employee of the Authority, and

(b) any of its functions to a committee comprising any number of voting members specified by the Authority.

(2) A function delegated under subparagraph (1) may be exercised or performed by the employee or committee concerned in accordance with the delegation and, when so exercised or performed, is deemed to have been exercised or performed by the Authority.

(3) A delegation under subparagraph (1) –

(a) does not prevent the Authority from exercising or performing the delegated function, and

(b) may be varied or revoked at will by the Authority.

(4) Nothing in this paragraph authorises –

(a) the Authority to delegate the power of delegation conferred by subparagraph (1) to any person, or

(b) an employee or committee to whom a function is delegated under subparagraph (1) to sub-delegate the function to any person.

(5) For the avoidance of doubt, section 4 of the Public Functions (Transfer and Performance) (Bailiwick of Guernsey) Law, 1991[ff] applies neither –

(a) to the Authority and its functions under this Law, nor

(b) to the Commissioner and the Commissioner's functions under this Law.

15. Delegation by the Commissioner.

(1) The Commissioner may in writing delegate to any other employee of the Authority any of the Commissioner's functions under this Law, including the Commissioner's power under paragraph 6 to exercise or perform, on behalf of the Authority and in its name, any function of the Authority under this Law other than a reserved function.

(2) A function delegated by the Commissioner under subparagraph (1) may be exercised or performed by the employee concerned in accordance with the delegation and, when so exercised or performed, is deemed to have been exercised or performed by the Commissioner.

(3) A delegation under subparagraph (1) –

(a) does not prevent the Commissioner from exercising or performing the delegated function, and

---

ff Ordres en Conseil Vol. XXXIII, p. 478.

(b) may be varied or revoked at will by the Commissioner.

(4) Nothing in this paragraph authorises –

(a) the Commissioner to delegate the power of delegation conferred by subparagraph (1) to any person, or

(b) an employee to whom a function is delegated under subparagraph (1) to sub-delegate the function to any person.

16. Residual power to regulate procedure.

Subject to the provisions of this Schedule, the Authority may regulate its own procedure.

17. Validity of proceedings.

The validity of any proceedings of the Authority is unaffected by –

(a) any vacancy in its membership,

(b) any defect in the appointment or election of any member,

(c) any ineligibility of an individual to be a voting member, or

(d) any lack of qualification of an individual to act as a member.

18. Authentication of the seal.

The application of the common seal of the Authority is to be authenticated by the signature of the Chairman, the Commissioner or another person authorised for this purpose.

19. Presumption of authenticity.

Unless the contrary is shown –

(a) any document purporting to be issued by the Authority or the Commissioner must be regarded as issued by the Authority or (as the case may be) Commissioner, and

(b) any document purporting to be signed by or on behalf of the Authority or the Commissioner must be regarded as signed by or on behalf of the Authority or (as the case may be) Commissioner.

20. Interpretation.

In this Schedule, "**reserved function**" means –

(a) the issuing of a public statement under section 64,

(b) the making of an order to pay an administrative fine under sections 73(2)(g) and 74,

(c) the making of the annual report required by paragraph 13, or

(d) any other function specified by the Authority by written notice given to the Commissioner.

SCHEDULE 7

GENERAL POWERS OF THE AUTHORITY

Sections 37(3)(b), 70, 88(3) and 111(1)

1. Power to require information.

(1) The Authority may by giving written notice to any controller or processor require the person concerned to give the Authority any information the Authority considers necessary for a purpose specified in subparagraph (2).

(2) The purposes referred to in subparagraph (1) are –

(a) to determine whether or not to investigate a complaint, conduct an inquiry, or exercise or perform any other function under this Law, in any particular circumstances,

(b) for the conduct of an investigation or inquiry,

(c) to make any determination under this Law,

(d) for the exercise or performance of any other function of the Authority under this Law.

(3) An information notice must include –

(a) a statement of the purpose in subparagraph (2) for which the notice is issued,

(b) a description of the information required by the Authority,

(c) a statement of the Authority's reasons for requiring that information in relation to the purpose for which the notice is issued,

(d) a statement of the form and manner in which, and the period within which ("**compliance period**"), the person concerned must give that information to the Authority, and

(e) the issue date.

(4) A compliance period must not be shorter than 28 days beginning the day after the issue date.

(5) Despite subparagraph (4), the Authority may specify a compliance period shorter than 28 days but not shorter than 7 days beginning the day after the issue date, but in this case the Authority must include in the notice a statement of its reasons for specifying that shorter period.

(6) The Authority may withdraw or amend an information notice by giving written notice to the person concerned.

(7) Nothing in this paragraph requires the person concerned to give the Authority any privileged items.

(8) In this paragraph –

"**information notice**" means the notice given under subparagraph (1), and

"**issue date**" means the date on which the information notice was issued.

