GDPR AND LED IMPLEMENTING REGULATIONS 2018

Index

Statutory Document No. 2018/0145

Data Protection Act 2018

GDPR AND LED IMPLEMENTING REGULATIONS 2018[1]

Approved by Tynwald: *18 July 2018*
Coming into Operation: *1 May 2018*

The Council of Ministers makes the following Regulations under section 5 of the Data Protection Act 2018.

PART 1 – PRELIMINARY

1 Title

These Regulations are the GDPR and LED Implementing Regulations 2018.[1]

2 Commencement

If approved by Tynwald, these Regulations come into operation on 1 August 2018.[2]

3 Overview

These Regulations are to be read and construed —

(a) as subordinate to the applied GDPR and the applied Law Enforcement Directive; and

(b) with —

(i) the Data Protection (Application of GDPR) Order 2018[3]; and

[1] This version of SD2018/0145 has been prepared for convenience and incorporates the corrections contained in correction notice SD2018/0145cn. This version of SD2018/0145 was approved by Tynwald on 18 July 2018.

[2] The Regulations as made were expressed to come into operation on 1 July 2018. However, under section 5(6) of the Data Protection Act 2018 the Regulations require Tynwald approval and under section 30(2) of the Legislation Act 2015 the Regulations cannot come into operation until they are approved by Tynwald. The Regulations, as approved by Tynwald on 18 July 2018, come into operation on 1 August 2018.

[3] SD 2018/0143

(ii) the Data Protection (Application of LED) Order 2018[4].

4 Deemed membership of the EU

(1) Subject to paragraph (2), the Island is deemed to be a Member State of the European Union.

(2) Paragraph (1) applies for the purposes of these Regulations in so far as those purposes reflect the provisions of —

(a) the GDPR, except Chapter V (transfers of personal data to third countries or international organisations); and

(b) the LED, except Chapter V (transfers of personal data to third countries or international organisations).

(3) For the avoidance of doubt, paragraph (1) —

(a) is not intended to and does not have the effect of rendering the Island a Member State of the European Union; and

(b) does not cede authority to the European Union in any respect, as these implementing regulations remain an enactment made by the Council of Ministers in exercise of power conferred by Tynwald; and therefore the extent to which the provisions of the GDPR and LED are applicable to the Island is solely dependent on decisions taken locally and given legislative effect by Manx legislation.

5 Interpretation

(1) Subject to paragraph (2), in these Regulations —

"the Act" means the *Data Protection Act 2018*;

"**applied GDPR**" means the GDPR as applied to the Island by the Data Protection (Application of GDPR) Order 2018[5], including all the exceptions, adaptations and modifications specified in the said order;

"**applied Law Enforcement Directive**" or **"applied LED"** means the Law Enforcement Directive as applied to the Island by the Data Protection (Application of LED) Order 2018[6], including all the exceptions, adaptations and modifications in the said order;

"archiving in the public interest" must be construed in accordance with the following stipulations —

(a) it refers to an activity engaged in by an organisation which acquires, preserves, appraises, arranges, describes, communicates, promotes, disseminates and provides access to records of enduring social value and which

[4] SD 2018/0144
[5] SD 2018/0143
[6] SD 2018/0144

holds the records in the interest of society, in order to support, inter alia, research and freedom of expression and information;

(b) organisations that gather and use data, information and records solely for their commercial gain do not operate in the public interest;

(c) any data protection obligations of archives and archive services under these Regulations must be proportionate to the size and resources of the organisation and take into account the public interest level and nature of the materials being archived;

"biometric data" means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data;

"**credit reference agency**" means a person carrying on a business comprising the furnishing of persons with information relevant to the financial standing of natural persons and collected by that person for that purpose;

"data concerning health" means personal data relating to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status;

"Data Protection Convention" means the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data[7] which was opened for signature on 28 January 1981, as amended up to the day on which these Regulations come into operation;

"**data protection legislation**" means —

(a) the applied GDPR;

(b) the applied Law Enforcement Directive;

(c) these Regulations; and

(d) regulations made under these Regulations, pursuant to section 5 of the Act;

(e) any other order made under section 4 of the Act in respect of any EU instrument relating to the protection of personal data other than the GDPR or the LED; or

(f) any implementing regulations made in respect of an order referred to in subparagraph (e), and any regulations made

[7] European Treaty Series - No. 108.

under such implementing regulations pursuant to section 5 of the Act;

"enactment" includes —

(a) an enactment passed or made after these Regulations;

(b) an enactment comprised in a public document;

"filing system" means any structured set of personal data which is accessible according to specific criteria, whether held by automated means or manually and whether centralised, decentralised or dispersed on a functional or geographical basis;

"GDPR" or **"General Data Protection Regulation"** means Regulation (EU) 2016/679 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 Data Protection Regulation);

"genetic data" means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which results, in particular, from an analysis of a biological sample from the natural person in question;

"health professional" means any of the following, —

(a) a registered medical practitioner (including any person who is provisionally registered under section 15 or 21 of the Medical Act 1983 (an Act of Parliament) and is engaged in such employment as is mentioned in section 15(3) or 21(3) of that Act);

(b) a registered dentist as defined in section 11(1) of the *Dental Act 1985*;

(c) a registered nurse or midwife, within the meaning of section 3 of the *Health Care Professionals Act 2014*;

(d) a member of a profession related or supplementary to medicine and specified in regulations[8] made by the Department of Health and Social Care for the purposes of this definition, who fulfils such conditions (as to registration or otherwise) as may be so specified;

"health record" means a record which —

(a) consists of data concerning health; and

(b) has been made by or on behalf of a health professional in connection with the diagnosis, care or treatment of the natural person to whom the data relate;

[8] Tynwald procedure – approval required.

"identifiable living natural person" means a living natural person who can be identified, directly or indirectly, in particular by reference to —

(a) an identifier such as a name, an identification number, location data or an online identifier; or

(b) one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the natural person;

"inaccurate", in relation to personal data, means incorrect or misleading as to any matter of fact;

"Information Commissioner" has the same meaning in these Regulations as it has in the *Freedom of Information Act 2015*;

"international obligation of the Island" includes —

(a) an EU obligation; and

(b) an obligation that arises under an international agreement or arrangement which has been extended to the Island by the United Kingdom;

"international organisation" means an organisation and its subordinate bodies governed by international law, or any other body which is set up by, or on the basis of, an agreement between two or more countries;

"**Law Enforcement Directive**" or **"LED"** means Directive (EU) 2016/680 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;

"personal data" has the meaning given in Article 4(1) of the applied GDPR[9];

"prescribed" means prescribed in regulations which , in accordance with section 5(3)(b) and (7) of the Act, are made under these Regulations;

"public document" has the meaning given in section 15 of the *Interpretation Act 2015*;

"publish" means make available to the public or a section of the public;

"third country" means a State, territory or jurisdiction, or a part of any of the foregoing, —

(a) other than the Island; and

[9] The identical definition appears in Article 3(1) of the applied LED.

(b) which is not a Member State of the European Union;

"the Tribunal", in relation to an application or appeal under these Regulations, means the Tribunal referred to in regulation 119;

"tribunal" means any tribunal to which the *Tribunals Act 2006* applies.

(2) The list of terms defined paragraph (1) is not an exhaustive list of terms which have a particular meaning in these Regulations. As these Regulations are to be read in conjunction with the applied GDPR and the applied LED —

(a) Article 4 of the applied GDPR; and

(b) in respect of Part 3 of these Regulations, Article 3 of the applied LED,

are to be consulted, as both those Articles contain definitions of terms used in these Regulations but not defined in paragraph (1).

(3) For the purposes of Article 86 of the applied GDPR, "**official documents**" includes any of the following that has duly emanated from the appropriate and properly constituted authority —

(a) all deeds, forms, or correspondence presented or produced to the Land Registry relating to registrations or dealings under the *Land Registration Act 1982* or the Land Registry Rules 2000 or any entry on the register made under either of those enactments; and

(b) any map, survey, record or book made or kept pursuant to any enactment,

regardless of the form in which the document is constituted.

6 Meaning of "controller"

(1) Paragraphs (2) and (3) qualify the definition of "controller" that appears in Article 4(7) of the applied GDPR.

(2) Where data are processed only —

(a) for purposes for which they are required by an enactment to be processed; and

(b) by means which an enactment required to be used for such processing,

the controller is the person on whom the obligation to process the data is imposed by the enactment or any one of the enactments (if there is more than one).

(3) The definition of "controller" in Article 4(7) of the applied GDPR is also subject to regulations 148 and 149.

7 Meaning of "public authority" and "public body"

(1) For the purposes of the applied GDPR, the following (and only the following) are "public authorities" or "public bodies" under the law of the Island —

(a) a public authority as defined by section 6(1) of the *Freedom of Information Act 2015*, subject to paragraph (2); and

(b) an authority or a body specified by the Council of Ministers in regulations (Tynwald procedure – approval required).

(2) The Council of Ministers may by regulations provide that a person that would otherwise qualify under paragraph (1) as a public authority is not a public authority for the purposes of the applied GDPR.

Tynwald procedure – approval required.

8 Application of these Regulations

(1) Except as otherwise provided by or under regulations 87 to 89, these Regulations apply to a controller[10] and a processor[11] in respect of any personal data only if —

(a) the controller or processor is established in the Island and the data are processed in the context of that establishment; or

(b) the controller or processor is not established in the Island but uses equipment in the Island for processing the personal data otherwise than for the purposes of transit through the Island.

(2) A controller or processor falling within paragraph (1)(b) must nominate for the purposes of these Regulations a representative established in the Island.

(3) For the purposes of paragraphs (1) and (2), each of the following is to be treated as established in the Island —

(a) a natural person who is ordinarily resident in the Island;

(b) a body incorporated under the law of the Island;

(c) a partnership or other unincorporated association formed under the law of the Island; and

(d) any person who does not fall within subparagraph (a), (b) or (c) but maintains in the Island —

[10] Defined in Article 4(7) of the applied GDPR and so to be construed in these Regulations, except where used in respect of a "competent authority" (see regulation 28). Where "controller" is used in these Regulations in respect of a competent authority, it must be construed in accordance with the definition in Article 3(8) of the applied LED.

[11] Defined in Article 4(8) of the applied GDPR and in identical terms in Article 3(9) of the applied LED.

(i) an office, branch or agency through which he or she carries on any activity; or

(ii) a regular practice,

and references to establishment in another country or territory have a corresponding meaning.

(4) These Regulations also apply to a controller in respect of the processing of personal data to which the applied GDPR applies where, —

(a) the controller is established in a country or territory other than the Island and the personal data are processed in the context of the activities of that establishment;

(b) the personal data relates to a natural person who is in the Island when the processing takes place; and

(c) the purpose of the processing is, —

(i) to offer goods or services to natural persons in the Island, whether or not for payment; or

(ii) to monitor natural persons' behaviour in the Island.

(5) These Regulations also apply to a processor in respect of the processing of personal data to which the applied GDPR applies where, —

(a) the controller on whose behalf the processor acts is established in a country or territory other than the Island and the personal data are processed in the context of the activities of that establishment; or

(b) the processor is established in a country or territory other than the Island and the personal data are processed in the context of the activities of that establishment,

and the conditions in paragraph (4)(b) and (c) are satisfied.

(6) Paragraphs (4) and (5) have effect subject to any provision made under regulation 83 providing for the Information Commissioner to carry out functions in relation to other controllers or processors.

(7) In this regulation, references to a person established in the Island include the following, —

(a) a natural person who is ordinarily resident in the Island;

(b) a body incorporated under the law of the Island;

(c) a partnership or other unincorporated association formed under the law of the Island; and

(d) a person not within subparagraph (a), (b) or (c) who maintains, and carries on activities through, an office, branch or agency or other stable arrangement in the Island.

(8) For the purposes of this regulation, —

(a) a processor who is considered a controller by virtue of Article 28(1) of the applied GDPR is to be treated as a controller; and

(b) where there is more than one controller, the reference in paragraph (5)(a) to the controller is to one or more of them.

PART 2 – PROVISIONS SUPPLEMENTARY TO THE APPLIED GDPR

Purpose

9 Purpose of this Part

(1) This Part supplements the applied GDPR, on the basis that the GDPR is automatically law in Member States and was accordingly written in a manner which lends itself to application and enforcement with minimal supporting or supplementary provisions in actual Member State law.

(Note that, in accordance with regulation 4, the Island is "deemed" to be a Member State solely for the purposes of these Regulations. This is merely for ease of reference and, in reality, does not have the effect of conferring on the Island actual membership of the EU. The Island is therefore not an "actual Member State".)

(2) There is a difference between "the GDPR" and "the applied GDPR", which is as follows —

(a) "the GDPR" is the original EU instrument and applies to all "actual Member States" of the EU; whereas

(b) "the applied GDPR"[12] is the Island's version of the original.

The "applied GDPR" applies to the Island as part of the law of the Island and is distinguishable from the original based on the exceptions, adaptations and modifications evident in it.

(3) Accordingly, this Part relies on (but does not replicate) provisions already in the applied GDPR which confer clear rights, responsibilities, duties and obligations on specified legal persons and natural persons.

(4) This Part also requires every controller and processor to which the applied GDPR applies to comply with the registration requirements in Schedule 7.

(5) Schedule 9 specifies restrictions and exemptions to the application of the provisions of the applied GDPR. Those restrictions and exemptions are in addition to the restrictions specified in regulations 20 to 24 or specified in regulations made under regulation 25.

[12] See the definition of this term in regulation 5(1).

(6) The principles relating to the processing of personal data are set out in Article 5 of the applied GDPR.

Lawfulness of processing

10 Lawfulness of processing: public interest etc

In Article 6(1) of the applied GDPR (lawfulness of processing), the reference in point (e) to processing of personal data that is necessary for the performance of a task carried out in the public interest or in the exercise of the controller's official authority includes processing of personal data that is necessary for —

(a) the administration of justice;

(b) the exercise of a function of Tynwald and its branches;

(c) the exercise of a function conferred on a person by an enactment; or

(d) the exercise of a function of the Crown, a Department or a Statutory Board.

Child's consent

11 Child's consent in relation to information society services

(1) In Article 8(1) (conditions applicable to child's consent in relation to information society services) —

(a) references to "16 years" are to be read as references to "13 years"; and

(b) the reference to "information society services" does not include preventive or counselling services.

(2) In this regulation, "information society service" has the meaning given to that term by Article 4(25) of the applied GDPR. (See also the power conferred on the Council of Ministers by section 163 of the *Equality Act 2017*.)

