EXPLANATORY MEMORANDUM

The Data Protection (Bailiwick of Guernsey) Law, 2017

This Law replaces the current Data Protection (Bailiwick of Guernsey) Law, 2001 with provisions to implement the General Data Protection Regulation (Regulation (EU) 2016/679) and the Law Enforcement Directive (Directive (EU) 2016/680) of the European Parliament.

This 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 confers rights on data subjects (the living individuals to whom the personal data relates).

PART I

PRELIMINARY

Section 1 sets out the object of this Law. It is intended 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 the General Data Protection Regulation and the Law Enforcement Directive. It also makes other provisions considered appropriate in relation to the processing of personal data, including provisions to protect the significant interests of individuals in relation to their personal data.

Section 2 provides that this Law applies to processing of personal data by automated means or where the data is part of a filing system, and only where the processing is in the context of a controller or processor established in the Bailiwick or the personal data of a Bailiwick resident is processed in the context of the offering of goods or services to the resident or the monitoring of the resident's behaviour in the Bailiwick. Section 2 also gives effect to Schedule 1, which sets out the application of the Law to the Crown, public committees and the Police.

Section 3 states that the Law applies regardless where the processing takes place and has extra-territorial application, unless the context requires otherwise.

Section 4 exempts from this Law the processing of personal data by an individual solely for the purpose of the individual's personal, family or household affairs.

Section 5 directs that so far as it is possible, other enactments must be given effect in a way which is consistent with this Law. This means for example, that where other enactments impose duties or confer powers, these duties and powers must so far as possible be construed in a manner consistent with the provisions of this Law.

PART II

DUTIES AND PRINCIPLES OF PROCESSING

Section 6 requires the controller of personal data to comply or ensure compliance with the data protection principles in this section.

Section 7 provides that to be lawful, processing of special category data (sensitive data such as health data, racial or ethnic origin, or criminal convictions) must satisfy at least one condition in Part 2 or 3 of Schedule 2. Processing of other types of personal data will need to satisfy at least one condition in Part 1 or 2 of Schedule 2.

Section 8 provides that whether or not personal data is processed fairly must be determined having regard to the method by which it is obtained, that personal data is to be regarded as fairly obtained if it consists of information obtained from a person who is authorised or required to supply it by or under an enactment, and that processing of personal data containing identifiers prescribed by an Ordinance must be regarded as unfair unless it complies with conditions prescribed by an Ordinance.

Section 9 provides that 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 (set out in Schedule 9). But further processing of personal data is deemed to be compatible with any purpose for which the data is collected if the data subject's explicit consent is obtained, the further processing is for a historical or scientific purpose or the further processing is specifically authorised or required by an enactment.

Section 10 sets out rules governing consent for the processing of personal data. Consent is not valid unless it satisfies the requirements in section 10(1), having regard to whether the

person giving consent is a child and if so, the age of the child. A data subject can withdraw consent to processing at any time, and the controller must provide a procedure for withdrawal that is at least as simple as the procedure for giving consent. Consent to the processing of criminal data is not valid unless the controller is authorised or required by an enactment to process the criminal data, or to make a request for it.

Section 11 provides for anonymisation of personal data. The controller is required to notify the data subject of anonymisation, but Part III of this Law does not apply to anonymised data.

PART III

DATA SUBJECT RIGHTS

Section 12 requires controllers that collect personal data directly or indirectly from data subjects to give data subjects the information in Schedule 3. That information must be given to data subjects at or before the time of collection.

Section 13 requires controllers in any other case to give data subjects the information in Schedule 3 within a reasonable period of processing, and in any case at or before the time of first communication with the data subject, disclosure to another recipient and the expiry of one month following the processing.

Section 14 gives data subjects who have given their personal data to a controller, for the conclusion or performance of a contract in the case of automated processing, the right to request that personal data be returned to them or transmitted to another controller ("**right to data portability**".

Section 15 gives data subjects the right to request from a controller confirmation as to whether the controller is processing the data subject's personal data, as well as the information in Schedule 3 and copies of their personal data ("**right of access**").