2. <u>Issue of warrants.</u>

(1) If the Bailiff is satisfied by information on oath supplied by an authorised officer that there are reasonable grounds for suspecting that –

(a) either –

(i) a controller or processor is breaching, has breached or is likely to breach an operative provision, or

(ii) an offence under this Law is being or was committed, and

(b) there is material on those premises (other than privileged items) which is likely to be of substantial value (whether by itself or together with other material) to establishing the breach, likely breach or offence in question,

the Bailiff may, subject to subparagraph (2), issue a warrant under this paragraph.

(2) The Bailiff must not issue a warrant under subparagraph (1) unless the Bailiff is satisfied –

(a) that an authorised officer has given seven days' notice in writing to the occupier of the premises in question demanding access to the premises, and

(b) that either –

(i) access was demanded at a reasonable hour and was unreasonably refused, or

(ii) although entry to the premises was granted, the occupier unreasonably refused to comply with a request made by an authorised officer –

(a) to permit the authorised officer to do anything which the officer could have done under paragraph 4(1)(a) to (k) if that officer were executing a warrant, or

(b) for the occupier to do anything which the officer could have required the occupier to do under paragraph 4(1)(a) to (k) if that officer were executing a warrant, and

(c) that the occupier, has, after the refusal, been notified by an authorised officer of the application for the warrant and has had an opportunity of being heard by the Bailiff on the question whether or not it should be issued.

(3) Subparagraph (2) does not apply if the Bailiff is satisfied that –

(a) the case is one of urgency,

(b) compliance with that subparagraph would defeat the object of the entry, or

(c) compliance with that subparagraph is impracticable, for example if the premises are unoccupied or, despite reasonable efforts, the occupier cannot be identified or contacted.

(4) A warrant must –

(a) state the name of the authorised officer who applied for it, the date on which it is issued, and the premises to be searched,

(b) state that it is issued under paragraph 2 of this Schedule, and

(c) so far as practicable, identify the things to be sought.

(5) The court must ensure that two copies are made of each warrant, and that those copies are clearly certified as copies.

3. <u>Procedure for obtaining a warrant</u>.

(1) An application for a warrant –

(a) must be made and supported by information in writing, and

(b) must state –

(i) that the warrant would be issued under paragraph 2 of this Schedule,

(ii) the ground on which the authorised officer makes the application,

(iii) the premises which it is desired to enter and search, and

(iv) so far as is practicable, the things to be sought.

(2) The authorised officer making the application must answer on oath any question that the officer is asked by the Bailiff.

4. <u>Execution of warrants</u>.

(1) An authorised officer executing a warrant issued under paragraph 2 may at any time within one month of the date of the warrant enter the premises specified in the warrant and exercise all or any of the following powers –

(a) search those premises and examine, test, open, inspect or operate anything at those premises,

(b) photograph, film or otherwise record anything at those premises,

(c) require any person at those premises to produce any processing equipment,

(d) require any person at those premises to permit the authorised officer to observe the processing of personal data that takes place at those premises,

(e) require any person at those premises to give the authorised officer any information, which may include (without limiting the generality of this subparagraph) –

(i) information relating to those premises,

(ii) information relating to the ownership, identity, origin or any other matter relating to any processing equipment,

(iii) information relating to the processing of personal data, or

(iv) the name and address of any controller, processor or other person involved in the processing of personal data,

(f) take copies of or extracts from any information (including, in the case of information in a non-legible form, a copy of or an extract from that information in a legible form),

(g) if anything at the premises cannot be conveniently removed, secure it against interference,

(h) seize any equipment, device, information or other thing, which is at the premises and detain it for as long as the authorised officer considers necessary,

(i) inspect any information (in whatever form they are held) relating to the business of a controller or processor,

(j) where any such information is stored in electronic form –

(i) inspect and check the operation of any equipment, device or other thing which is or has been in use in connection with that information,

(ii) require any person having charge of, or otherwise concerned with the operation of, the equipment, device, or other thing to provide the authorised officer any facilities or assistance that

the officer considers necessary or expedient to obtain access to or make legible any information kept in or by that equipment, device or other thing, or

(iii) require that information to be produced in a form in which that information may be taken away, and

(k) require any person at the premises to provide the authorised officer any facilities or assistance that the officer considers necessary or expedient in relation to the exercise of any of the officer's powers under items (a) to (j) of this subparagraph.

(2) Nothing in subparagraph (1)(a) to (k) applies to privileged items.

(3) An authorised officer executing a warrant –

(a) must be accompanied by a police officer,

(b) must do so at a reasonable hour, and

(c) may use reasonable force if necessary.

(4) The authorised officer need not comply with subparagraph (3)(b) if it appears to that officer that compliance with the provision would defeat the object of the entry.