Special categories of personal data

12 Special categories of personal data and criminal convictions etc data

(1) Paragraphs (2) and (3) make provision about the processing of personal data described in Article 9(1) of the applied GDPR (prohibition on processing of special categories of personal data) in reliance on an exception in any of the following provisions under Article 9(2) of the applied GDPR —

(a) point (b) (employment, social security and social protection);

(b) point (g) (substantial public interest);

(c) point (h) (health and social care);

(d) point (i) (public health); or

(e) point (j) (archiving, research and statistics).

(2) The processing meets the requirements for authorisation[13] by or a basis in the law of the Island or as part of the Island only if it meets a condition in Part 1 of Schedule 2.

(3) The processing meets the requirement in point (g) of Article 9(2) of the applied GDPR for a basis in the law of the Island only if it meets a condition in Part 2 of Schedule 2.

(4) Paragraph (5) makes provision about the processing of personal data relating to criminal convictions and offences or related security measures that is not carried out under the control of official authority.

(5) The processing meets the requirements in Article 10 of the applied GDPR for authorisation by, or a basis in, the law of the Island only if it meets a condition in Part 2 or 3 of Schedule 2.

(6) The Council of Ministers may by regulations amend Schedule 2 by adding, varying or omitting conditions or safeguards.

Tynwald procedure – approval required.

13 Special categories of personal data etc.: supplementary

(1) For the purposes of Article 9(2)(h) of the applied GDPR (processing for health or social care purposes etc.), the circumstances in which the processing of personal data is carried out subject to the conditions and safeguards referred to in Article 9(3) of the applied GDPR (obligation of secrecy) include circumstances in which it is carried out —

(a) by or under the supervision of a health professional or a social worker; or

(b) by another person who in the circumstances owes a duty of confidentiality under an enactment or rule of law.

(2) In Article 10 of the applied GDPR, references to personal data relating to criminal convictions and offences or related security measures include personal data relating to —

(a) the alleged commission of offences by the data subject; or

(b) proceedings for an offence committed or alleged to have been committed by the data subject or the disposal of such proceedings, including sentencing.

(3) In paragraph (1), "social worker" has the same meaning as is given to that term in section 140 of the *Regulation of Care Act 2013*.

[13] The requirements for authorisation here referred to are those specified in provisions of the applied GDPR listed in paragraph (1).

Rights of the data subject

14 Limits on fees that may be charged by controllers

(1) The Council of Ministers may by regulations specify limits on the fees that a controller may charge in reliance on —

(a) Article 12(5) of the applied GDPR (reasonable fees when responding to manifestly unfounded or excessive requests); or

(b) Article 15(3) of the applied GDPR (reasonable fees for provision of further copies).

(2) The Council of Ministers may by regulations —

(a) require controllers of a description specified in the regulations to produce and publish guidance about the fees that they charge in reliance on those provisions; and

(b) specify what the guidance must include.

Tynwald procedure – negative.

15 Obligations of credit reference agencies

(1) This regulation applies where a controller is a credit reference agency.

(2) The controller's obligations under Article 15(1) to (3) of the applied GDPR (confirmation of processing, access to data and safeguards for third country transfers) are taken to apply only to personal data relating to the data subject's financial standing, unless the data subject has indicated a contrary intention.

(3) Where the controller discloses personal data in pursuance of Article 15(1) to (3) of the applied GDPR, the disclosure must be accompanied by a statement informing the data subject of the data subject's rights to have inaccurate information corrected.

16 Automated decision-making authorised by law: safeguards

(1) This regulation makes provision for the purposes of Article 22(2)(b) of the applied GDPR (exception from taking significant decisions based solely on automated processing for decisions that are authorised by law and subject to safeguards for the data subject's rights, freedoms and legitimate interests).

(2) A decision is a "significant decision" for the purposes of this regulation if, in relation to a data subject, it —

(a) produces legal effects concerning the data subject; or

(b) significantly affects the data subject.

(3) A decision is a "qualifying significant decision" for the purposes of this regulation if —

(a) it is a significant decision in relation to a data subject;

(b) it is required or authorised by law; and

(c) it does not fall within Article 22(2)(a) or (c) of the applied GDPR (decisions necessary to a contract or made with the data subject's consent).

(4) Where a controller takes a qualifying significant decision in relation to a data subject based solely on automated processing —

(a) the controller must, as soon as reasonably practicable, notify the data subject in writing that a decision has been taken based solely on automated processing; and

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

(i) reconsider the decision; or

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

(5) If a request is made to a controller under paragraph (4), the controller must, before the end of the period of 21 days beginning with receipt of the request —

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

(b) comply with the request; and

(c) by notice in writing inform the data subject of —

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

(ii) the outcome of complying with the request.

(6) The Council of Ministers may by regulations make such further provision as the Council of Ministers considers appropriate to provide suitable measures to safeguard a data subject's rights, freedoms and legitimate interests in connection with the taking of qualifying significant decisions based solely on automated processing.

Tynwald procedure – approval required.

(7) Regulations under paragraph (6) may amend this regulation.

Accreditation of certification providers

17 Accreditation and duties of accredited person, and related regulations

(1) For the purposes of a code of conduct as defined in Articles 40 and 41 of the applied GDPR, the Information Commissioner may accredit any person to monitor compliance with a code if the Information Commissioner considers that the person has —

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

(b) established procedures that allow the person to assess the eligibility of the controllers and processors concerned to apply the code, monitor their compliance with its provisions and to review periodically the implementation of the code;

(c) established procedures and structures to handle complaints about infringements of the code or the manner in which the code has been, or is being, implemented by a controller or processor, and to make those procedures and structures transparent to data subjects and the public; and

(d) no conflict of interests in connection with the degree or performance of the person's other tasks and duties.

(2) In cases of infringement of the code by any controller or processor that purports to apply or implement the code, the accredited person must —

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

(b) notify the Information Commissioner of any action taken by the accredited person and the reasons for the action.

(3) The Information Commissioner may suspend or revoke an accreditation under paragraph (1) if —

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

(b) the accredited person contravenes paragraph (2).

(4) The Council of Ministers may by regulations provide for the establishment of mechanisms, seals or marks to certify or signify —

(a) that particular processing operations by controllers or processors comply with these Regulations; or

(b) the existence of appropriate safeguards for the protection of personal data by controllers or processors established in a third country for the purposes of personal data transfers to third countries or international organisations as provided for by Article 46 of the applied GDPR.

Tynwald procedure – approval required.

(5) No person is disqualified from being accredited under this regulation solely on account of the person not being resident or present in the Island.

Specific processing situations

18 Processing for archiving, research and statistical purpose: safeguards

(1) Subject to suitable and specific measures being taken to safeguard the fundamental rights and freedoms of data subjects, personal data may be processed, in accordance with Article 89 of the applied GDPR, for —

(a) archiving purposes in the public interest;

(b) scientific or historical research purposes; or

(c) statistical purposes.

(2) Processing of personal data for the purposes referred to in paragraph (1) must respect the principle of data minimisation[14].

(3) Where the purposes referred to in subparagraph (a), (b) or (c) of paragraph (1) can be fulfilled by processing which does not permit, or no longer permits, identification of data subjects, the processing of personal data for such purposes must be fulfilled in that manner.

(4) Such processing does not satisfy the requirement in Article 89(1) for the processing to be subject to appropriate safeguards for the rights and freedoms of the data subject if the processing is carried out for the purposes of measures or decisions with respect to a particular data subject, unless the purposes for which the processing is necessary include the purposes of approved medical research.

(5) In this regulation, "approved medical research" means medical research carried out by a person who has approval to carry out that research from the Department of Health and Social Care.

(6) The Council of Ministers may by regulations change the meaning of "approved medical research" for the purposes of this regulation, including by amending paragraph (5).

Tynwald procedure – approval required.

Scope of other general processing

19 Automated or structured processing of personal data

(1) Data protection legislation applies to the manual unstructured processing of personal data held by an FOI public authority.[2]

(2) In this regulation —

"automated or structured processing of personal data" means —

(a) processing of personal data carried on wholly or partly by automated means; and

[14] See Article 5(1)(c) of the applied GDPR.

(b) processing of personal data that forms part of a filing system or is intended to form part of a filing system;

"manual unstructured processing of personal data" means processing of personal data which is not automated or structured processing of data.

(3) In this regulation and regulations 20 and 21 —

(a) "FOI public authority" means a "public authority" as that latter term is defined in section 6(1) of the *Freedom of Information Act 2015*;

(b) references to personal data "held" by an FOI public authority are to be interpreted in accordance with section 8(2) of the *Freedom of Information Act 2015*.

Exemptions and restrictions, etc.

20 Manual unstructured data held by FOI public authorities

(1) The provisions of the applied GDPR and these Regulations listed in paragraph (2) do not apply to manual unstructured personal data held by FOI public authorities.

(2) The provisions are —

(a) in Chapter II of the applied GDPR (principles) —

(i) Articles 5(1)(a) to (c), (e) and (f) (principles relating to processing, other than the accuracy principle);

(ii) Article 6 (lawfulness);

(iii) Article 7 (conditions for consent);

(iv) Article 8, paragraph 1 and 2 (child's consent);

(v) Article 9 (processing of special categories of personal data);

(vi) Article 10 (data relating to criminal convictions, etc.); and

(vii) Article 11(2) (processing not requiring identification);

(b) in Chapter III of the applied GDPR (rights of the data subject) —

(i) Article 13(1) to (3) (personal data collected from data subject: information to be provided);

(ii) Article 14(1) to (4) (personal data collected other than from data subject: information to be provided);

(iii) Article 20 (right to data portability); and

(iv) Article 21(1) (objections to processing);

(c) in Chapter V of the applied GDPR, Articles 44 to 49 (transfers of personal data to third countries or international organisations); and

(d) regulations 127 and 128 of these Regulations.

(see also paragraph 1(2) of Schedule 6).

(3) A controller is not obliged to comply with Article 15(1) to (3) of the applied GDPR (right of access by the data subject) in relation to manual unstructured personal data held by FOI public authorities if —

(a) the request under that Article does not contain a description of the personal data; or

(b) the controller estimates that the cost of complying with the request, so far as relating to the personal data, would exceed the appropriate maximum.

(4) Paragraph (3)(b) does not remove the controller's obligation to confirm whether or not personal data concerning the data subject are being processed unless the estimated cost of complying with that obligation alone in relation to the personal data would exceed the appropriate maximum.

(5) In paragraph (4) —

"the appropriate maximum" means the maximum amount specified by the Council of Ministers by regulations.

Tynwald procedure – laying only.

21 Manual unstructured data used in longstanding historical research

(1) The provisions of the applied GDPR listed in paragraph (2) do not apply to manual unstructured personal data held by FOI public authorities at any time when —

(a) the personal data —

(i) are subject to processing which was already underway immediately before 1 April 2003; and

(ii) are processed only for the purposes of historical research; and

(b) the processing is not carried out —

(i) for the purposes of measures or decisions with respect to a particular natural person; or

(ii) in a way that causes, or is likely to cause, substantial damage or substantial distress to a data subject.

(2) Those provisions are —

(a) in Chapter II of the applied GDPR (principles), Article 5(1)(d) (the accuracy principle); and

(b) in Chapter III of the applied GDPR (rights of the data subject) —

(i) Article 16 (right to rectification); and

(ii) Article 17(1) and (2) (right to erasure).

(3) The restrictions in this regulation apply in addition to the restrictions in regulation 20.

22 National security and defence exemption and restriction

(1) A provision of the applied GDPR or these Regulations mentioned in paragraph (2) does not apply to the processing of personal data to which data protection legislation applies if exemption or restriction of the application of data protection legislation is required for —

(a) the purpose of safeguarding national security; or

(b) defence purposes.[3]

(2) The provisions are —

(a) Chapter II of the applied GDPR (principles) except for —

(i) Article 5(1)(a) (lawful, fair and transparent processing), so far as it requires processing of personal data to be lawful;

(ii) Article 6 (lawfulness of processing);

(iii) Article 9 (processing of special categories of personal data);

(b) Chapter III of the applied GDPR (rights of data subjects);

(c) in Chapter IV of the applied GDPR —

(i) Article 33 (notification of personal data breach to the Information Commissioner);

(ii) Article 34 (communication of personal data breach to the data subject);

(d) Chapter V of the applied GDPR (transfers of personal data to third countries of international organisations);

(e) in Chapter VI of the applied GDPR —

(i) Article 57(1)(a) and (h) (Information Commissioner's duties to monitor and enforce the applied GDPR and to conduct investigations);

(ii) Article 58 (investigative, corrective, authorisation and advisory powers of Information Commissioner);

(f) Chapter VIII of the applied GDPR (remedies, liabilities and penalties) except for —

(i) Article 83 (general conditions for imposing administrative fines);

(ii) Article 84 (penalties);

(g) in Part 6 of these Regulations —

(i) in regulation 84 (general functions of the Information Commissioner), paragraphs (3) and (8);

(ii) in regulation 84, paragraph (9), so far as it relates to Article 58(2)(i) of the applied GDPR;

(iii) regulation 88 (inspection in accordance with international obligations);

(h) in Part 7 of these Regulations —

(i) regulations 101 to 111 and Schedule 4 (Information Commissioner's notices and powers of entry and inspection);

(ii) regulations 126 to 128 (offences relating to personal data);

(i) in Part 8 of these Regulations, regulation 139 (representation of data subjects).

23 National security: certificate

(1) Subject to paragraph (3), a certificate signed by the Chief Minister certifying that exemption from all or any of the provisions listed in regulation 22(2) is, or at any time was, required in relation to any personal data for the purpose of safeguarding national security is conclusive evidence of that fact.

(2) A certificate under paragraph (1) —

(a) may identify the personal data to which it applies by means of a general description; and

(b) may be expressed to have prospective effect.

(3) Any person directly affected by a certificate under paragraph (1) may, in accordance with regulation 120, appeal to the Tribunal against the certificate.

(4) If, on an appeal under paragraph (3), the Tribunal finds that, applying the principles applied by a court on an application for petition of doleance, the Chief Minister did not have reasonable grounds for issuing a certificate, the Tribunal may —

(a) allow the appeal; and

(b) quash the certificate.

(5) Where, in any proceedings under or by virtue of the applied GDPR or these Regulations, it is claimed by a controller that a certificate under paragraph (1) which identifies the personal data to which it applies by means of a general description applies to any personal data, another party to the proceedings may appeal to the Tribunal on the ground that the certificate does not apply to the personal data in question.