Section 16 provides for an exception to the right to data portability and right of access, where compliance with the request would result in disclosing information relating to an identified or identifiable other individual. In this case, the controller must engage in a balancing exercise, taking into account the matters in section 16(3), and must withhold that

information where reasonable to do so to protect the significant interests of the other individual. If the information is withheld, the controller may provide limited viewing access to that information where appropriate.

Section 17 provides that, where personal data is processed for direct marketing purposes, the controller must give the data subject notice and the data subject has the right to require the controller to cease processing the data.

Section 18 applies where processing is necessary for the legitimate interests of the controller or a third party, or where it is necessary for the exercise or performance by a public authority of a public function or task in the public interest. In this case, the data subject has the right to require the controller to cease processing the data, unless the public interest in the objective of the processing outweighs the significant interests of the data subject.

Section 19 provides that, where the processing is necessary for a historical or scientific purpose (e.g. archiving or statistics), the data subject has the right to require the controller to cease the processing unless the controller is a public authority, the historical or scientific purpose is in the public interest and the public interest outweighs the data subject's significant interests.

Section 20 gives data subjects the right to rectify inaccurate or incomplete personal data, where the controller is reasonably able to verify that the data is inaccurate or incomplete. Where verification is not reasonable to expect, the controller must add to the data a statement that the data subject disputes the accuracy or completeness of that data.

Section 21 gives data subjects the right to request erasure of personal data in a number of circumstances, e.g. where the data is no longer necessary for the purpose for which it was processed. There several exceptions to this right, based on the purpose for which the data was processed.

Section 22 gives data subjects the right to restrict processing of personal data in certain temporary or limited circumstances.

Section 23 applies where any rectification or erasure of personal data or restriction of processing is carried out in accordance with section 20, 21 or 22. Controllers are required to notify data subjects of the contact details of any person to whom that data has been disclosed,

and of any lifting of a restriction on processing. Controllers must also notify recipients of that data of any rectification or erasure of personal data or restriction of processing.

Section 24 gives data subjects the right not to be subject to decisions based on automated processing, subject to a few exceptions.

Section 25 requires controllers to take reasonable steps to facilitate the exercise of data subject rights under this Part of this Law.

Section 26 applies sections 27 to 29 to any request made to a controller to exercise any data subject right in sections 14 to 22 (other than section 16).

Section 27 requires controllers to comply with the request, subject to any exception or exemption provided in this Law, as soon as practicable and in any case within the designated period. The designated period is one month from the day the controller receives the request, the day on which the controller receives any information reasonably necessary to verify the identity of the requestor, or the day on which any fee or charge payable under this Law is paid, whichever is the latest.

Section 28 allows controllers to require any additional information reasonably necessary to confirm the identity of the requestor.

Section 29 provides for exceptions to the data subject rights where a request is clearly unfounded or frivolous, vexatious, unnecessarily repetitive or otherwise excessive.

PART IV

DUTIES OF CONTROLLERS AND PROCESSORS

Section 30 requires controllers to give any information required under this Law in writing and in a concise, transparent, easily visible, easily accessible, intelligible and clearly legible, form, subject to certain exceptions.

Section 31 requires controllers to take reasonable steps to ensure that processing of personal data is carried out in compliance with this Law and to be able to demonstrate compliance upon request.

Section 32 requires controllers to carry out proportionate measures to effectively comply with data protection principles, ensure by default that only personal data that is necessary for a specific purpose is processed, and integrate necessary safeguards to comply with this Law and safeguard data subject rights.

Section 33 provides for the respective legal duties of joint controllers, including the requirement for an explicit agreement to set out their respective responsibilities.

Section 34 prohibits causing or permitting a processor to process personal data unless the processor provides the controller with sufficient guarantees that reasonable measures will be carried out to ensure that the processing meets the requirements of this Law and to safeguard data subject rights. In addition, there must be a contract between the controller and the processor setting out a number of matters, including the duties of the controller and the processor.

Section 35 imposes a number of duties on processors, including to process data only on written instructions from controllers, informing the controller if the processor is required by law to process personal data contrary to those written instructions, and deleting personal data or returning it to the controller at the end of the provision of the processing services.

Section 36 restricts processors from engaging secondary processors unless certain conditions are satisfied.