5. <u>Safeguards for warranted entry, search, etc.</u>

(1) An authorised officer executing a warrant to enter any premises must, if the owner or occupier of those premises is present –

(a) identify himself or herself to the owner or occupier, and

(b) produce the warrant to the owner or occupier.

(2) If the owner or occupier is not present at the time the authorised officer leaves those premises, the officer –

(a) must leave the premises as effectively secured against trespassers as the officer found them, and

(b) must leave in a prominent place on those premises written notice that those premises have been entered and searched under paragraph 4 of

this Schedule, including the officer's name and an address at which that officer may be contacted and a copy of the warrant.

(3) An authorised officer who seizes anything from the premises must leave with the owner or occupier of the premises (if present) or leave on the premises (if the owner or occupier is not present), a statement stating –

(a) particulars of what has been seized, and

(b) that the officer has seized it.

6. <u>Endorsement, return and inspection of warrants.</u>

(1) An authorised officer executing a warrant must, after executing it, make an endorsement on it stating –

(a) whether the things sought were found, and

(b) whether any things, other than the things which were sought, were seized.

(2) A warrant which has been executed, or which has not been executed within the time allowed for its execution, must be returned to the court.

(3) The court must retain a returned warrant for 12 months beginning on the date of its return.

(4) If, during the period for which a warrant is to be retained under subparagraph (3), the owner or occupier of the premises to which it relates asks to inspect it, the court must allow that owner or occupier to do so.

7. <u>Persons exercising powers may bring other persons and things.</u>

(1) An authorised officer entering any premises under paragraph 4 may bring onto the premises any person, equipment, device or other thing to assist the officer in the exercise of the officer's powers under any provision of this Schedule.

(2) For the avoidance of doubt, a person brought onto the premises by an authorised officer under subparagraph (1) may exercise any power conferred

on an authorised officer by any provision of this Schedule under the direction and supervision of an authorised officer.

8. Detention, storage and disposal of seized property.

(1) Seized property may be stored by the Authority in any manner and place it sees fit until disposed of in accordance with this paragraph.

(2) Any person who appears to the Authority to be the owner of the property must be given reasonable access to that property.

(3) Any seized property must be returned to its owner within 40 days of its seizure, except –

(a) where the owner of the property has consented to the continued detention or storage, or to the sale, destruction or other disposal, of the property,

(b) where an authorised officer believes on reasonable grounds that the property is required –

(i) for the conduct of any investigation or inquiry, or

(ii) as evidence in any proceedings for an offence under this Law, or

(c) where a competent court has ordered otherwise.

(4) Unless a competent court orders otherwise, any seized property retained under subparagraph (3)(b) must be returned to its owner as soon as practicable after the latest of the following –

(a) the completion of the investigation, inquiry or other proceedings mentioned in that subparagraph,

(b) the completion of any other proceedings (including appeals) arising from those proceedings, and

(c) the expiry of any period for appeal arising from those proceedings.

9. Power to conduct or require data protection audits

(1) This paragraph applies where the Authority believes on reasonable grounds that a controller or processor –

(a) has failed to comply with a requirement made by the Authority or an authorised officer under any provision of this Schedule, or

(b) has otherwise failed to cooperate with the Authority in the exercise or performance of any of the Authority's functions under this Law.

(2) Where this paragraph applies, the Authority may –

(a) conduct a data protection audit of any part of the operations of the controller or processor, or

(b) require the controller or processor to appoint a person approved by the Authority to –

(i) conduct a data protection audit of any part of the operations of the controller or processor, at the expense of the controller or processor, and

(ii) report the findings of the audit to the Authority, at the expense of the controller or processor.

(3) The Authority must specify the terms of reference of any audit to be conducted or required under subparagraph (2).

10. Interpretation of this Schedule.

In this Schedule –

"**the Bailiff**" means –

(a) in relation to a warrant or an application for a warrant to be executed in Alderney, the Chairman of the Court of Alderney or, if the Chairman is unavailable, a Jurat of the Court of Alderney,

(b) in relation to a warrant or an application for a warrant to be executed in Sark, the Seneschal, and

(c) in any other case, the Bailiff, Deputy Bailiff, Judge of the Royal Court, Lieutenant-Bailiff or Juge Délégué,

"**the court**", in relation to a warrant issued by –

(a) the Chairman of the Court of Alderney or a Jurat of the Court of Alderney, means the Court of Alderney,

(b) the Seneschal, means the Court of the Seneschal, and

(c) the Bailiff, Deputy Bailiff, Judge of the Royal Court, Lieutenant-Bailiff or Juge Délégué, means the Royal Court,

"**information**", for the avoidance of doubt, includes any personal data processed by a processor or in the context of a controller, and

"**seized property**" means any property seized or detained by an authorised officer in the exercise of a power conferred by this schedule.