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

(7) On an appeal under paragraph (5), the Tribunal may determine that the certificate does not so apply.

(8) A document purporting to be a certificate under paragraph (1) is to be —

(a) received in evidence; and

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

(9) A document which purports to be certified by or on behalf of the Chief Minister as a true copy of a certificate issued by that the Chief Minister under paragraph (1) is in any legal proceedings, evidence of that certificate.

24 Regulatory activity

The exemption or restriction in respect of regulatory activity is specified in paragraph 20 of Schedule 9.

25 Power to prescribe additional exemptions or restrictions

(1) The Council of Ministers may make regulations prescribing any additional exemptions or restrictions it considers necessary.

(2) Exemptions or restrictions made under this regulation may be to such extent as the Council of Ministers —

(a) considers appropriate; and

(b) specifies in the regulations.

Tynwald procedure – approval required.

PART 3 – LAW ENFORCEMENT PROCESSING

CHAPTER 1

Purpose and scope

26 Purpose of this Part

(1) This Part makes provision to give effect to the applied Law Enforcement Directive.

(2) The Law Enforcement Directive, being a "Directive" as distinct from a "Regulation" (which the GDPR is)[15], is written in a style that indicates that it requires laws other than itself to be made to give effect to it. The Law Enforcement Directive contains numerous provisions that use

[15] Under EU law, "Regulations" are automatically binding on all Member States and typically leave relatively few matters for Member States to address by discrete domestic legislation. By contrast, "Directives" are not generally written in a manner than lends itself to direct application without the need for Member States to enact discrete domestic legislation to put in place the legal rules that the Directives require. There remains, however, a legal obligation on Member States to take the steps mandated by Directives, which invariably means the enacting of discrete domestic legislation is obligatory.

language such as "Member States shall provide"; in some instances, provisions state that "Members States shall provide by law".

(3) Accordingly, this Part complies with stipulations such as those referred to in paragraph (2) by expressly making provisions of the type the Law Enforcement Directive mandates. In most instances the provisions of this Part follow very closely the language of the corresponding, expressly identified Articles of the applied LED. However, they differ from that language to the extent required to impose the specific obligations that the corresponding Articles of the applied LED demand be imposed.

(4) In these Regulations —

(a) the considerations specified in paragraphs (2); and

(b) the description, set out in paragraph (3), of the approach to giving domestic legislative effect to some provisions of the LED,

apply equally to the provisions specified in paragraph (5).

(5) Those provisions are —

(a) in Part 4, regulations 63 to 66 (data protection officers under the applied LED); and

(b) in Part 5, regulations 70 to 74 (transfers under the applied LED).

27 Processing to which this Part applies

(1) This Part applies to —

(a) the processing by a competent authority of personal data wholly or partly by automated means; and

(b) the processing by a competent authority otherwise than by automated means of personal data which forms part of a filing system or is intended to form part of a filing system.

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

(3) For the meaning of "competent authority", see Article 3(7) of the applied LED and regulation 28.

Definitions

28 Meaning of "competent authority"

(1) In this Part, "**competent authority**" (in keeping with Article 3(7) of the applied LED) means —

(a) a person specified in Schedule 1; and

(b) any other person if and to the extent that the person has statutory functions for any of the law enforcement purposes.

(2) The Council of Ministers may by regulations amend Schedule 1 —

(a) so as to add a person to, or remove a person from, the Schedule;

(b) so as to reflect any change in the name of a person specified in the Schedule.

(3) Regulations —

(a) under paragraph (2)(a); or

(b) made for the purposes of both paragraphs (2)(a) and (b),

are subject to the affirmative resolution procedure.

(4) Regulations under paragraph (2)(b) are subject to the negative resolution procedure.

(5) In this regulation, "statutory function" means a function under or by virtue of any enactment.

29 "The law enforcement purposes"

For the purposes of this Part, "**the law enforcement purposes**" are the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.

30 Meaning of "controller" and "processor"

(1) In this Part (as well as in Parts 4, 5 and 7 in so far as those Parts relate to processing of personal data by competent authorities), "**controller**" means the competent authority which, alone or jointly with others, —

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

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

(2) Where personal data are processed only —

(a) for purposes for which it is required by an enactment to be processed; and

(b) by means by which it is required by an enactment to be processed,

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

(3) In this Part (as well as in Parts 5 and 7 in so far as those Parts relate to processing of personal data by competent authorities), "**processor**" means any natural or legal person, public authority, agency or another body who processes personal data on behalf of the controller (other than a person who is an employee of the controller).

31 Other definitions

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

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

(3) "**Profiling**" means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

(4) "**Recipient**", in relation to any personal data, means any natural or legal person, public authority, agency or another body to whom the data are disclosed, whether a third party or not, but it does not include a public authority to whom disclosure is or may be made in the framework of a particular inquiry in accordance with the law.

CHAPTER 2

32 Principles relating to processing of personal data

The principles relating to the processing of personal data are as set out in Article 4(1) of the applied Law Enforcement Directive.

33 Safeguards: archiving

(1) This regulation applies in relation to the processing of personal data for a law enforcement purpose where the processing is necessary —

(a) for archiving purposes in the public interest;

(b) for scientific or historical research purposes; or

(c) for statistical purposes.

(2) The processing is not permitted if —

(a) it is carried out for the purposes of, or in connection with, measures or decisions with respect to a particular data subject; or

(b) it is likely to cause substantial damage or substantial distress to a natural person.

CHAPTER 3

34 Time-limits for storage and review: Article 5 of the applied LED

The controller or the processor, or both (as the case may be) must either —

(a) erase personal data upon the request of the data subject or in accordance with a requirement under any enactment; or

(b) review the need for the storage of personal data,

within 5 years of the date on which the data were first stored.

35 Distinction between different categories of data subject: Article 6 of the applied LED

(1) The controller must, where applicable and as far as possible, make a clear distinction between personal data of different categories of data subjects, such as —

(a) persons with regard to whom there are serious grounds for believing that they have committed or are about to commit a criminal offence;

(b) persons convicted of a criminal offence;

(c) victims of a criminal offence or persons with regard to whom certain facts give rise to reasons for believing that he or she could be the victim of a criminal offence; and

(d) other parties to a criminal offence, such as persons who might be called on to testify in investigations in connection with criminal offences or subsequent criminal proceedings, persons who can provide information on criminal offences, or contacts or associates of one of the persons referred to in subparagraph (a) or (b).

(2) In order to comply with paragraph (1), a controller has such powers as may be prescribed by the Council of Ministers.

Tynwald procedure – approval required.

36 Distinction between personal data and verification of quality of personal data: Article 7 of the applied LED

(1) Personal data based on facts must be distinguished, as far as possible, from personal data based on personal assessments.

(2) A competent authority must take all reasonable steps to ensure that personal data which are inaccurate, incomplete or no longer up to date are not transmitted or made available.

(3) In order to comply with paragraph (2), each competent authority must as far as possible —

(a) verify the quality of personal data before they are transmitted or made available; and

(b) in every transmission of personal data, add necessary information enabling the receiving competent authority to assess —

(i) the degree of accuracy, completeness and reliability of personal data; and

(ii) the extent to which they are up to date.

(4) In any case where it emerges that —

(a) incorrect personal data have been transmitted; or

(b) personal data have been unlawfully transmitted,

the controller or processor (as the case may be) must notify the recipient without delay and must act in accordance with paragraph (5).

(5) Where paragraph (4) applies, in accordance with regulation 45 the controller or processor (as the case may be) must, as appropriate to the circumstances, rectify or erase the personal data.

37 Lawfulness of processing: Article 8 of the applied LED

(1) Processing is lawful only if and to the extent that processing is —

(a) necessary for the performance of a task carried out by a competent authority for the purposes set out in Article 1(1) of the applied LED and regulation 29; and

(b) in accordance with any law of the Island that meets the requirements in paragraph (2).

(2) Those requirements are that the law must specify, at least —

(a) the objectives of the processing;

(b) the personal data to be processed; and

(c) the purposes of the processing.

(3) The conditions for processing are set out in Schedule 12.

(4) The requirements in paragraph (2)(b) are limited to law which has been enacted or amended after the commencement of these Regulations.

38 Specific processing conditions: Article 9 of the applied LED

(1) Personal data collected by competent authorities for the purposes set out in Article 1(1) of the applied LED must not be processed for purposes other than those set out in the said Article 1(1) unless such processing is authorised by the law of the Island.

(2) Where personal data are processed for purposes other than those set out in Article 1(1) of the applied LED, the provisions of the applied GDPR (as supplemented elsewhere in these Regulations) apply unless the processing is carried out in an activity which falls outside the scope of any portion of Union law that applies to the Island as part of the law of the Island.

(3) Where a competent authority is entrusted by law with the performance of tasks other than those performed for the purposes set out in Article 1(1), the applied GDPR (as supplemented elsewhere in these Regulations) applies to processing for such purposes, including for

archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, unless the processing is carried out in an activity which falls outside the scope of any portion of Union law that applies to the Island as part of the law of the Island.

(4) Where specific conditions for processing are imposed by law, the transmitting competent authority must inform the recipient of such personal data of those conditions and the requirement to comply with them.

(5) The transmitting competent authority must not apply conditions pursuant to paragraph (4) to recipients in other Member States or to agencies, offices and bodies established pursuant to Chapters 4 and 5 of Title V of the TFEU other than those applicable to similar transmissions of data within the Member State of the transmitting competent authority.

39 Processing of special categories of personal data: Article 10 of the applied LED

(1) Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation is prohibited.

This is subject to paragraph (2).

(2) The prohibition in paragraph (1) does not apply, and the processing of the data referred to in that paragraph will therefore be permitted only —

(a) where it is strictly necessary; and

(b) one of the following applies —

(i) the processing is authorised by the law of the Island;

(ii) the processing is for the purpose of protecting the vital interests of the data subject or of another natural person; or

(iii) the processing relates to data which are manifestly made public by the data subject.

40 Automated individual decision-making: Article 11 of the applied LED

(1) A decision based solely on automated processing, including profiling, which produces an adverse legal effect concerning the data subject or significantly affects him or her is prohibited unless paragraph (2) applies.

(2) The prohibition in paragraph (1) does not apply if the processing referred to in that paragraph is authorised by —

(a) Manx law; or

(b) Union or Member State law to which the controller is subject,

and which provides appropriate safeguards for the rights and freedoms of the data subject.

(3) The appropriate safeguards referred to in paragraph (2) must include at least the right to obtain human intervention on the part of the controller.

(4) Decisions referred to in paragraph (1) must not be based on special categories of personal data referred to in regulation 39, unless suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place.

(5) Profiling that results in discrimination against natural persons on the basis of special categories of personal data referred to in regulation 39 is prohibited.

CHAPTER 4

Rights of the data subject

41 Communication and modalities for exercising the rights of the data subject: Article 12 of the applied LED

(1) The controller must take reasonable steps to —

(a) provide to the data subject any information referred to in regulation 42; and

(b) make any communication with the data subject —

(i) with regard to regulations 40, 43 to 47 and 61; and

(ii) relating to processing,

in a concise, intelligible and easily accessible form, using clear and plain language.[4]

(2) The controller must provide the information referred to in paragraph (1) —

(a) by any appropriate means, including electronic means; and

(b) as a general rule, in the same form as the request.

(3) The controller must facilitate the exercise of the rights of the data subject under regulations 40 and 43 to 47.

(4) The controller must, without undue delay, inform the data subject in writing about the steps that have been taken or are being taken in pursuance of his or her request.[5]

(5) Information provided under regulation 42 and any communication made or action taken pursuant to regulations 40, 43 to 47 and 61 must be free of charge.

(6) Where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character, the controller may either —

(a) charge a reasonable fee, taking into account the administrative costs of providing the information or communication or taking the action requested; or

(b) refuse to act on the request.

(7) Where paragraph (6) applies, the controller must in writing demonstrate the manifestly unfounded or excessive character of the request —

(a) to the data subject; and

(b) to the Information Commissioner, on the Information Commissioner's request pursuant to an information notice under regulation 101.

(8) Where the controller has reasonable doubts concerning the identity of the natural person making a request referred to in Article 14 or 16 (or alternatively, either or both of regulations 43 and 45) of the applied LED, the controller may request the provision of additional information necessary to confirm the identity of the data subject.

42 Information to be given or made available to the data subject: Article 13 of the applied LED

(1) The controller must make available to the data subject at least the following information —

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

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

(c) the purposes of the processing for which the personal data are intended;

(d) the right to lodge a complaint with the Information Commissioner and the Information Commissioner's contact details; and

(e) the existence of the right to request from the controller access to and rectification or erasure of personal data and restriction of processing of the personal data concerning the data subject.

(2) In addition to the information referred to in paragraph (1), the controller must give to the data subject, in specific cases, the following further information to enable the exercise of his or her rights —

(a) the legal basis for the processing;

(b) the period for which the personal data will be stored, or, where that is not possible, the criteria used to determine that period;

(c) where applicable, the categories of recipients of the personal data, including in third countries or international organisations;

(d) where necessary, further information, in particular where the personal data are collected without the knowledge of the data subject.

(3) The Council of Ministers may by regulations permit the delay, restrict, or omit the provision of the information to the data subject pursuant to paragraph (2) to the extent that, and for as long as, such a measure constitutes a necessary and proportionate measure in a democratic society with due regard for the fundamental rights and the legitimate interests of the natural person concerned, in order to —

(a) avoid obstructing official or legal inquiries, investigations or procedures;

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

(c) protect public security;

(d) protect national security; or

(e) protect the rights and freedoms of others.

Tynwald procedure – approval required.

(4) For the purposes of Article 13 of the applied LED, the Council of Ministers may determine and by regulations prescribe categories of processing which may wholly or partly fall under any of the subparagraphs of paragraph (3).

43 Right of access by the data subject: Article 14 of the applied LED

(1) Subject to regulation 44, the data subject has the right to obtain from the controller, in writing and within the applicable time period, confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information —

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

(b) the categories of personal data concerned;

(c) the recipients or categories of recipients to whom the personal data have been disclosed, in particular recipients in third countries or international organisations;

(d) where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;

(e) the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject;

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

(g) communication of the personal data undergoing processing and of any available information as to their origin.[6]

(2) This paragraph defines "the applicable time period" for the purposes of this regulation and regulation 45 —

"the applicable time period" means the period of 1 month, or such longer period as may be specified in regulations, beginning with the relevant time;

"the relevant time" means the latest of the following —

(a) when the controller receives the request in question;

(b) when the controller receives the information (if any) requested in connection with a request under these Regulations or the applied GDPR;

(c) when the fee (if any) charged in connection with the request under these Regulations or the applied GDPR is paid.