Section 37 requires controllers and processors to keep prescribed records, produce those records for inspection on request, and make prescribed returns of information to the Data Protection Authority ("**the Authority**"). In addition, they are required to cooperate with the Authority and give authorised officers access to premises which they are entitled to enter under this Law.

PART V

ADMINISTRATIVE DUTIES

Section 38 requires a controller established in the Bailiwick (within the meaning of section 111(1), but not a legal entity in Guernsey, Alderney or Sark, to nominate a Guernsey, Alderney or Sark legal entity as its representative in the Bailiwick.

Section 39 requires controllers and processors established in the Bailiwick to be registered in accordance with regulations made under Schedule 4. Failure to register is an offence.

Section 40 authorises regulations to be made to require registered controllers and registered processors to pay a prescribed levy to the Authority to cover the costs of establishing the Authority and its operating costs.

PART VI

SECURITY OF PERSONAL DATA

Section 41 requires controllers and processors to take reasonable steps to ensure the security of personal data. This could include pseudonymisation or encryption.

Section 42 requires processors, upon becoming aware of a personal data breach, to notify controllers. Controllers are in turn required to notify the Authority of any personal data breach within 72 hours, unless the breach is unlikely to result in any risk to the significant interests of the data subject.

Section 43 requires controllers to notify a data subject of any personal data breach if the breach is likely to pose a high risk to the significant interests of the data subject.

PART VII

DATA PROTECTION IMPACT ASSESSMENTS AND PRIOR CONSULTATION

Section 44 forbids controllers from causing or permitting high-risk processing unless a detailed data protection impact assessment is carried out before the processing.

Section 45 requires controllers to consult the Authority in writing where a data protection impact assessment reveals that proposed processing would be high-risk processing in the absence of mitigating measures.

Section 46 requires a committee of the States to consult the Authority before enacting or making, or recommending the enactment or making, of any high-risk legislation.

PART VIII
DATA PROTECTION OFFICERS

Section 47 requires controllers and processors to jointly designate data protection officers where processing is carried out in the context of public authorities or where late-scale and systematic monitoring of data subjects, or large-scale processing of special category data, is involved.

Section 48 provides for voluntary designation of data protection officers, or designations where required by an Ordinance.

Section 49 specifies the requirements to be met in designating a data protection officer.

Section 50 sets out the functions of data protection officers.

Section 51 requires designating entities to notify the Authority and the public of a designation, and to support data protection officers in the performance of their functions under this Law.

PART IX
CODES OF CONDUCT AND CERTIFICATION MECHANISMS

Section 52 allows the Authority to approve codes of conduct to encourage or facilitate compliance with the Law or demonstrate that controllers or processors bound to such codes have appropriate safeguards for the protection of personal data, for the purposes of cross-boundary transfers permitted under section 59.

Section 53 provides for the Authority to accredit a monitoring body for an approved code of conduct if a set of conditions is met.

Section 54 allows the Home Affairs Committee ("**the Committee**") to make regulations to provide for certification that processing operations comply with the Law or that appropriate safeguards exist for the purposes of cross-boundary transfers permitted under section 59.

PART X

TRANSFERS TO UNAUTHORISED JURISDICTIONS

Section 55 prohibits the transfer of personal data to a person in an unauthorised jurisdiction for the purposes of processing or in circumstances where the transferor knew or should have known that the data would be processed after the transfer. The only exceptions allowed are in sections 56, 57 and 59.

Section 56 allows a transfer where there are appropriate safeguards for the protection of personal data.

Section 57 allows a transfer where the Authority has given specific authorisation for the transfer.

Section 58 provides for the Authority to approve binding corporate rules for the purposes of the safeguards required by section 56. Those rules must be legally binding, must confer enforceable rights on data subjects and must specify the matters in Schedule 5 in a manner that provides appropriate safeguards for the protection of personal data and protection of the significant interests of data subjects.

Section 59 allows a transfer in several other circumstances, such as where required by an order of a court or tribunal or where the data subject has given informed and explicit consent to the transfer.

PART XI

THE DATA PROTECTION AUTHORITY

Section 60 establishes the Authority and gives effect to Schedule 6, in respect of the Authority and its constitution and proceedings.

Section 61 confers a range of functions on the Authority, including administering the Law and promoting awareness of the Law amongst controllers, processors and the public.