SCHEDULE 8

GENERAL EXCEPTIONS AND EXEMPTIONS

Section 96

Part I

Exemptions from Part III of this Law based on nature of personal data

1. Confidential references given by the controller.

A reference given by the controller is exempt from a provision of Part III if given or proposed to be given in confidence for the purpose of –

(a) the education, training or employment, or prospective education, training or employment, of the data subject,

(b) the appointment, or prospective appointment, of the data subject to any office, or

(c) the provision, or prospective provision, by the data subject of any service.

2. Judicial appointments and honours.

Personal data is exempt from a provision of Part III if processed solely for the purpose of –

(a) assessing any person's suitability for judicial office or the office of Queen' s Counsel, or

(b) the conferring by the Crown of any honour or dignity.

3. Examination data.

Personal data is exempt from a provision of Part III if recorded by any candidate during an examination.

4. **Marking data**.

(1) This paragraph applies where a request under Part III of this Law is made for or in relation to marking data.

(2) In subparagraph (1), "**marking data**" means marks or other information processed in the context of the controller –

(a) for the purpose of determining the examination results of a candidate,

(b) for the purpose of enabling such a determination, or

(c) in consequence of such a determination.

(3) Where this paragraph applies, in the application of section 27 to the request, section 27(5) is substituted with the following subsection –

"(5) In this section –

"**the designated period**", in relation to a request, means –

(a) if the relevant day falls on or after the publication day, one month following the relevant day, but

(b) if the relevant day falls before the publication day, the period ending on the earlier of the following dates –

(i) the date that is five months following the relevant day, or

(ii) the date that is two months following the publication day,

"**the publication day**", in relation to any examination and examination candidate, means the day on which the results of the examination are first published or (if not published) when they are first made available or communicated to the candidate concerned,

"**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 necessary to confirm the identity of the requestor, and

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

5. Privileged items.

Privileged items are exempt from a provision of Part III.

Part II
Exemptions from designated provisions on grounds of prejudice

6. 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.

7. Management forecasting or planning.

(1) This paragraph applies to personal data processed for the purposes of management forecasting or management planning to assist the controller in the conduct of any business or other activity.

(2) Personal data to which this paragraph applies is exempt from a designated provision to the extent that the application of the provision to the data would be likely to prejudice the conduct of the business or other activity concerned.

8. Financial service data.

(1) Financial service data is exempt from a designated provision to the extent that either Condition A or Condition B is satisfied.

(2) Condition A is that –

(a) the application of the provision to the data would be likely to affect the price of any instrument, or

(b) the controller reasonably believes that to be the case.

(3) Condition B is that -

(a) the relevant person reasonably believes that the application of the provision to the personal data in question could affect a decision of any person—

(i) whether to deal in, subscribe for or issue any instrument, or

(ii) to act (or not to act) in a way likely to have an effect on a business activity (such as an effect on the industrial strategy of a person, the capital structure of an undertaking or the legal or beneficial ownership of a business or asset), and

(b) the application of the provision to that personal data would be likely to prejudice –

(i) the orderly functioning of financial markets or the efficient allocation of capital within the economy, or

(ii) any other important financial or economic interest of the Bailiwick.

(4) In this paragraph –

"**corporate finance service**" means a service consisting of –

(a) underwriting in respect of issues of, or the placing of issues of, any instrument,

(b) services relating to such underwriting, or

(c) advice to undertakings on capital structure, industrial strategy and related matters or advice or service relating to mergers or the purchase of undertakings,

"**financial service data**" means personal data that is processed for the purpose of, or in connection with, a corporate finance service provided by a relevant person,

"**instrument**" means any instrument listed in section C of Annex I to Directive 2004/39/EC[gg] of the European Parliament and of the Council of 21 April 2004 on markets in financial instruments, and a reference to "**any instrument**" includes a reference to an instrument not yet in existence but which is to be or may be created,

"**price**" includes value,

"**relevant person**" means –

(a) any person who holds a licence to carry on controlled investment business under Part I of the Protection of Investors (Bailiwick of Guernsey) Law, 1987[hh] or is an exempted person under Part IV of that Law,

(b) any person who, by reason of a permission under Part 4A of the Financial Services and Markets Act 2000[ii] ("**that Act**"), is able to carry on a corporate finance service without contravening the general prohibition within the meaning of section 19 of that Act ("**that general prohibition**"),

(c) an EEA firm of the kind mentioned in paragraph 5(a) or (b) of Schedule 3 to that Act which has qualified for authorisation

---

gg O.J. L 145 of 30.4.2004, p. 1.