(3) The power to make regulations referred to in the definition of "the applicable time period" is exercisable by the Council of Ministers.

Tynwald procedure – negative.

(4) Those regulations may not specify a period which is longer than 3 months.

44 Limitations to the right of access: Article 15 of the applied LED

(1) The Council of Ministers may by regulations restrict, wholly or partly, the data subject's right of access to the extent that, and for so long as such a partial or complete restriction constitutes a necessary and proportionate measure in a democratic society with due regard for the fundamental rights and legitimate interests of the natural person concerned, in order to —

(a) avoid obstructing official or legal inquiries, investigations or procedures;

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

(c) protect public security;

(d) protect national security; or

(e) protect the rights and freedoms of others.

Tynwald procedure – approval required.

(2) The Council of Ministers may determine and by regulations prescribe categories of processing which may wholly or partly fall under subparagraphs (a) to (e) of paragraph (1).

Tynwald procedure – approval required.

(3) In the cases referred to in paragraphs (1) and (2), the controller must inform the data subject, without undue delay, in writing of any refusal or restriction of access and of the reasons for the refusal or the restriction. Such information may be omitted where the provision of it would undermine a purpose under paragraph (1).

(4) The controller must —

(a) inform the data subject of the possibility of lodging a complaint with the Information Commissioner or seeking a judicial remedy;

(b) document the factual or legal reasons on which its decision under this paragraph is based; and

(c) make the information referred to in subparagraph (b) available to the Information Commissioner.

45 Right to rectification or erasure of personal data and restriction of processing: Article 16 of the applied LED

(1) The data subject has the right —

(a) to obtain from the controller without undue delay the rectification of inaccurate personal data relating to him or her;

(b) taking into account the purposes of the processing, to have incomplete personal data completed, including by means of providing a supplementary statement;

(c) subject to paragraphs (2) and (3), to obtain from the controller the erasure of personal data concerning him or her where —

(i) processing infringes the provisions adopted in regulations 32, 37 or 39; or

(ii) personal data must be erased in order to comply with a legal obligation to which the controller is subject.[7]

(2) The controller must, within "the applicable time period" as defined in regulation 43(2), erase personal data which to which the conditions set out in paragraph (1)(c)(i) and (ii) apply.

This duty is subject to paragraph (3).[8]

(3) Instead of erasure, the controller must restrict processing where —

(a) the accuracy of the personal data are contested by the data subject and their accuracy or inaccuracy cannot be ascertained; or

(b) the personal data must be maintained for the purposes of evidence.

(4) Where processing is restricted pursuant to paragraph (3)(a), the controller must inform the data subject before lifting the restriction of processing.

(5) The controller must inform the data subject in writing of any refusal of rectification or erasure of personal data or restriction of processing and of the reasons for the refusal.

(6) The Council of Ministers may by regulations restrict, wholly or partly, the obligation to provide such information to the extent that such a restriction constitutes a necessary and proportionate measure in a democratic society with due regard for the fundamental rights and legitimate interests of the natural person concerned in order to —

(a) avoid obstructing official or legal inquiries, investigations or procedures;

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

(c) protect public security;

(d) protect national security; or

(e) protect the rights and freedoms of others.

Tynwald procedure – approval required.

(7) The controller must —

(a) inform the data subject of the possibility of lodging a complaint with the Information Commissioner or seeking a judicial remedy;

(b) communicate the rectification of inaccurate personal data to the competent authority from which the inaccurate personal data originated;

(c) where —

(i) personal data have been rectified or erased; or

(ii) processing of personal data has been restricted pursuant to paragraphs (1) to (4),

provide for the controller to notify the recipients.

(8) Recipients notified in accordance with paragraph (7)(c) must rectify or erase the personal data or restrict processing of the personal data under their responsibility.

46 Exercise of rights by data subject and verification by the Information Commissioner: Article 17 of the applied LED

(1) In the cases referred to in regulations 42(3), 44(3) and 45(5) to (7), the rights of the data subject may also be exercised through the Information Commissioner.

(2) The controller must inform the data subject of the possibility of exercising his or her rights through the Information Commissioner pursuant to paragraph (1).

(3) Where the right referred to in paragraph (1) is exercised, the Information Commissioner must inform the data subject —

(a) that, at least, all necessary verifications or a review by the Information Commissioner have taken place; and

(b) of his or her right to seek a judicial remedy.

47 Rights of the data subject in criminal investigations and proceedings: Article 18 of the applied LED

The rights conferred on the data subject by regulations 42, 43 and 45 may be exercised where personal data are contained in a judicial decision or record or case file processed in the course of criminal investigations and proceedings.

CHAPTER 5

Controller and processor

48 Obligations of the controller: Article 19 of the applied LED

(1) The controller must implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with the applied LED.

This is subject to paragraph (2).

(2) In complying with paragraph (1), the controller must take into account the nature, scope, context and purposes of the processing, as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons

(3) The controller must ensure that the measures taken in accordance with paragraph (1) —

(a) include the implementation of appropriate data protection policies by the controller (this is subject to paragraph (4)); and

(b) are reviewed every 5 years and updated if necessary.

(4) Paragraph (3)(a) need not be complied with where compliance would be disproportionate in relation to the processing activities.

49 Data protection by design and by default: Article 20 of the applied LED

(1) The controller must —

(a) implement appropriate technical and organisational measures such as pseudonymisation, which are designed to implement data protection principles (such as data minimisation) in an effective manner; and

(b) integrate the necessary safeguards into the processing.

This is subject to paragraph (2).

(2) In complying with paragraph (1), the controller must take into account —

(a) the best technological solutions that are currently available;

(b) the cost of implementation; and

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

(d) the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, both —

(i) at the time of the determination of the means for processing; and

(ii) at the time of the processing itself.

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

(4) The obligation under paragraph (3) applies to —

(a) the amount of personal data collected;

(b) the extent of the processing of the personal data;

(c) the period of storage of the personal data; and

(d) the accessibility of the personal data.

(5) The measures referred to in paragraph (3) must ensure that by default personal data are not, without the controller's intervention, made accessible to an indefinite number of persons.

50 Joint controllers: Article 21 of the applied LED

(1) Where two or more controllers jointly determine the purposes and means of processing, they are joint controllers for the purposes of these Regulations and the applied LED.

(2) Joint controllers must in a transparent manner determine their respective responsibilities for compliance with the applied LED and these Regulations, in particular as regards the exercise of the rights of the data subject and their respective duties to provide the information required by regulation 42, by means of an arrangement between them unless, and in so far as, the respective responsibilities of the controllers are determined by Union or Member State law to which the controllers are subject.

(3) Subject to paragraph (4), the arrangement provided for in paragraph (2) must designate the contact point for data subjects when taking steps to exercise their rights.

(4) The joint controllers must decide between themselves which of them can act as a single contact point for data subjects to exercise their rights.

(5) Irrespective of the arrangement reached in accordance with paragraphs (2) to (4), a data subject may exercise his or her rights under these Regulations in respect of and against each of the joint controllers.

51 Processor: Article 22 of the applied LED

(1) Where processing is to be carried out on behalf of a controller, the controller may use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of the applied LED and these Regulations and ensure the protection of the rights of the data subject.

(2) The processor must not engage another processor without prior specific or general written authorisation by the controller.

(3) In the case of a general written authorisation, the processor must inform the controller of any intended changes concerning the addition or replacement of other processors, thereby giving the controller the opportunity to object to such changes.

(4) The processing by a processor must be governed by a contract or other legal act, and such contract or other legal act must —

(a) be binding on the processor with regard to the controller; and

(b) set out —

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

(ii) the nature and purpose of the processing;

(iii) the type of personal data;

(iv) the categories of data subjects; and

(v) the obligations and rights of the controller.[9]

(5) The contract or other legal act must also stipulate, in particular, that the processor —

(a) acts only on instructions from the controller;

(b) ensures that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;

(c) assists the controller by any appropriate means to ensure compliance with the provisions on the data subject's rights;

(d) at the choice of the controller, deletes or returns all the personal data to the controller after the end of the provision of data processing services, and deletes copies unless Manx law requires storage of the personal data;

(e) makes available to the controller all information necessary to demonstrate compliance with this paragraph; and

(f) complies with the conditions referred to in paragraphs (2) to (4) for engaging another processor.

(6) The contract or other legal act must be in writing, which may be in an electronic form.

(7) If a processor determines, in infringement of the applied LED or these Regulations, the purposes and means of the processing, that processor will for the purposes of the applied LED or these Regulations be considered to be a controller in respect of that processing.

52 Processing under the authority of the controller or processor: Article 23 of the applied LED

(1) A person listed in paragraph (2) must not process personal data unless required to do so by Manx law.

(2) The persons to whom paragraph (1) applies are —

(a) the processor; and

(b) any person acting under the authority of the controller or of the processor.

53 Controller's records of processing activities: Article 24 of the applied LED

(1) A controller must maintain a record of all categories of processing activities under its responsibility.

(2) A record under paragraph (1) must contain all of the following —

(a) the name and contact details of the controller and, where applicable, the joint controller and the data protection officer;

(b) the purposes of the processing;

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

(d) a description of the categories of data subject and of the categories of personal data;

(e) where applicable, the use of profiling;

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

(g) an indication of the legal basis for the processing operation, including transfers, for which the personal data are intended;

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

(i) where possible, a general description of the technical and organisational security measures referred to in regulation 59(1) and (2).

(3) A controller must —

(a) ensure that the records required by this regulation are kept in writing, which may be in electronic form; and

(b) make the records available to the Information Commissioner on request.

54 Processor's records of processing activities: Article 24 of the applied LED

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

(2) A record under paragraph (1) must contain all of the following —

(a) the name and contact details of the processor or processors, of each controller on behalf of which the processor is acting and, where applicable, the data protection officer;

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

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

(d) where possible, a general description of the technical and organisational security measures referred to in regulation 59(1) and (2).

(3) A processor must —

(a) ensure that the records required by this regulation are kept in writing, which may be in electronic form; and

(b) make the records available to the Information Commissioner on request.

55 Logging: Article 25 of the applied LED

(1) A controller and a processor, or both (as the case may be), must keep a log for at least the following processing operations in automated processing systems —

(a) collection;

(b) alteration;

(c) consultation;

(d) disclosure (including transfers);

(e) combination; and

(f) erasure.

(2) The logs in respect of consultation and disclosure must make it possible to establish the justification, date and time of such operations and, as far as possible, the identification of the person who consulted or disclosed personal data, and the identity of the recipients of such personal data.

(3) Logs must be used solely for verification of the lawfulness of processing, self-monitoring, ensuring the integrity and security of the personal data, and for criminal proceedings.

(4) The controller and the processor must make the logs available to the Information Commissioner on request.

56 Cooperation with the Information Commissioner: Article 26 of the applied LED

Every controller and every processor must cooperate, on request, with the Information Commissioner in the performance of the Information Commissioner's tasks.

57 Data protection impact assessment: Article 27 of the applied LED

(1) Having regard to the considerations listed in paragraph (2), a controller must carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. This must be done prior to the processing.

(2) The considerations are —

(a) the type of processing (in particular, whether it uses new technologies);

(b) the nature, scope, context and purposes of the processing;

(c) whether the processing, in light of subparagraph (a) or (b), is likely to result in a high risk to the rights and freedoms of natural persons.

(3) The assessment required by paragraph (1) must contain at least —

(a) a general description of the envisaged processing operations;

(b) an assessment of the risks to the rights and freedoms of data subjects;

(c) the measures envisaged to address those risks;

(d) safeguards;

(e) security measures and mechanisms.

(4) The required minimum content (as listed in paragraph (3)) must —

(a) be designed —

(i) to ensure the protection of personal data; and

(ii) with due regard for the rights and legitimate interests of data subjects and other persons concerned; and

(b) demonstrate compliance with the applied LED.

(5) This regulation does not in any way limit the application of Article 35 (data protection impact assessment) or Article 36 (prior consultation) of the applied GDPR.

58 Prior consultation of the Information Commissioner: Article 28 of the applied LED

(1) Where either of the conditions listed in paragraph (2) is met, a controller or a processor, as the case may be, must consult the Information Commissioner prior to processing which will form part of a new filing system to be created.

(2) The conditions are —

(a) a data protection impact assessment as required by regulation 57 indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk; or

(b) the type of processing, in particular, where using new technologies, mechanisms or procedures, involves a high risk to the rights and freedoms of data subjects.

(3) The Information Commissioner may establish a list of the processing operations that are to be subject to consultation under paragraph (1).

(4) A controller must provide the Information Commissioner with the data protection impact assessment pursuant to regulation 57 and, on request, with any other information to allow the Information Commissioner to make an assessment of the compliance of the processing and in particular of the risks for the protection of personal data of the data subject and of the related safeguards.

(5) Where the condition in paragraph (6) are met, the Information Commissioner must provide, within a period of 6 weeks of receipt of the request for consultation, written advice to the controller and, where applicable, to the processor, and may use any of the Information Commissioner's powers referred to in Article 47 of the applied LED.

(6) The condition referred to in paragraph (5) is that the Information Commissioner is of the opinion that the intended processing referred to in paragraph (1) would infringe the provisions of this Part, in particular, where the controller has insufficiently identified or mitigated the risk.

(7) The period referred to in paragraph (5) may be extended by a month, taking into account the complexity of the intended processing.

(8) The Information Commissioner must inform the controller and, where applicable, the processor of any such extension within one month of receipt of the request for consultation, together with the reasons for the delay.

Security of personal data

59 Security of processing: Article 29 of the applied LED

(1) Having regard for the considerations listed in paragraph (2), a controller and a processor must implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk involved in the processing of personal data, in particular as regards the processing of special categories of personal data referred to in Article 10 of the applied LED.

(2) The considerations referred to in paragraph (1) are —

(a) the best technological solutions that are currently available;

(b) the costs of implementation;

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

(d) the risk of varying likelihood and severity for the rights and freedoms of natural persons.