Section 62 requires the Authority to act independently in exercising or performing its functions.

Section 63 provides for the Authority to publish opinions or guidance on issues related to the protection of personal data, including compliance with any provision of this Law.

Section 64 allows the Authority, in the public interest, to issue a public statement in relation to any aspect of various functions of the Authority under the Law, including complaints, investigations, inquiries or any notification made to the Authority of a personal data breach.

Section 65 requires the Authority to take steps to facilitate international cooperation in the enforcement of legislation for the protection of personal data.

Section 66 provides that the Authority should be regarded as the designated authority in the Bailiwick for the purposes of Article 13 of the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (1981) and the competent supervisory authority of the Bailiwick under the GDPR. This section also allows the Committee to make regulations to confer powers or impose duties on the Authority for the purposes of that Convention and the GDPR.

PART XII

ENFORCEMENT BY THE AUTHORITY

Section 67 allows aggrieved individuals to make a complaint to the Authority if they consider that a controller or processor has breached or is likely to breach any provision of Parts II to X of the Law ("**operative provision**").

Section 68 provides for the Authority to investigate each complaint, subject to a few limited exceptions, for example where the complaint is clearly unfounded or vexatious.

Section 69 provides for the Authority to conduct inquiries on its own initiative, which may be conducted together with an investigation or separately.

Section 70 gives the Authority and its authorised officers the powers in Schedule 7.

Section 71 provides for the Authority, on the conclusion of an investigation, to make a breach determination or conversely a determination that the person concerned has not breached or is not likely to breach an operative provision.

Section 72 provides for the Authority, on the conclusion of an inquiry, to make a breach determination or conversely a determination that the person concerned has not breached or

is not likely to breach an operative provision. In addition, the Authority can also make recommendations to the Committee, the States of Deliberation (or States of Guernsey) or States of Alderney or the Chief Pleas of Sark.

Section 73 authorises the Authority, upon making a breach determination, to impose a range of sanctions on the person concerned. These include a reprimand or warning, or an order ("**enforcement order**") to take specified actions or pay a civil penalty by way of an administrative fine.

Section 74 provides for the Authority to order an administrative fine for breaches of specified operative provisions of the Law.

Section 75 imposes limits on the amount of the administrative fine that may be ordered in any specific case.

Section 76 requires the Authority to provide the person concerned with an opportunity to make written or oral representations to the Authority before the Authority makes a breach determination or enforcement order against that person, subject to exceptions on limited grounds.

Section 77 excludes courts and tribunals acting in a judicial capacity from the jurisdiction of the Authority.

PART XIII

CIVIL PROCEEDINGS FOR BREACH OF STATUTORY DUTY

Section 78 defines expressions used in this part of the Law.

Section 79 provides for injured parties to bring a civil action against a controller or processor for breach of an operative provision, where the breach causes "damage" (defined widely in section 111(1) to includes financial loss, distress, inconvenience and other adverse effects).

Section 80 sets out makes additional provisions concerning liability in these civil actions: defendants are exempt from liability if they prove that they are not responsible in any way for the damage concerned; processors are generally exempt from liability except in limited circumstances; and controllers and processors may be jointly liable in a civil action.

PART XIV

APPEALS AND OTHER PROCEEDINGS

Section 81 defines expressions used in this part of the Law.

Section 82 allows complainants to appeal to the Court a failure by the Authority to give complainants notice that a complaint is being investigated (or not being investigated), or notice of the progress of any investigation into a complaint.

Section 83 allows complainants to appeal to the Court a decision of the Authority not to investigate a complaint or a determination that a controller or processor has not breached or is not likely to breach an operative provision.

Section 84 allows a person against whom a breach determination or an enforcement order is made to appeal the determination or order to the Court.

Section 85 allows the Authority to bring civil proceedings in the Court in respect of any breach or anticipated breach of an operative provision by a controller or processor.

Section 86 allows a court to suspend proceedings relating to processing in the context of a controller or processor where proceedings are pending in another court concerning the same subject matter and processing in the context of the same controller or processor.

PART XV

OFFENCES AND CRIMINAL PROCEEDINGS

Section 87 creates the offence of obtaining or disclosing personal data without the consent of the controller, and related offences of procuring, selling or retaining such data.