hh Ordres en Conseil Vol. XXX, p. 281; as amended by Ordres en Conseil Vol. XXX, p. 243; Vol. XXXV(1), p. 271; Vol. XXXVI, p. 264; Vol. XXXVII, p. 24; Order in Council No. XVII of 2002; Nos. XV and XXXII of 2003; No. XVIII of 2008; Nos. XIII and XX of 2010; Recueil d'Ordonnances Tome XXIV, p. 324; Tome XXVI, p. 333; Tome XXVIII, p. 87; Ordinance No. XXXIII of 2003; No. XXXI of 2008; No. VII of 2009; Nos. XII, XX and XXXIX of 2015; Nos. II, IX and XXIX of 2016; the Transfer of Funds (Guernsey) Ordinance, 2017; Alderney Ordinance No. III of 2017; Sark Ordinance No. X of 2017; G.S.I. No. 83 of 2010; and G.S.I. No. 50 of 2017.

ii An Act of Parliament (Chapter 8 of 2000).

under paragraph 12 of that schedule, and may lawfully carry on a corporate finance service,

(d) a person who is exempt from that general prohibition in respect of any corporate finance service—

(i) as a result of an exemption order made under section 38(1) of that Act, or

(ii) by reason of section 39(1) of that Act (appointed representatives),

(e) any person, not falling within paragraph (b), (c) or (d) who may lawfully carry on a corporate finance service in the United Kingdom,

(f) any person who, in the course of employment, provides to their employer a service falling within paragraph (b) or (c) of the definition of "**corporate finance service**", or

(g) any partner who provides to other partners in the partnership a service falling within paragraph (b) or (c) of the definition of "**corporate finance service**".

9. **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.

10. **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 this Law,

(b) perjury, or

(c) perverting the course of justice.

11. 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.

12. Public information.

(1) Public information is exempt from a 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.

13. Historical or scientific information.

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.

14. **Tax and crime information.**

(1) Tax information and crime information is exempt from a designated provision to the extent that the application of the provision to the information would be likely to prejudice the purpose for which that information is processed.

(2) In this paragraph,

"**crime information**" means personal data processed for a law enforcement purpose, and

"**tax information**" –

(a) means personal data processed for the purpose of the assessment or collection 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, and

(b) for the avoidance of doubt, includes a classification applied to the data subject as part of a system of risk assessment which is operated by a public authority for that purpose.

15. **Protective functions**.

(1) Personal data processed by any person for the exercise or performance of any protective function 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 proper discharge of that function.

(2) In subparagraph (1), "**protective function**" means any function conferred or imposed by law on the person for any of these purposes –

(a) to protect the public or any section of it against –

(i) dishonesty, malpractice or other seriously improper conduct,

(ii) unfitness or incompetence,

(iii) the conduct of a person against whom a declaration of insolvency has been or is made, or whose affairs have been, or are, in a state of désastre,

(iv) misconduct or mismanagement in the administration of any body or association,

(v) failure in services provided by any person,

(b) to protect the property of non-profit organisations or charities from loss or misapplication,

(c) to recover the property of non-profit organisations or charities,

(d) to secure the health, safety and welfare of persons at work,

(e) to protect persons other than persons at work against any risk to their health or safety arising out of or in connection with the actions of persons at work, or

(f) to protect the reputation and standing of the Bailiwick.

16. <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 (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.

Part III
Wider Exemptions in the Public Interest

17. Journalism, art, literature and academia.

(1) Personal data processed only for the purpose of journalism or an artistic, literary or academic purpose, is exempt from a provision of Part II, III, IV, VII, IX, X, XI or XII or section 43 of this Law to the extent that –

(a) the processing is undertaken with a view to the publication by any person of any journalistic, artistic, literary or academic material,

(b) the application of the provision to the personal data would be likely to prejudice the purpose concerned in connection with the publication of that material, and

(c) having particular regard to the importance of freedom of expression and information, the public interest in the publication of that material outweighs the significant interests of the data subject.

(2) For the avoidance of doubt, no power conferred by a provision of Part XI or XII of this Law may be exercised in relation to personal data which by virtue of subparagraph (1) is exempt from the provision concerned.

(3) The States of Deliberation may by Ordinance make such further provision as they consider necessary or expedient as to the balancing of the rights of data subjects and the public interest in freedom of expression and information in relation to the processing of personal data for a purpose mentioned in subparagraph (1).

(4) In subparagraph (1), "**freedom of expression and information**" means the right protected under article 10 of the European Convention on Human

Rights and Fundamental Freedoms as incorporated in the Human Rights (Bailiwick of Guernsey) Law, 2000.

18. Public security, etc.

(1) Personal data is exempt from any provision of Parts II to XII or XV of this Law 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 this 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 this 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.

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 paragraph (a).

Part IV
Interpretation of this Schedule

20. Interpretation.

In this Schedule –

"**a provision of Part III**" means –

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

(b) any provision of section 6 or any other section of this Law so far as the provision corresponds to a right or duty in Part III of this Law,

"**designated provision**" means –

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

(b) section 43, and

(c) any other provision of this Law so far as the provision corresponds to a right or duty in Part III of this Law or in section 43, and

"**examination**" includes any process for determining the knowledge, intelligence, skill or ability of a candidate by reference to the candidate's performance in any test, work or other activity, for any academic, professional or other purpose.