(3) In respect of automated processing, every controller and every processor must, after evaluating the risks, implement measures designed to —

(a) deny unauthorised persons access to processing equipment used for processing (‘equipment control’);

(b) prevent the unauthorised reading, copying, modification or removal of data media (‘data media control’);

(c) prevent the unauthorised input of personal data and the unauthorised inspection, modification or deletion of stored personal data (‘storage control’);

(d) prevent the use of automated processing systems by unauthorised persons using data communication equipment (‘user control’);

(e) ensure that persons authorised to use an automated processing system have access only to the personal data covered by their access authorisation (‘data access control’);

(f) ensure that it is possible to verify and establish the bodies to which personal data have been or may be transmitted or made available using data communication equipment (‘communication control’);

(g) ensure that it is subsequently possible to verify and establish which personal data have been put into automated processing systems and when and by whom the personal data were input (‘input control’);

(h) prevent the unauthorised reading, copying, modification or deletion of personal data during transfers of personal data or during transportation of data media ('transport control');

(i) ensure that installed systems may, in the case of interruption, be restored ('recovery'); and

(j) ensure that the functions of the system perform, that the appearance of faults in the functions is reported ('reliability') and that stored personal data cannot be corrupted by means of a malfunctioning of the system ('integrity').

60 Notification of a personal data breach to the Information Commissioner: Article 30 of the applied LED

(1) In the case of a personal data breach, the controller must notify the personal data breach to the Information Commissioner, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons.

This is subject to paragraph (2).

(2) Notification under paragraph (1) must be without undue delay and, where feasible, not later than 72 hours after the controller became aware of the personal data breach. Where such notification is made more than 72 hours after the controller became aware of the breach, the notification must be accompanied by a statement of the reasons for the delay.

(3) A processor must notify the controller without undue delay after becoming aware of a personal data breach.

(4) A notification under paragraph (1) must, at least, —

(a) describe 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) communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;

(c) describe the likely consequences of the personal data breach; and

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

(5) Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.

(6) Every controller must document any personal data breach referred to in paragraph (1). Such documentation must comprise the facts relating to the personal data breach, its effects and the remedial action taken, and

must be made available to the Information Commissioner on request with sufficient detail to permit the Information Commissioner to verify compliance with Article 30 of the applied LED.

(7) Where a personal data breach involves personal data that have been transmitted by or to the controller in another Member State, the Information Commissioner must without delay communicate the information referred to in paragraph (4) to that controller.

61 Communication of a personal data breach to the data subject: Article 31 of the applied LED

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

(2) The communication to the data subject referred to in paragraph (1) must describe in clear and plain language the nature of the personal data breach and must contain at least the information and measures referred to in subparagraphs (b), (c) and (d) of regulation 60(4).

(3) The communication to the data subject referred to in paragraph (1) is not required if any of the following conditions is met —

(a) the controller has implemented appropriate technological and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption; or

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

(c) it would involve disproportionate effort.

(4) In the case described in paragraph (3)(c), the controller must instead make a public statement or otherwise engage in public communication that has the effect of informing data subjects of the breach in a manner and to an extent that, in the opinion of the Information Commissioner, is appropriate in the circumstances.

(5) If the controller has not already communicated the personal data breach to the data subject, the Information Commissioner, having considered the likelihood of the personal data breach resulting in a high risk, may require it to do so, or may decide that any of the conditions referred to in paragraph (3) is met.

(6) The communication to the data subject referred to in paragraph (1) may be delayed, restricted or omitted subject to the conditions and on the

grounds referred to in Article 13(3) of the applied LED and regulation 42(3).

PART 4 – DATA PROTECTION OFFICERS

Data protection officers under the applied GDPR

62 Designation of data protection officers under the applied GDPR

The provisions on designation, position and tasks of data protection officers are as set out in Articles 37 to 39 of the applied GDPR.

Data protection officers under the applied LED

63 General provision on designation of the data protection officer: Article 32 of the applied LED

(1) The controller must designate a data protection officer.

This is subject to paragraph (2).

(2) Paragraph (1) does not apply to courts and other independent judicial authorities when acting in their judicial capacity.

(3) The controller must publish the contact details of the data protection officer and communicate them to the Information Commissioner.

64 Designation of data protection officers for competent authorities: Article 32 of the applied LED

(1) Any two or more competent authorities may designate a single data protection officer to serve all of them.

(2) In complying with paragraph (1), the competent authorities must take account of their organisational structure and size.

65 Position of the data protection officer: Article 33 of the applied LED

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

(2) The controller must support the data protection officer in performing the tasks referred to regulation 66 by providing, —

(a) access to personal data and processing operations; and

(b) resources necessary —

(i) to carry out those tasks; and

(ii) to maintain his or her expert knowledge.

66 Tasks of the data protection officer: Article 34 of the applied LED

The controller must entrust to the data protection officer at least the following tasks —

(a) to inform and advise the controller and the employees who carry out processing of their obligations pursuant to the applied LED and other data protection legislation;

(b) to monitor compliance with the applied LED, with data protection legislation and with the policies of the controller in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits;

(c) to provide advice where requested as regards the data protection impact assessment and monitor its performance pursuant to regulation 57;

(d) to cooperate with the Information Commissioner;

(e) to act as the contact point for the Information Commissioner on issues relating to processing, including the prior consultation referred to in regulation 58, and to consult, where appropriate, with regard to any other matter.

67 Data protection officer for applied GDPR and applied LED

(1) In keeping with Recitals (10) and (11) of the applied LED, a competent authority may process personal data for purposes other than those of the applied LED, in which case the applied GDPR would apply to such processing.

(2) On the basis of paragraph (1), a controller may designate a single data protection officer to perform the associated functions under both the applied GDPR and the applied LED only where the controller —

(a) is a competent authority; and

(b) also processes personal data for purposes other than those of the applied LED.

PART 5 – TRANSFERS OF PERSONAL DATA TO THIRD COUNTRIES OR INTERNATIONAL ORGANISATIONS

Transfers under the applied GDPR

68 General principles for cross-border data transfers

(1) A controller or a processor must not transfer personal data for processing or in circumstances where the controller or processor knew or should have known that it will be processed after the transfer, to a third country or an international organisation unless that country or organisation ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

(2) The level of protection referred to in paragraph (1) is adequate if —

(a) the European Commission has so decided, by means of an implementing act under Article 45 of the GDPR;

(b) there are safeguards in place that meet the requirements of Article 46; or

(c) the transfer falls within the exceptions set out in Schedule 10.

(3) The Council of Ministers may by regulations —

(a) amend Schedule 10;

(b) make further provision about international transfers of data.

Tynwald procedure – approval required.

69 Transfer subject to other appropriate safeguards

(1) In the absence of an adequacy decision under Article 45 (or safeguards in place that meet the requirements of Article 46(2)) of the GDPR, a controller or processor may transfer personal data to a third country or an international organisation only if the controller or processor has provided other appropriate safeguards in accordance with this regulation, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available in that country or organisation.

(2) Subject to specific authorisation from the Information Commissioner and where there is a mechanism for data subjects to enforce their data subject rights and obtain effective legal remedies against the controller, processor or recipient of that personal data in the jurisdiction concerned, other appropriate safeguards referred to in paragraph (1) may also be provided for by —

(a) contractual clauses between the controller or processor and the controller, processor or the recipient of the personal data in the third country or international organisation; or

(b) where both the transferor and the controller, processor or recipient of the personal data in the third country or international organisation concerned are public authorities, provisions in administrative arrangements between those public authorities that include enforceable and effective data subject rights.

(3) In determining whether to authorise a transfer under this regulation, the Information Commissioner must have regard to factors that include, but are not limited to, any opinions or decisions of the European Data Protection Board under Article 64, 65 or 66 of the GDPR that appear to the Information Commissioner to be relevant.

Transfers under the applied LED

70 General principles for transfers of personal data: Article 35 of the applied LED

(1) Subject to paragraph (2), competent authorities may transfer personal data which —

(a) are undergoing processing; or

(b) are intended for processing after transfer to a third country or to an international organisation, including for onward transfers to another third country or international organisation.

(2) Paragraph (1) applies only where the following conditions are met —

(a) the transfer is necessary for the purposes set out in Article 1(1) of the applied LED;

(b) the personal data are transferred to a controller in a third country or international organisation that is an authority competent for the purposes referred to in Article 1(1) of the applied LED;

(c) where personal data are transferred or made available from another Member State, that Member State has given its prior authorisation to the transfer in accordance with its national law;

(d) the European Commission has adopted an adequacy decision pursuant to Article 36 of the applied LED, or in the absence of such a decision, appropriate safeguards have been provided or exist pursuant to Article 37 of the applied LED, or, in the absence of an adequacy decision pursuant to Article 36 of the applied LED and of appropriate safeguards in accordance with Article 37 of the applied LED, derogations for specific situations apply pursuant to Article 38 of the applied LED; and

(e) in the case of an onward transfer to another third country or international organisation, the competent authority that carried out the original transfer or another competent authority of the same Member State authorises the onward transfer, after taking

into due account all relevant factors, including the seriousness of the criminal offence, the purpose for which the personal data were originally transferred and the level of personal data protection in the third country or an international organisation to which personal data are onward transferred.

(3) Transfers without the prior authorisation by another Member State in accordance with paragraph (2)(c) may only take place if the transfer of the personal data is necessary for the prevention of an immediate and serious threat to public security of a Member State or a third country or to essential interests of a Member State and the prior authorisation cannot be obtained in good time.

(4) In the case described in paragraph (3), the authority responsible for giving prior authorisation must be informed without delay.

(5) For the avoidance of doubt, all provisions of this Part must be applied in order to ensure that the level of protection of natural persons required by the applied LED is not undermined.

71 Transfers on the basis of an adequacy decision: Article 36 of the applied LED

(1) A transfer of personal data to a third country or an international organisation may take place where the Commission has decided that the third country, a territory or one or more specified sectors within that third country, or the international organisation in question ensures an adequate level of protection.

(2) A transfer under paragraph (1) does not require any specific authorisation.

(3) A decision pursuant to the applied LED is without prejudice to transfers of personal data to the third country, the territory or one or more specified sectors within that third country, or the international organisation in question pursuant to Articles 37 and 38 of the applied LED.

72 Transfers subject to appropriate safeguards: Article 37 of the applied LED

(1) A transfer of personal data to a third country or an international organisation may take place where —

(a) appropriate safeguards with regard to the protection of personal data are provided for in a legally binding instrument; or

(b) the controller has assessed all the circumstances surrounding the transfer of personal data and concludes that appropriate safeguards exist with regard to the protection of personal data.

(2) The controller must inform the Information Commissioner about categories of transfers under paragraph (1)(b).

(3) When a transfer is based on paragraph (1)(b) —

(a) such a transfer must be documented; and

(b) the documentation must be made available to the Information Commissioner on request, including —

(i) the date and time of the transfer;

(ii) information about the receiving competent authority;

(iii) the justification for the transfer; and

(iv) the personal data transferred.

73 Derogations for specific situations: Article 38 of the applied LED

(1) In the absence of an adequacy decision pursuant to Article 36 of the applied LED, or of appropriate safeguards pursuant to Article 37 of the applied LED, a transfer or a category of transfers of personal data to a third country or an international organisation may take place only on the condition that the transfer is necessary for any of the purposes specified in paragraph (2).

(2) Those purposes are —

(a) in order to protect the vital interests of the data subject or another person;

(b) to safeguard the legitimate interests of the data subject, where the law of the Member State transferring the personal data so provides;

(c) for the prevention of an immediate and serious threat to public security of a Member State or a third country;

(d) in individual cases for the purposes set out in Article 1(1) of the applied LED; or

(e) in an individual case for the establishment, exercise or defence of legal claims relating to the purposes set out in Article 1(1) of the applied LED.

(3) Personal data must not be transferred if the transferring competent authority determines that fundamental rights and freedoms of the data subject concerned override the public interest in the transfer set out in paragraph (2)(d) and (e).

(4) Where a transfer is for any of the purposes specified in paragraph (2) —

(a) such a transfer must be documented; and

(b) the documentation must be made available to the Information Commissioner on request, including —

(i) the date and time of the transfer;

(ii) information about the receiving competent authority;

(iii) the justification for the transfer; and

(iv) the personal data transferred.

74 Transfers of personal data to recipients established in third countries: Article 39 of the applied LED

(1) By way of derogation from Article 35(1)(b) of the applied LED and without prejudice to any international agreement referred to in paragraph (3), the competent authorities referred to in Article 3(7)(a) of the applied LED, in individual and specific cases, may transfer personal data directly to recipients established in third countries only if —

(a) the other provisions of the applied LED are complied with; and

(b) all the conditions specified in paragraph (2) are fulfilled.

(2) The conditions referred to in paragraph (1)(b) are as follows —

(a) the transfer is strictly necessary for the performance of a task of the transferring competent authority as provided for by Union or Member State law for the purposes set out in Article 1(1) of the applied LED;

(b) the transferring competent authority determines that no fundamental rights and freedoms of the data subject concerned override the public interest necessitating the transfer in the case at hand;

(c) the transferring competent authority considers that the transfer to an authority that is competent for the purposes referred to in Article 1(1) of the applied LED in the third country is ineffective or inappropriate, in particular because the transfer cannot be achieved in good time;

(d) the authority that is competent for the purposes referred to in Article 1(1) of the applied LED in the third country is informed without undue delay, unless this is ineffective or inappropriate;

(e) the transferring competent authority informs the recipient of the specified purpose or purposes for which the personal data are only to be processed by the latter provided that such processing is necessary.

(3) An international agreement referred to in paragraph (1) must be a bilateral or multilateral international agreement in force between Member States and third countries in the field of judicial cooperation in criminal matters and police cooperation.

(4) The transferring competent authority must inform the Information Commissioner about transfers under Article 39 of the applied LED.

(5) Where a transfer is based on paragraph (1), that transfer must be documented.

Regulations for transfers of personal data under the applied GDPR

75 Power to make regulations for transfers under the applied GDPR

(1) The Council of Ministers may by regulations specify, for the purposes of Article 49(1)(d) of the applied GDPR —

(a) circumstances in which a transfer of personal data to a third country or international organisation is to be taken to be necessary for important reasons of public interest; and

(b) circumstances in which a transfer of personal data to a third country or international organisation which is not required by an enactment is not to be taken to be necessary for important reasons of public interest.

Tynwald procedure – laying only.

(2) The Council of Ministers may by regulations restrict the transfer of a category of personal data to a third country or international organisation where —

(a) the third country or international organisation is not the subject of a favourable adequacy decision under Article 45(3) of the GDPR; and

(b) the Council of Ministers considers the restriction to be necessary for important reasons of public interest.

Tynwald procedure – laying only.

PART 6 – THE INFORMATION COMMISSIONER

76 The Information Commissioner

(1) There continues to be an Information Commissioner.

(2) Schedule 2 to the *Freedom of Information Act 2015* continues to have effect.