Section 88 creates the offence of obstructing the Authority or any member, employee or authorised officer of the Authority ("**Authority official**") in the exercise of functions under the Law, including failing to comply with a requirement or making false, deceptive or misleading statements.

Section 89 makes it an offence to impersonate Authority officials.

Section 90 imposes a duty of confidentiality on Authority officials, agents of the Authority or the Commissioner, and data protection officers, and makes it an offence to breach that duty.

Section 91 provides for a number of exceptions from that duty of confidentiality.

Section 92 imposes criminal liability on directors and other officers, where an offence is committed by a body corporate, limited partnership with legal personality or foundation, with the consent or connivance of, or attributable to any neglect on the part of, those directors or other officers.

Section 93 imposes criminal liability on partners, committee members and other officers, where an offence is committed by an unincorporated body with the consent or connivance of, or attributable to any neglect on the part of those partners, committee members or other officers.

Section 94 sets out the penalties for offences under the Law and provides for further court orders in the case of conviction for an offence.

Section 95 provides that those penalties apply in relation to Alderney and Sark, despite provisions to the contrary in the Government of Alderney Law, 2004 or the Reform (Sark) Law, 2008.

PART XVI

GENERAL AND MISCELLANEOUS

Section 96 gives effect to the exceptions and exemptions in Schedule 8.

Section 97 allows data protection organisations, by agreement with a person, to represent the person in making any complaint to the Authority or bringing a civil action under section 79.

Section 98 avoids contractual terms that require individuals to supply to another person health records made by health professionals and obtained by the individual in the exercise of a data subject right.

Section 99 provides, where a breach of an operative provision is alleged to have been committed by an unincorporated body, for proceedings to be brought and notices served in the name of the unincorporated body and not in the name of any of its members.

Section 100 provides for the privilege against self-incrimination.

Section 101 excludes Authority officials acting in the discharge or purported discharge of functions under the Law from personal liability, except in cases of bad faith.

Section 102 provides for the service of notices and other documents under the Law.

Section 103 authorises the States of Deliberation to make provisions by Ordinance relating to the processing of personal data for a crime-related purpose, including provisions to implement data protection provisions equivalent to the Law Enforcement Directive.

Section 104 authorises the States of Deliberation to make provisions by Ordinance relating to respect for private life and protection of personal data in relation to electronic communications. This would include provisions to implement provisions equivalent to any e-Privacy Directive in the future.

Section 105 authorises the States of Deliberation to make provisions by Ordinance requiring authorising, prohibiting or restricting the processing of identifiers or personal data, including in the context of recruitment or employment.

Section 106 authorises the States of Deliberation to amend the Law by Ordinance where it appears to be necessary or expedient to do so for certain purposes, including protecting the rights of individuals in relation to their personal data and providing for the free movement of personal data in a manner equivalent to the GDPR or the Law Enforcement Directive, enabling the Authority and the Commissioner to effectively and efficiently exercise or perform their functions, or maintaining or enhancing the reputation or standing of the Bailiwick.

Section 107 authorises the States of Deliberation to make transitional, savings and consequential provisions by Ordinance.

Section 108 sets out fairly standard provisions concerning Ordinances. It also requires, before an Ordinance is made, consultation with the Authority and (in the case of an Ordinance affecting Alderney) the Policy & Finance Committee of the States of Alderney, and (in the case of an Ordinance affecting Sark) the Policy and Performance Committee of the Chief Pleas of Sark.

Section 109 sets out fairly standard provisions concerning Regulations. It also requires, before Regulations are made, consultation with the Authority and (in the case of an Ordinance

affecting Alderney) the Policy & Finance Committee of the States of Alderney, and (in the case of an Ordinance affecting Sark) the Policy and Performance Committee of the Chief Pleas of Sark.

Section 110 gives effect to Schedule 9, which gives meaning to special expressions used in the Law.

Section 111 sets out the interpretation provisions, including definitions of terms used in the Law.

Section 112 provides for Schedule 10, which sets out an index of expressions defined in the Law.

Section 113 repeals the existing Data Protection (Bailiwick of Guernsey) Law, 2001 and Ordinances made under that Law.

Section 114 sets out the name of this Law.

Section 115 provides for the commencement of this Law by Ordinance.