SCHEDULE 9

EXPRESSIONS WITH SPECIAL MEANINGS

Sections 110 and 111(1)

1. Identifiable individual.

An individual is identifiable from any information where the individual can be directly or indirectly identified from the information, including –

(a) by reference to a name or an identifier,

(b) by reference to one or more factors specific to the person's physical, physiological, genetic, mental, economic, cultural or social identity,

(c) where, despite pseudonymisation, that information is capable of being attributed to that individual by the use of additional information, or

(d) by any other means reasonably likely to be used, taking into account objective factors such as technological factors and the cost and amount of time required for identification in the light of the available technology at the time of processing.

2. Processing in the context of a controller or processor.

Personal data is processed in the context of a controller or processor if the personal data is processed –

(a) by or on behalf of the controller or processor, or

(b) otherwise in the course of or in connection with any activity of the controller or processor.

3. Necessary for a particular purpose or aim.

Whether or not the processing of personal data is necessary for any particular purpose or aim must be determined having regard to –

(a) whether or not processing of that personal data in the particular circumstances would be proportionate to the purpose or aim, having regard to the proportionality factors, and

(b) whether or not it is practicable in all the circumstances to achieve that purpose or aim without so processing the personal data.

4. <u>Proportionality factors</u>.

(1) The proportionality factors are –

(a) the nature of the personal data, including whether it is special category data,

(b) the data subject, including whether the data subject is a child,

(c) the context in which the personal data has been collected or otherwise processed, and in particular the relationship between the data subject and the controller,

(d) the reasonable expectations of the data subject in relation to the processing of that personal data,

(e) the possible consequences of the processing for data subjects,

(f) the interests at stake, and in particular any significant interests of the data subject or any other individual who is a third party,

(g) the existence of appropriate safeguards for the protection of the personal data or the protection of significant interests of data subjects,

(h) where disclosure of the personal data is or may be involved, the entities to which, and the purposes for which, the personal data is or may be disclosed,

(i) where disclosure of the personal data without consent of the data subject is or may be involved, whether the controller owes the data subject a duty of confidentiality, and

(j) where storage of the personal data is or may be involved, the period for which the personal data is or may be stored.

(2) A person weighing the proportionality factors in any case involving special category data must have particular regard to the importance of protecting special category data from processing where the data subject has not given explicit consent to the processing of the special category data.

5. <u>Processing for historical or scientific purpose</u>.

(1) Subject to subparagraphs (2) and (3), personal data is processed for a historical or scientific purpose, if it is processed for –

(a) the purpose of archiving in the public interest,

(b) a scientific or historical research purpose, or

(c) a statistical purpose.

(2) Personal data may be regarded as processed for a historical or scientific purpose even if the data is disclosed –

(a) to any person for research purposes only,

(b) to the data subject or a person acting on the data subject's behalf,

(c) at the request, or with the consent, of the data subject or a person acting on the data subject's behalf, or

(d) in circumstances in which the person making the disclosure has reasonable grounds for believing that the disclosure falls within item (a), (b) or (c) of this subparagraph.

(3) Personal data must not be regarded as processed for a historical or scientific purpose where the data is processed –

(a) in order to make a decision, or facilitate or allow a decision to be made, with respect to a particular data subject, or

(b) in such a way that substantial damage is, or is likely to be, caused to any data subject.

6. **<u>High risk to significant interests of data subjects</u>**.

(1) Subject to subparagraph (2), whether any processing of personal data is likely to pose a high risk to the significant interests of data subjects must be determined having regard to the nature, scope, context and purpose of the processing, having particular regard to whether a new technology, mechanism or procedure is used to process the personal data.

(2) Processing of personal data is deemed to be likely to pose a high risk to the significant interests of data subjects where it involves –

(a) a systematic and extensive evaluation of personal aspects relating to data subjects based on automated processing, and decisions are based on the evaluation that affect the significant interests of data subjects,

(b) large-scale processing of special category data,

(c) large-scale and systematic monitoring of a public place, or

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

7. **<u>Breach of an operative provision or duty</u>**.

(1) A controller or processor breaches an operative provision or a duty if –

(a) any processing of personal data in the context of the controller or processor fails to comply with or contravenes the operative provision, or as the case may be, the duty, or

(b) the controller or processor fails to comply with or contravenes the operative provision, or as the case may be, the duty.

(2) A controller or processor is likely to breach an operative provision if –

(a) any processing or related act or omission is likely to fail to comply with or contravene the operative provision, or

(b) the controller or processor is likely to fail to comply with or contravene the operative provision in connection with any processing or related act or omission.