General functions

77 General functions under the applied GDPR and safeguards

(1) The Information Commissioner is the supervisory authority in the Island for the purposes of Article 51 of the applied GDPR.

(2) General functions are conferred on the Information Commissioner by the following provisions of the applied GDPR —

(a) Article 57 (tasks); and

(b) Article 58 (powers).

(3) The Information Commissioner's functions in relation to the processing of personal data to which the applied GDPR applies include —

(a) a duty to advise Tynwald, a Department or Statutory Board and other institutions and bodies on legislative and administrative measures relating to the protection of natural persons' rights and freedoms with regard to the processing of personal data; and

(b) a power to issue, on the Information Commissioner's own initiative or on request, opinions to Tynwald, a Department or Statutory Board, or other institutions and bodies as well as to the public on any issue related to the protection of personal data.

(4) The Information Commissioner's functions under Article 58 of the applied GDPR are subject to the safeguards in paragraphs (5) to (9).

(5) The Information Commissioner's power under Article 58(1)(a) of the applied GDPR may be exercised by giving an information notice under regulation 101.

(6) The Information Commissioner's power under Article 58(1)(b) of the applied GDPR may be exercised —

(a) by the Information Commissioner, in accordance with regulation 104 (that is, by means of an assessment notice); or

(b) by an approved person, in accordance with regulation 78.

(7) The Information Commissioner's powers under Article 58(1)(e) and (f) of the applied GDPR may be exercised —

(a) in accordance with Schedule 4 (see regulation 111); or

(b) to the extent that they are exercised in conjunction with the power under Article 58(1)(b) of the applied GDPR, in accordance with regulation 104 (that is, by means of an assessment notice).

(8) The following powers are exercisable only by giving an enforcement notice under regulation 106 —

(a) the Information Commissioner's powers under Article 58(2)(c) to (g) and (j) of the applied GDPR;

(b) the Information Commissioner's power under Article 58(2)(h) of the applied GDPR to order a certification body to withdraw, or not to issue, a certification under Articles 42 and 43 of the applied GDPR.

(9) The Information Commissioner's powers under Articles 58(2)(i) and 83 (administrative fines) of the applied GDPR are exercisable only by giving a penalty notice under regulation 112.

(10) This regulation is without prejudice to other functions conferred on the Information Commissioner, whether by the applied GDPR, these Regulations, or otherwise.[10]

78 Power to require data protection audits

(1) This regulation applies only where the circumstances make it reasonably impracticable for the Information Commissioner to conduct an audit in accordance with Article 58(1)(b) of the applied GDPR and regulation 77(6) of these Regulations.

(2) Where this regulation applies, the Information Commissioner may instruct a controller or processor —

(a) to engage, for the purpose of conducting the audit, a person—

(i) who is suitably qualified and experienced; and

(ii) with whom the controller or processor has agreed terms (including as to remuneration, which must be at the expense of the controller or processor);

(iii) who meets with the approval of the Information Commissioner (such approval to be signified in writing by the Information Commissioner);

(b) to ensure that the Information Commissioner is promptly furnished with a report on the findings of the audit,

and, subject to the right of appeal in paragraph (5), the controller or processor must comply with this instruction within the time limit stated in the terms of reference specified in accordance with paragraph (3).

(3) The terms of reference for the audit referred to in paragraph (2) must be specified by the Information Commissioner.

(4) The Information Commissioner's approval referred to in paragraph (2)(a) must not be unreasonably withheld.

(5) A controller or processor aggrieved by an instruction given by the Information Commissioner under paragraph (2) may appeal to the Tribunal. The following provisions apply to any such appeal —

(a) where an appeal is filed, the appellant need not comply with the instruction in question until the appeal has been —

(i) decided against the appellant; or

(ii) abandoned without a determination having been made;

(b) the Tribunal may call upon the Information Commissioner to provide evidence that satisfies the Tribunal as to why —

(i) it is reasonably impracticable for the Information Commissioner to conduct the audit pursuant to paragraph (1);

(ii) the Information Commissioner has withheld approval pursuant to paragraph (4); or

(iii) the terms of reference for the audit specified by the Information Commissioner pursuant to paragraph (3) are justified;

(c) after hearing an appeal, the Tribunal may —

(i) uphold the instruction of the Information Commissioner and order the appellant to comply with it;

(ii) modify the instruction to whatever extent it considers appropriate; or

(iii) overrule the Information Commissioner's instruction.

(6) The Information Commissioner may publish a list of persons the Information Commissioner considers suitably qualified and experienced to conduct audits. Any such publication will not constitute satisfaction of the requirement imposed by paragraph (2)(a)(iii).[11]

79 Other general functions

(1) The Information Commissioner, —

(a) is to be the supervisory authority in the Island for the purposes of Article 41 of the applied LED (as permitted by Article 41(3)); and

(b) is to continue to be the designated authority in the Island for the purposes of Article 13 of the Data Protection Convention.

(2) For the purposes of the applied LED (see Article 42) and without limiting the applicability of equivalent provisions in Article 52 of the applied GDPR, the Information Commissioner, —

(a) must act with complete independence in performing the Information Commissioner's tasks and exercising the Information Commissioner's powers in accordance with the applied LED;

(b) in the performance of the Information Commissioner's tasks and in exercise of the Information Commissioner's powers in accordance with the applied LED, must —

(i) remain free from external influence, whether direct or indirect; and

(ii) neither seek nor take instructions from anybody;

(c) must refrain from any action incompatible with the Information Commissioner's duties; and

(d) during the Information Commissioner's term in office, must not engage in any incompatible occupation, whether gainful or not.

(3) This regulation is without prejudice to other functions conferred on the Information Commissioner, whether by these Regulations or otherwise.

80 Competence in relation to courts, etc.

Nothing in these Regulations permits or requires the Information Commissioner to exercise functions in relation to the processing of personal data by —

(a) a natural person acting in a judicial capacity;

(b) a court or tribunal acting in its judicial capacity; or

(c) a natural person or body acting in judicial proceedings pursuant to a Manx enactment conferring judicial functions upon that natural person or body.

(and see also Article 55(3) of the applied GDPR).

International role

81 Co-operation and mutual assistance

(1) In the applied GDPR, Article 50 requires the Information Commissioner to take appropriate steps to develop international cooperation for the protection of personal data.

(2) Article 40 of the applied LED requires the Information Commissioner to take appropriate steps to develop international cooperation for the protection of the personal data for which the applied LED makes provision.

(3) Schedule 3 makes provision as to the functions to be carried out by the Information Commissioner for the purposes of Article 13 of the Data Protection Convention (co-operation between parties).

82 Inspection of personal data in accordance with international obligations

(1) The Information Commissioner may inspect personal data where the inspection is necessary in order to discharge an international obligation of the Island, subject to the restriction in paragraph (2).

(2) The power is exercisable only if the personal data, —

(a) is processed wholly or partly by automated means; or

(b) is processed otherwise than by automated means and forms part of a filing system or is intended to form part of a filing system.

(3) The power under paragraph (1) includes power to inspect, operate and test equipment which is used for the processing of personal data.

(4) Before exercising the power under paragraph (1), the Information Commissioner must by written notice inform the controller and any processor that the Information Commissioner intends to do so.

(5) Paragraph (4) does not apply if the Information Commissioner considers that the case is urgent.

(6) It is an offence, —

(a) intentionally to obstruct a person exercising the power under paragraph (1); or

(b) to fail without reasonable excuse to give a person exercising that power any assistance the person may reasonably require.

(See regulation 141(1), which specifies the penalty for offences under this regulation.)

83 Further international role

(1) The Information Commissioner must carry out data protection functions which the Council of Ministers directs the Information Commissioner to carry out for the purpose of enabling a Department or Statutory Board to give effect to an international obligation of the Island.

(2) The Information Commissioner may provide an authority carrying out data protection functions under the law of a British overseas territory with assistance in carrying out those functions.

(3) The Council of Ministers may direct that assistance under paragraph (2) is to be provided on terms, including terms as to payment, specified or approved by the Council of Ministers.

(4) In this regulation, —

"assistance" includes assistance in the form of notification, complaint referral, investigative assistance and information exchange;

"data protection functions" means functions relating to the protection of natural persons with respect to the processing of personal data.

Codes of practice

84 Data-sharing code

(1) The Information Commissioner may prepare a code of practice which contains, —

(a) practical guidance in relation to the sharing of personal data in accordance with the requirements of the data protection legislation; and

(b) such other guidance as the Information Commissioner considers appropriate to promote good practice in the sharing of personal data.

(2) Where a code under this regulation is in force, the Information Commissioner may prepare amendments of the code or a replacement code.

(3) Before preparing a code or amendments under this regulation, the Information Commissioner must consult the Council of Ministers and such of the following as the Information Commissioner considers appropriate, —

(a) trade associations;

(b) data subjects; or

(c) persons who appear to the Information Commissioner to represent the interests of data subjects.

(4) A code under this regulation may include transitional provision or savings.

(5) In this regulation, —

"good practice in the sharing of personal data" means such practice in the sharing of personal data as appears to the Information Commissioner to be desirable having regard to the interests of data subjects and others, including compliance with the requirements of the data protection legislation;

"the sharing of personal data" means the disclosure of personal data by transmission, dissemination or otherwise making it available;

"trade association" includes a body representing controllers or processors.

85 Direct marketing code

(1) The Information Commissioner may prepare a code of practice which contains, —

(a) practical guidance in relation to the carrying out of direct marketing in accordance with the requirements of the data protection legislation and any other relevant enactment; and

(b) such other guidance as the Information Commissioner considers appropriate to promote good practice in direct marketing.

(2) Where a code under this regulation is in force, the Information Commissioner may prepare amendments of the code or a replacement code.

(3) Before preparing a code or amendments under this regulation, the Information Commissioner must consult the Council of Ministers and such of the following as the Information Commissioner considers appropriate, —

(a) trade associations;

(b) data subjects;

(c) persons who appear to the Information Commissioner to represent the interests of data subjects.

(4) A code under this regulation may include transitional provisions or savings.

(5) In this regulation, —

"direct marketing" means the communication (by whatever means) of advertising or marketing material which is directed to particular natural persons;

"good practice in direct marketing" means such practice in direct marketing as appears to the Information Commissioner to be desirable having regard to the interests of data subjects and others, including compliance with the requirements mentioned in paragraph (1)(a);

"trade association" includes a body representing controllers or processors.

86 Approval of data-sharing and direct marketing codes

(1) When a code is prepared under regulation 84 or 85 —

(a) the Information Commissioner must submit the final version to the Council of Ministers; and

(b) the Council of Ministers must lay the code before Tynwald.

(2) If, within the 40-day period, Tynwald and its branches[16] resolve not to approve the code, the Information Commissioner must not issue the code.

(3) If no such resolution is made within that period, —

(a) the Information Commissioner must issue the code; and

(b) the code comes into force at the end of the period of 21 days beginning with the day on which it is issued.

(4) If, as a result of paragraph (2), there is no code in force under regulation 84 or 85, the Information Commissioner must prepare another version of the code.

(5) Nothing in paragraph (2) prevents another version of the code being laid before Tynwald.

(6) In this regulation, "the 40-day period" means, —

(a) if the code is laid before both the House of Keys and the Legislative Council on the same day, the period of 40 days beginning with that day; or

(b) if the code is laid before the House of Keys and the Legislative Council on different days, the period of 40 days beginning with the later of those days.

(7) In calculating the 40-day period, no account is to be taken of any period during which Tynwald or any of its branches is —

(a) dissolved or prorogued; or

[16] In accordance with the provisions of the relevant Standing Orders.

(b) adjourned for more than 4 days.

(8) This regulation, other than paragraph (4), applies in relation to amendments prepared under regulations 84 and 85 as it applies in relation to codes prepared under those regulations.

87 Publication and review of data-sharing and direct marketing codes

(1) The Information Commissioner may publish a code issued under regulation 86(3).

(2) Where an amendment of a code is issued under regulation 86(3), the Information Commissioner must publish, —

(a) the amendment; or

(b) the code as amended by it.

(3) The Information Commissioner must keep under review each code issued under regulation 86(3) for the time being in force.

(4) Where the Information Commissioner becomes aware that the terms of such a code could result in a breach of an international obligation of the Island, the Information Commissioner must exercise the power under regulation 84(2) or 85(2) with a view to remedying the situation.

88 Effect of data-sharing and direct marketing codes

(1) A failure by a person to act in accordance with a provision of a code issued under regulation 86(3) does not of itself make that person liable to legal proceedings in a court or tribunal.

(2) A code issued under regulation 86(3), including an amendment or replacement code, is admissible in evidence in legal proceedings.

(3) In any proceedings before a court or tribunal, the court or tribunal must take into account a provision of a code issued under regulation 86(3) in determining a question arising in the proceedings if, —

(a) the question relates to a time when the provision was in force; and

(b) the provision appears to the court or tribunal to be relevant to the question.

(4) Where the Information Commissioner is carrying out a function described in paragraph (5), the Information Commissioner must take into account a provision of a code issued under regulation 86(3) in determining a question arising in connection with the carrying out of the function if, —

(a) the question relates to a time when the provision was in force; and

(b) the provision appears to the Information Commissioner to be relevant to the question.

(5) Those functions are functions under, —

(a) the data protection legislation; or

(b) any other relevant enactment.

89 Codes of practice

(1) The Council of Ministers may by regulations require the Information Commissioner, —

(a) to prepare appropriate codes of practice giving guidance as to good practice in the processing of personal data; and

(b) to make them available to such persons as the Information Commissioner considers appropriate.

Tynwald procedure – laying only.

(2) Before preparing such codes, the Information Commissioner must consult such of the following as the Information Commissioner considers appropriate, —

(a) trade associations;

(b) data subjects;

(c) persons who appear to the Information Commissioner to represent the interests of data subjects.

(3) Regulations made under this regulation, —

(a) must describe the personal data or processing to which the code of practice is to relate; and

(b) may describe the persons or classes of person to whom it is to relate.

(4) In this regulation, —

"good practice in the processing of personal data" means such practice in the processing of personal data as appears to the Information Commissioner to be desirable having regard to the interests of data subjects and others, including compliance with the requirements of the data protection legislation;

"trade association" includes a body representing controllers or processors.

Information provided to the Information Commissioner

90 Disclosure of information to the Information Commissioner

No enactment or rule of law prohibiting or restricting the disclosure of information precludes a person from providing the Information Commissioner with information necessary for the discharge of the Information Commissioner's functions under the data protection legislation.