(3) In subparagraph (2), "**processing or related act or omission**", in relation to any controller or processor, means –

(a) any proposed processing in the context of the controller or processor, or

(b) any intended act or intended omission of the controller or processor, in relation to any processing or proposed processing in the context of the controller or processor.

SCHEDULE 10

INDEX OF DEFINED EXPRESSIONS

Section 112

Each expression in the left-hand column of the table below is defined or given meaning by the corresponding provision in the right-hand column of this table.

Expression	**Provision of this Law**
A provision of Part III	Paragraph 20 of Schedule 8
That Act	Paragraph 8(4) of Schedule 8
Action	Section 78
Adequacy decision	Section 111(1)
Administrative fine	Section 111(1)
Administrative offence	Paragraph 16(2) of Schedule 8
Alderney person	Section 111(1)
Anonymised	Section 11(3)
Approved code	Section 111(1)
Approved mechanism	Section 111(1)
Authorised jurisdiction	Section 111(1)
Authorised officer	Section 111(1)
The authorised person	Section 35(3)
The authorising person	Section 35(3)
The Authority	Section 111(1)
Authority official	Section 111(1)

Expression	Provision of this Law
Automated processing	Section 24(5); section 111(1)
Automatic decision	Section 24(5)
The Bailiff	Paragraph 10 of Schedule 7
The Bailiwick	Section 111(1)
Bailiwick resident	Section 2(5)
Binding corporate rules	Section 111(1)
Biometric data	Section 111(1)
Body corporate	Section 111(1)
Breach (of operative provision or duty)	section 111(1); paragraph 7 of Schedule 9
Breach of duty	Section 78
Breach determination	Section 111(1)
Business	Section 111(1)
By law	Section 111(1)
By post	Section 102(2)(a)
Category	Section 111(1)
Chief Officer of Police	Paragraph 2(3) of Schedule 1
Child	Section 111(1)
Code	Section 52(7)
Code of conduct	Section 52(7)
The Commissioner	Section 111(1)
The Committee	Section 111(1)

Expression	Provision of this Law
Community provision	Section 111(1)
Comparable foreign enactment	Section 91(2)
Competent supervisory authority	Section 111(1)
Complainant	Section 81
Complaint	Section 111(1)
Compliance period	Paragraph 1(3)(d) of Schedule 7
Consent	Section 111(1)
Controller	Section 111(1)
Controller or processor	Section 78
Controller's representative	Section 111(1)
Controlling undertaking	Section 111(1)
Controller undertaking	Section 111(1)
The Convention	Section 111(1)
Corporate finance service	Paragraph 8(4) of Schedule 8
Country	Section 111(1)
The Court	Section 81; paragraph 10 of Schedule 7
Court A	Section 86(1)
Court A's proceedings	Section 86(1)
Court B	Section 86(1)
Court B's proceedings	Section 86(1)
Credit reference agency	Section 15(5)
Crime information	Paragraph 14(2) of Schedule 8

Expression	Provision of this Law
Criminal data	Section 111(1)
Damage	Section 111(1)
Data protection impact assessment	Section 111(1)
Data protection officer	Section 111(1)
Data protection organisation	Section 111(1)
Data protection principle	Section 111(1)
Data subject	Section 16(6); section 111(1)
Data subject right	Section 111(1)
Designated date	Section 45(7)
Designated jurisdiction	Section 111(1)
Designated official	Section 90(5)
The designated period	Section 27(5); paragraph 4(3) of Schedule 8
Designated provision	Paragraph 20 of Schedule 8
Designating entity	Section 49(3)
Document	Section 102(10); section 111(1)
Duty	Section 111(1)
Enactment	Section 107(4); section 111(1)
Enforcement order	Section 111(1)
Enterprise	Section 111(1)
Equipment	Section 111(1)
Established in the Bailiwick	Section 111(1)

Expression	Provision of this Law
Examination	Paragraph 20 of Schedule 8
Exemptable provision	Paragraph 18(1) of Schedule 8
Fairly (in relation to processing)	Section 8; section 111(1)
Filing system	Section 111(1)
Financial service data	Paragraph 8(4) of Schedule 8
The first controller	Section 14(1)(a)
Former Directive	Section 111(1)
Foundation	Section 111(1)
Foundation official	Section 111(1)
Freedom of expression and information	Paragraph 17(4) of Schedule 8
Function	Section 111(1)
Function that is of a public nature	Section 111(1)
Further controller or processor	Section 55(2)
The GDPR	Section 111(1)
General partner	Section 111(1)
Genetic data	Section 111(1)
That general prohibition	Paragraph 8(4) of Schedule 8
Group of undertakings	Section 111(1)
Guernsey person	Section 111(1)
Health	Section 111(1)
Health data	Section 111(1)
Health or social care purpose	Paragraph 10(b) of Schedule 2