91 Confidentiality of information

(1) Without limiting section 64 of the *Freedom of Information Act 2015*, it is an offence for a person who is or has been the Information Commissioner, or a member of the Information Commissioner's staff or an agent of the Information Commissioner, knowingly or recklessly to disclose information which, —

(a) has been obtained by, or provided to, the Information Commissioner under or for the purposes of the data protection legislation or the Unsolicited Communications Regulations 2005;[17]

(b) relates to an identified or identifiable living natural person or business; and

(c) is not available to the public from other sources at the time of the disclosure and has not previously been available to the public from other sources,

unless the disclosure is made with lawful authority.

(2) For the purposes of paragraph (1), a disclosure is made with lawful authority only if and to the extent that, —

(a) the disclosure was made with the consent of the natural person or of the person for the time being carrying on the business;

(b) the information was provided for the purpose of its being made available to the public (in whatever manner) under a provision of the data protection legislation or the *Freedom of Information Act 2015*;

(c) the disclosure was made for the purposes of, and is necessary for, the discharge of a function under the data protection legislation or the *Freedom of Information Act 2015*;

(d) the disclosure was made for the purposes of, and is necessary for, the discharge of an EU obligation;

(e) the disclosure was made for the purposes of criminal or civil proceedings, however arising; or

(f) having regard to the rights, freedoms and legitimate interests of any person, the disclosure was necessary in the public interest.

(See regulation 141(2), which specifies the penalty for offences under this regulation.)

92 Guidance about privileged communications

(1) The Information Commissioner may produce and publish guidance about, —

(a) how the Information Commissioner proposes to secure that privileged communications which the Information Commissioner

[17] SD 393/05

obtains or has access to in the course of carrying out the Information Commissioner's functions are used or disclosed only so far as necessary for carrying out those functions; and

(b) how the Information Commissioner proposes to comply with restrictions and prohibitions on obtaining or having access to privileged communications which are imposed by an enactment.

(2) The Information Commissioner, —

(a) may alter or replace the guidance; and

(b) must publish any altered or replacement guidance.

(3) The Information Commissioner must consult the Council of Ministers before publishing guidance under this regulation (including altered or replacement guidance).

(4) The Information Commissioner must arrange for guidance under this regulation (including altered or replacement guidance) to be laid before Tynwald.

(5) In this regulation, "privileged communications" means, —

(a) communications made, —

(i) between professional legal adviser and the adviser's client; and

(ii) in connection with the giving of legal advice to the client with respect to legal obligations, liabilities or rights; and

(b) communications made, —

(i) between a professional legal adviser and the adviser's client or between such an adviser or client and another person;

(ii) in connection with or in contemplation of legal proceedings; and

(iii) for the purposes of such proceedings.

(6) In paragraph (5)—

(a) references to the client of a professional legal adviser include references to a person acting on behalf of the client; and

(b) references to a communication include, —

(i) a copy or other record of the communication; and

(ii) anything enclosed with or referred to in the communication if made as described in paragraph (5)(a)(ii) or in paragraph (5)(b)(ii) and (iii).

Fees

93 Fees for services

(1) The Information Commissioner may require a person other than a data subject or a data protection officer to pay a reasonable fee for a service provided to the person or at the person's request, which the Information Commissioner is required or authorised to provide under the data protection legislation.

(2) In this regulation, "service" includes "data protection audits" authorised by Article 58(1)(b) of the applied GDPR.

(3) The Council of Ministers may make regulations expressly including or excluding particular services in or from, as the case may be, the services to which this regulation applies.

Tynwald procedure – approval required.

94 Manifestly unfounded or excessive requests by data subjects etc.

(1) Where a request to the Information Commissioner from a data subject or a data protection officer is manifestly unfounded or excessive, the Information Commissioner may, —

(a) charge a reasonable fee for dealing with the request; or

(b) refuse to act on the request.

(2) An example of a request that may be excessive is one that merely repeats the substance of previous requests.

(3) In any proceedings where there is an issue as to whether a request described in paragraph (1) is manifestly unfounded or excessive, it is for the Information Commissioner to show that it is.

(4) Paragraphs (1) and (3) apply only in cases in which the Information Commissioner does not already have such powers and obligations under Article 57(4) of the applied GDPR.

95 Guidance about fees

(1) The Information Commissioner must, with the written concurrence of the Treasury, produce and publish guidance about the fees the Information Commissioner proposes to charge in accordance with, —

(a) regulation 93 or 94; or

(b) Article 57(4) of the applied GDPR.

(2) Before publishing the guidance, the Information Commissioner must consult the Council of Ministers.

Charges

96 Charges payable to the Information Commissioner by controllers and processors[12]

(1) The Council of Ministers may by regulations require controllers and (where applicable) processors to pay charges of an amount specified in the regulations to the Information Commissioner.

Tynwald procedure – approval required.

(2) Regulations under paragraph (1) may require a controller and (where applicable) a processor to pay a charge regardless of whether the Information Commissioner has provided, or proposes to provide, a service to the controller.

(3) Regulations under paragraph (1) may make provision —

(a) about the time or times at which, or period for which, a charge must be paid;

(b) for cases in which a discounted charge is payable;

(c) for cases in which no charge is payable; or

(d) for cases in which a charge which has been paid is to be refunded.

(4) In making regulations under paragraph (1), the Council of Ministers must have regard to the desirability of securing that the charges payable to the Information Commissioner under such regulations are sufficient to offset, —

(a) expenses incurred by the Information Commissioner in discharging the Information Commissioner's functions under the data protection legislation;

(b) any expenses of the Council of Ministers in respect of the Information Commissioner so far as attributable to those functions,

(c) to the extent that the Council of Ministers considers appropriate, any deficit previously incurred (whether before or after the making of these Regulations) in respect of the expenses mentioned in subparagraph (a); and

(d) to the extent that the Council of Ministers considers appropriate, expenses incurred by the Council of Ministers in respect of the inclusion of any officers or staff of the Information Commissioner in any scheme under the *Public Sector Pensions Act 2011*.

(5) The Council of Ministers may from time to time require the Information Commissioner to provide information about the expenses referred to in paragraph (4)(a).

(6) The Council of Ministers may by regulations make provision, —

(a) requiring a controller and (where applicable) a processor to provide information to the Information Commissioner; or

(b) enabling the Information Commissioner to require a controller and (where applicable) a processor to provide information to the Information Commissioner,

for either or both of the purposes mentioned in paragraph (7).

Tynwald procedure – approval required.

(7) Those purposes are, —

(a) determining whether a charge is payable by the controller and (where applicable) the processor under regulations under paragraph (1); and

(b) determining the amount of a charge payable by the controller and (where applicable) the processor.

(8) The provision that may be made under paragraph (6)(a) includes provision requiring a controller and (where applicable) a processor to notify the Information Commissioner of a change in the controller's and (where applicable) the processor's circumstances of a kind specified in the regulations.

97 Regulations under regulation 96: supplementary

(1) Before making regulations under regulation 96(1) or (6), the Council of Ministers must consult, —

(a) such representatives of persons likely to be affected by the regulations as the Council of Ministers thinks appropriate; and

(b) such other persons as the Council of Ministers thinks appropriate,

(and see also regulation 135).

(2) The Information Commissioner, —

(a) must keep under review the working of regulations under regulation 96(1) or (6); and

(b) may from time to time submit proposals to the Council of Ministers for amendments to be made to the regulations.

(3) The Council of Ministers must review the working of regulations under regulation 96(1) or (6) every 5 years.

Reports, etc.

98 Reporting to Tynwald

(1) The Information Commissioner must, —

(a) produce a general report on the carrying out of the Information Commissioner's functions annually;

(b) arrange for it to be laid before Tynwald; and

(c) publish it.

(2) The report must include the annual report required under Article 59 of the applied GDPR.

(3) The Information Commissioner may produce other reports relating to the carrying out of the Information Commissioner's functions and arrange for them to be laid before Tynwald.

(4) For the purposes of the applied LED and without limiting the applicability of equivalent provisions in Articles 55 to 59 of the applied GDPR, —

(a) the requirements of Articles 45 to 48 of the applied LED are to be regarded as having, in this regulation, been provided for by law; and

(b) for the avoidance of doubt, Article 49 of the applied LED has the force of law and therefore must be complied with by the Information Commissioner.

99 Publication by the Information Commissioner

A duty under these Regulations for the Information Commissioner to publish a document is a duty for the Information Commissioner to publish it, or arrange for it to be published, in such form and manner as the Information Commissioner considers appropriate.

100 Notice from the Information Commissioner

(1) This regulation applies in relation to a notice authorised or required by these Regulations to be given to a person by the Information Commissioner.

(2) The notice may be given to a natural person —

(a) by delivering it to the natural person;

(b) by sending it to the natural person by post addressed to the natural person at his or her usual or last-known place of residence or business; or

(c) by leaving it for the natural person at that place.

(3) The notice may be given to a body corporate or unincorporate, —

(a) by sending it by post to the proper officer of the body at its principal office; or

(b) by addressing it to the proper officer of the body and leaving it at that office.

(4) The notice may be given to the person by other means, including by electronic means, with the person's consent.

(5) In this regulation, —

"principal office", in relation to a registered company, means its registered office;

"proper officer", in relation to any body, means the secretary or other executive officer, including but not limited to the registered agent, board of directors, or equivalent governing body, as may be charged with the conduct of its general;

"registered company" means a company registered under the enactments relating to companies for the time being in force in the Island.

(6) For the purposes of this regulation, so far as it relates to the addresses of controllers —

(a) the address of a registered company is that of its registered office; and

(b) the address of a person (other than a registered company) carrying on a business is that of the person's principal place of business on the Island.

(7) This regulation is without prejudice to any other lawful method of giving a notice.

PART 7 – ENFORCEMENT

Information notices

101 Information notices

(1) The Information Commissioner may, by written notice (an "**information notice**"), —

(a) require a controller or processor to provide the Information Commissioner with information that the Information Commissioner reasonably requires for the purposes of carrying out the Information Commissioner's functions under data protection legislation; or

(b) require any person to provide the Information Commissioner with information that the Information Commissioner reasonably requires for the purposes of —

(i) investigating a suspected failure of a type described in regulation 106(2) or a suspected offence under data protection legislation; or

(ii) determining whether the processing of personal data is carried out by an individual in the course of a purely personal or household activity.

(2) An information notice must state why the Information Commissioner requires the information.

(3) An information notice —

(a) may specify or describe particular information or a category of information;

(b) may specify the form in which the information must be provided;

(c) may specify the time at which, or the period within which, the information must be provided;

(d) may specify the place where the information must be provided.

This is subject to the restrictions in paragraphs (5) to (7).

(4) An information notice must provide information about the rights of appeal under regulation 120.

(5) An information notice may not require a person to provide information before the end of the period within which an appeal may be brought against the notice.

(6) If an appeal is brought against an information notice, the information need not be provided pending the determination or withdrawal of the appeal.

(7) If an information notice —

(a) states that, in the Information Commissioner's opinion, the information is required urgently; and

(b) gives the Information Commissioner's reasons for reaching that opinion,

paragraphs (5) and (6) do not apply but the notice must not require the information to be provided before the end of the period of 72 hours beginning with the day on which the notice is given.

(8) The Information Commissioner may cancel an information notice by written notice to the person to whom it was given.

(9) In paragraph (1), in relation to a person who is a controller or processor for the purposes of the applied GDPR, the reference to a controller or processor includes a representative of a controller or processor designated under Article 27 of the applied GDPR (representatives of controllers or processors not established in the European Union).

(10) The provisions of this regulation and of regulations 102 and 103 do not in any way limit the Information Commissioner's ability to exercise any powers conferred on him or her by Article 58 of the applied GDPR that are not specifically referred to in any of those regulations. Accordingly, the Information Commissioner may exercise any of those powers that may reasonably be exercised independently of serving an information notice.[13]

102 Information notices: restrictions

(1) The Information Commissioner may not give an information notice with respect to the processing of personal data for the special purposes unless —

(a) a determination under regulation 130 with respect to the data or the processing has taken effect; or

(b) the Information Commissioner —

(i) has reasonable grounds for suspecting that such a determination could be made; and

(ii) the information is required for the purposes of making such a determination.

(2) An information notice does not require a person to give the Information Commissioner information in respect of a communication which is made —

(a) between a professional legal adviser and the adviser's client; and

(b) in connection with the giving of legal advice to the client with respect to obligations, liabilities or rights under the data protection legislation.

(3) An information notice does not require a person to give the Information Commissioner information in respect of a communication which is made —

(a) between a professional legal adviser and the adviser's client or between such an adviser or client and another person;

(b) in connection with or in contemplation of proceedings under or arising out of the data protection legislation; and

(c) for the purposes of such proceedings.

(4) In paragraphs (2) and (3), references to the client of a professional legal adviser include references to a person acting on behalf of the client.

(5) An information notice does not require a person to provide the Information Commissioner with information if doing so would, by revealing evidence of the commission of an offence, expose the person to proceedings for that offence.

(6) The reference to an offence in paragraph (5) does not include an offence under, —

(a) these Regulations; or

(b) section 5 of *the Perjury Act 1952* (false statements made otherwise than on oath).

(7) An oral or written statement provided by a person in response to an information notice may not be used in evidence against that person on a

prosecution for an offence under these Regulations (other than an offence under regulation 141) unless in the proceedings, —

(a) in giving evidence the person provides information inconsistent with the statement; and

(b) evidence relating to the statement is adduced, or a question relating to it is asked, by that person or on that person's behalf.

(8) In paragraph (5), in relation to an information notice given to a representative of a controller or processor designated under Article 27 of the applied GDPR, the reference to the person providing the information being exposed to proceedings for an offence includes a reference to the controller or processor being exposed to such proceedings.

103 Offence of making false statements in an information notice

It is an offence for a person, in response to an information notice —

(a) to make a statement which the person knows to be false in a material respect;

(b) recklessly to make a statement which is false in a material respect.

(See regulation 141(2), which specifies the penalty for offences under this regulation.)[14]

Assessment notices

104 Assessment notice

(1) The Information Commissioner may by written notice (an "**assessment notice**") require a controller or processor to permit the Information Commissioner to carry out an assessment of whether the controller or processor has complied or is complying with data protection legislation.