Expression	Provision of this Law
Health professional	Section 111(1)
Health record	Section 98(2)
High risk	Section 111(1); paragraph 6 of Schedule 9
High-risk legislation	Section 46(3)
High-risk processing	Section 44(8)
Historical or scientific purpose	Section 111(1); paragraph 5 of Schedule 9
Identifiable	Section 111(1); paragraph 1 of Schedule 9
The identifiable person	Section 90(1)
Identifier	Section 111(1)
Implement	Section 106(3)
In the context of	Section 111(1); paragraph 2 of Schedule 9
In the context of employment	Section 105(3)
Individual	Section 111(1)
Information	Section 111(1); paragraph 10 of Schedule 7
Information notice	Section 111(1); paragraph 1(8) of Schedule 7
Information society service	Section 111(1)
The injured party	Section 79(2)
Inquiry	Section 111(1)
Instrument	Paragraph 8(4) of Schedule 8

Expression	Provision of this Law
International organisation	Section 111(1)
Investigation	Section 111(1)
Issue date	Paragraph 1(8) of Schedule 7
Joint controllers	Section 33(1)
This Law	Section 36(5) and (6); section 111(1)
Law Enforcement Directive	Section 111(1)
Law enforcement purpose	Section 111(1)
Lawfully (in relation to processing)	Section 7; section 111(1)
Legal proceedings	Section 111(1)
Likely to breach (operative provision or duty)	Section 111(1); paragraph 7 of Schedule 9
Limited partnership	Section 111(1)
Machine-readable format	Section 111(1)
Marking data	paragraph 4(2) of Schedule 8
Medical device	Paragraph 11(b) of Schedule 2
Medicinal product	Paragraph 11(b) of Schedule 2
Member	Section 111(1)
Monitoring body	Section 111(1)
Necessary	Section 111(1); paragraph 3 of Schedule 9
Negotiation record	Paragraph 9(2) of Schedule 8
Non-profit organisation	Section 111(1)
Offence	Paragraph 10(2) of Schedule 8

Expression	Provision of this Law
Official	Section 111(1)
Operative provision	Section 111(1)
Organisational measures	Section 111(1)
The other individual	Section 16(1)
Parental responsibility	Section 111(1)
Person	Section 111(1)
The person concerned	Section 111(1)
Personal data	Section 111(1)
Personal data breach	Section 111(1)
Police officer	Section 111(1)
Prejudice	Section 111(1)
Premises	Section 111(1)
Prescribed	Section 8(2); section 111(1)
Price	Paragraph 8(4) of Schedule 8
Primary processor	Section 36(1)
Privileged items	Section 111(1)
Processing	Section 111(1)
Processing equipment	Section 111(1)
Processing or related act or omission	Paragraph 7(3) of Schedule 9
Processor	Section 111(1)
Profiling	Section 111(1)
Progress	Section 111(1)

Expression	Provision of this Law
Proportionality factors	Section 111(1); paragraph 4 of Schedule 9
Protective function	Paragraph 15(2) of Schedule 8
Pseudonymisation	Section 111(1)
Public authority	Section 111(1)
Public committee	Section 111(1)
Public information	Paragraph 12(2) of Schedule 8
Public office	Section 111(1)
Public register	Section 111(1)
Public security	Section 111(1)
Publication	Section 111(1)
The publication day	Paragraph 4(3) of Schedule 8
Publish	Section 111(1)
(The) recipient	Section 111(1)
Register	Section 111(1)
Regulations	Section 111(1)
Regulatory purpose	Paragraph 16(2) of Schedule 8
The relevant day	Section 27(5); paragraph 4(3) of Schedule 8
Relevant employees	Section 50(1)(a)
Relevant person	Paragraph 8(4) of Schedule 8
Relevant personal data	Section 14(1)
Request	Section 26(3)

Expression	Provision of this Law
(The) requestor	Section 16(1); section 26(3)
Requirement	Section 88(3)
Reserved function	Paragraph 20 of Schedule 6
Restriction of processing	Section 111(1)
Royal Court	Section 111(1)
Safeguard data subject rights	Section 111(1)
Safeguards	Section 111(1)
Sanction	Section 111(1)
Sark person	Section 111(1)
Secondary processor	Section 36(1)
Seized property	Paragraph 10 of Schedule 7
Significant interests	Section 111(1)
Special category data	Section 111(1)
Standard data protection clauses	Section 111(1)
The statement concerned	Section 100(1)
The States	Section 111(1)
Statutory body	Section 111(1)
Subordinate legislation	Section 111(1)
Tax information	Paragraph 14(2) of Schedule 8
Third party	Section 111(1)
Transmitted	Section 102(2)(b)
Unauthorised jurisdiction	Section 111(1)

Expression	Provision of this Law
Undertaking	Section 111(1)
Use	Section 54(3)
Vital interests	Section 111(1)
Voting member	Section 111(1)
Working day	Section 102(10)