(2) An assessment notice may require the controller or processor to permit the Information Commissioner to do any of the following —

(a) to enter any premises or vehicle (both of which terms have in the regulation the same meanings as are ascribed to them in section 81(1) of the Police Powers and Procedures Act 1998) occupied or controlled by the controller or processor (excluding any dwelling house in respect of which either the Information Commissioner must have the consent of the occupier of the dwelling house or otherwise obtain a warrant in accordance with Schedule 4);

(b) to obtain access to any data processing equipment and means on the premises;

(c) to obtain access to all information, documents or material, necessary for the performance of his tasks;

(d) to observe the processing of personal data that takes place on the premises;

(e) to access all personal data on the premises necessary for the performance of his tasks under this Regulation;

(f) to interview any person who processes personal data for or on behalf of the controller or processor, provided that any interviewee must be provided with —

(i) notice of not less than 72 hours of the date and time of the prospective interview;

(ii) notice of the right to obtain legal advice or other professional advice prior to the prospective interview;

(iii) a reasonable period of not less than 72 hours for the purpose of obtaining such professional advice prior to the date and time of the interview set out in the notice;

(g) to be provided with a copy (in such form as may be requested) of any information, documents or materials accessed under regulation 104(2)(c) or personal data on the premises accessed under regulation 104(2)(e).

(See Schedule 4, paragraph 2 for action that the Information Commissioner can take if the controller or processor fails to comply with an assessment notice.)

(3) An assessment notice must provide information about the rights of appeal under regulation 120.

(4) An assessment notice may not require a person to do anything before the end of the period within which an appeal may be brought against the notice.

(5) If an appeal is brought against an assessment notice, the controller or processor need not comply with a requirement in the notice pending the determination of withdrawal of the appeal.

(6) (6) If an assessment notice —

(a) states that, in the Information Commissioner's opinion, it is necessary for the controller or processor to comply with a requirement in the notice urgently; and

(b) gives the Information Commissioner's reasons for reaching that opinion,

paragraphs (5) and (6) do not apply; but the notice must not require the controller or processor to comply with the requirement before the end of the period of 7 days beginning with the day on which the notice is given.

(7) The Information Commissioner may cancel an assessment notice by written notice to the controller or processor to whom it was given.

(8) Where the Information Commissioner gives an assessment notice to a processor, the Information Commissioner must, so far as reasonably practicable, give a copy of the notice to each controller for whom the processor processes personal data.

(9) The provisions of this regulation and of regulation 105 do not in any way limit the Information Commissioner's ability to exercise any powers conferred on him or her by Article 58 of the applied GDPR that are not specifically referred to in any of those regulations. Accordingly, the Information Commissioner may exercise any of those powers that may reasonably be exercised independently of serving an assessment notice.[15]

105 Assessment notices: restrictions

(1) An assessment notice does not have effect so far as compliance would result in the disclosure of a communication which is made —

(a) between a professional legal adviser and the adviser's client; and

(b) in connection with the giving of legal advice to the client with respect to obligations, liabilities or rights under the data protection legislation.

(2) An assessment notice does not have effect so far as compliance would result in the disclosure of a communication which is made —

(a) between a professional legal adviser and the adviser's client or between such an adviser or client and another person;

(b) in connection with or in contemplation of proceedings under or arising out of the data protection legislation; and

(c) for the purposes of such proceedings.

(3) In paragraphs (1) and (2) —

(a) references to the client of a professional legal adviser include references to a person acting on behalf of such a client; and

(b) references to a communication include —

(i) a copy or other record of the communication; and

(ii) anything enclosed with or referred to in the communication if made as described in paragraph (1)(b) or in paragraph (2)(b) and (c).

(4) The Information Commissioner may not give a controller or processor an assessment notice with respect to the processing of personal data for the special purposes.

Enforcement notices

106 Enforcement notices

(1) Where the Information Commissioner is satisfied that a person has failed, or is failing, as described in paragraph (2), (3), (4) or (5), the Information Commissioner may give the person a written notice (an **"enforcement notice"**) which requires the person —

(a) to take steps specified in the notice; or

(b) to refrain from taking steps specified in the notice,

or both (and see also regulations 107 and 108).

(2) The first type of failure is where a controller or processor has failed, or is failing, to comply with any of the following —

(a) a provision of Chapter II of the applied GDPR or Chapter 2 of Part 3 of these Regulations (principles of processing);

(b) a provision of Articles 12 to 22 of the applied GDPR, or Chapter 4 of Part 3 of these Regulations, conferring rights on a data subject;

(c) a provision of Articles 24 to 39 of the applied GDPR (obligations of controllers and processors), including a requirement to communicate a personal data breach to the Information Commissioner or a data subject;

(d) a provision of Article 30 or Article 31 of the applied LED namely the requirement to communicate a personal data breach to the Information Commissioner or a data subject;

(e) the principles for transfers of personal data to third countries, non-Convention countries and international organisations in Articles 44 to 49 of the applied GDPR; or

(f) the requirement, imposed by this subparagraph, to implement data protection policies that are compliant with guidance provided by the Information Commissioner under these Regulations.

(3) The second type of failure is where a monitoring body has failed, or is failing, to comply with an obligation under Article 41 of the applied GDPR (monitoring or approved codes of conduct).

(4) The third type of failure is where a person who is a certification provider —

(a) does not meet the requirements for accreditation;

(b) has failed, or is failing, to comply with an obligation under Article 42 or 43 of the applied GDPR (certification of controllers and processors); or

(c) has failed, or is failing, to comply with any other provision of the applied GDPR (whether in the person's capacity as a certification provider or otherwise).

(5) The fourth type of failure is where a controller or processor has failed, or is failing, to comply with regulations under regulation 96.[16]

(6) An enforcement notice given in reliance on paragraphs (2), (3) or (5) may only impose requirements which the Information Commissioner considers appropriate for the purpose of remedying the failure.

(7) An enforcement notice given in reliance on paragraph (4) may only impose requirements which the Information Commissioner considers appropriate having regard to the failure (whether or not for the purpose of remedying the failure).

(8) The Council of Ministers may by regulations confer power on the Information Commissioner to give an enforcement notice in respect of other failures.

(9) Before making regulations under this regulation, Council of Ministers must consult such persons as the Council of Ministers considers appropriate.

(10) Regulations made under this regulation —

(a) may make provision about the giving of enforcement notices in respect of the failure; and

(b) may amend this regulation and regulations 107 to 110.

Tynwald procedure – affirmative.

107 Enforcement notices: supplementary

(1) An enforcement notice must —

(a) state what the person has failed or is failing to do; and

(b) give the Information Commissioner's reasons for reaching that opinion.

(2) In deciding whether to give an enforcement notice in reliance on regulation 106(2), the Information Commissioner must consider whether the failure has caused or is likely to cause any person damage or distress.

(3) In relation to an enforcement notice given in reliance on regulation 106(2), the Information Commissioner's power under regulation 106(1)(b) to require a person to refrain from taking specified steps includes power —

(a) to impose a ban relating to all processing of personal data; or

(b) to impose a ban relating only to a specified description of processing of personal data, including by specifying one or more of the following —

(i) a description of personal data;

(ii) the purpose or manner of the processing;

(iii) the time when the processing takes place.

(4) An enforcement notice may specify the time or times at which, or period or periods within which, a requirement imposed by the notice must be complied with (but see the restrictions in paragraphs (6) to (8)).

(5) An enforcement notice must provide information about the rights of appeal under regulation 120.

(6) An enforcement notice must not specify a time for compliance with a requirement in the notice which falls before the end of the period within which an appeal can be brought against the notice.

(7) If an appeal is brought against an enforcement notice, a requirement in the notice need not be complied with pending determination or withdrawal of the appeal.

(8) If an enforcement notice —

(a) states that, in the Information Commissioner's opinion, it is necessary for a requirement to be complied with urgently; and

(b) gives the Information Commissioner's reasons for reaching that opinion,

paragraphs (6) and (7) do not apply but the notice must not require the requirement to be complied with before the end of the period of 7 days beginning with the day on which the notice is given.

(9) In this regulation, "specified" means specified in an enforcement notice.

108 Enforcement notices: rectification and erasure of personal data etc.

(1) Paragraphs (2) and (3) apply where an enforcement notice is given in respect of a failure by a controller or processor —

(a) to comply with a data protection principle relating to accuracy; or

(b) to comply with a data subject's request to exercise rights under Article 16, 17 or 18 of the applied GDPR (right to rectification, erasure or restriction of processing).[17]

(2) If an enforcement notice requires the controller or processor to rectify or erase inaccurate personal data, it may also require the controller or processor to rectify or erase any other data which —

(a) are held by the controller or processor; and

(b) contain an expression of opinion which appears to the Information Commissioner to be based on the inaccurate personal data.

(3) Where a controller or processor has accurately recorded personal data provided by the data subject or a third party but the data are inaccurate, the enforcement notice may require the controller or processor —

(a) to take steps specified in the notice to ensure the accuracy of the data;

(b) if relevant, to secure that the data indicate the data subject's view that the data are inaccurate; and

(c) to supplement the data with a statement of the true facts relating to the matters dealt with by the data that is approved by the Information Commissioner,

(as well as imposing requirements under paragraph (2)).

(4) When deciding what steps it is reasonable to specify under paragraph (3)(a), the Information Commissioner must have regard to the purpose for which the data were obtained and further processed.

(5) Paragraphs (6) and (7) apply where —

(a) an enforcement notice requires a controller or processor to rectify or erase personal data; or

(b) the Information Commissioner is satisfied that the processing of personal data which has been rectified or erased by the controller or processor involved a failure in paragraph (1).

(6) An enforcement notice may, if reasonably practicable, require the controller or processor to notify third parties to whom the data have been disclosed of the rectification or erasure.

(7) In determining whether it is reasonably practicable to require such notification, the Information Commissioner must have regard, in particular, to the number of people who would have to be notified.

(8) In this regulation, "data protection principle relating to accuracy" means the principle in Article 5(1)(d) of the applied GDPR.

109 Enforcement notices: restrictions

(1) The Information Commissioner may not give a controller or processor an enforcement notice in reliance on regulation 106(2) with respect to the processing of personal data for the special purposes unless —

(a) a determination under regulation 130 with respect to the data or the processing has taken effect; and

(b) the court has granted leave for the notice to be given.

(2) A court must not grant leave for the purposes of paragraph (1)(b) unless it is satisfied that —

(a) the Information Commissioner has reason to suspect a failure described in regulation 106(2) which is of substantial public importance; and

(b) the controller or processor has been given notice of the application for leave in accordance with rules of court or the case is urgent.

110 Enforcement notices: cancellation and variation

(1) The Information Commissioner may cancel or vary an enforcement notice by giving written notice to the person to whom it was given.

(2) A person to whom an enforcement notice is given may apply in writing to the Information Commissioner for cancellation or variation of the notice.

(3) An application under paragraph (2) may be made only —

(a) after the end of the period within which an appeal can be brought against the notice; and

(b) on the ground that, by reason of a change of circumstances, one or more of the provisions of that notice need not be complied with in order to remedy the failure identified in the notice.

Powers of entry and inspection

111 Powers of entry and inspection

Schedule 4 makes provision about powers of entry and inspection.

Penalties

112 Penalty notices

(1) If the Information Commissioner is satisfied that a person —

(a) has failed or is failing as described in regulation 106(2), (3), (4) or (5);

(b) has failed to comply with an information notice;

(c) has failed to comply with an assessment notice given, pursuant to regulation 77, in exercise of the Information Commissioner's powers under Article 58(1) of the applied GDPR; or

(d) has failed to comply with an enforcement notice,

the Information Commissioner may, by written notice (a "**penalty notice**"), require the person to pay to the Information Commissioner an amount specified in the notice.[18]

(2) In the case of a failure described in regulation 106(2), (3) or (4), when deciding whether to give a penalty notice to a person and determining the amount of the penalty, the Information Commissioner must have regard to the following, so far as relevant, —

(a) to the extent that the notice concerns a matter to which the applied GDPR applies, the matters listed in Article 83(1) and (2) of the applied GDPR;

(b) to the extent that the notice concerns a failure to comply with these Regulations, the matters listed in paragraph (3).

(3) Those matters are, —

(a) the nature, gravity and duration of the failure;

(b) the intentional or negligent character of the failure;

(c) any action taken by the controller or processor to mitigate the damage suffered by data subjects;

(d) the degree of responsibility of the controller or processor, taking into account technical and organisational measures implemented by the controller or processor;

(e) any relevant previous failures by the controller or processor;

(f) the degree of co-operation with the Information Commissioner, in order to remedy the failure and mitigate the possible adverse effects of the failure;

(g) the categories of personal data affected by the failure;

(h) the manner in which the infringement became known to the Information Commissioner, including whether, and if so to what extent, the controller or processor notified the Information Commissioner of the failure;

(i) the extent to which the controller or processor has complied with previous enforcement notices or penalty notices;

(j) adherence to approved codes of conduct or certification mechanisms;

(k) any other aggravating or mitigating factor applicable to the case, including financial benefits gained, or losses avoided, as a result of the failure (whether directly or indirectly); and

(l) whether the penalty would be effective, proportionate and dissuasive.

(4) Schedule 5 makes further provision about penalty notices, including provision requiring the Information Commissioner to give a notice of intent to impose a penalty and provision about payment, variation, cancellation and enforcement.

(5) The Council of Ministers may by regulations, —

(a) confer power on the Information Commissioner to give a penalty notice in respect of other failures; and

(b) make provision about the amount of the penalty that may be imposed.

Tynwald procedure – approval required.

(6) Before making regulations under paragraph (5), the Council of Ministers must consult such persons as the Council of Ministers considers appropriate.

(7) Regulations made under paragraph (5) may —

(a) make provision about the giving of penalty notices in respect of the failure; and

(b) amend this regulation and regulations 113 to 116.

113 Penalty notices: restrictions

(1) The Information Commissioner may not give a controller or processor a penalty notice in reliance on regulation 106(2) with respect to the processing of personal data for the special purposes unless, —

(a) a determination under regulation 130 with respect to the data or the processing has taken effect; and

(b) a court has granted leave for the notice to be given.

(2) A court must not grant leave for the purposes of paragraph (1)(b) unless it is satisfied that, —

(a) the Information Commissioner has reason to suspect a failure described in regulation 106(2) which is of substantial public importance; and

(b) the controller or processor has been given notice of the application for leave in accordance with rules of court or the case is urgent.

114 Maximum amount of penalty

(1) In relation to an infringement of a provision of the applied GDPR, the maximum amount of the penalty that may be imposed by a penalty notice is £1,000,000.

(2) This regulation applies despite Article 83 of the applied GDPR and, within the parameters of the significantly higher maximum fines provided for in the said Article 83, prescribes the maximum penalty imposable in the Island.

115 Fixed penalties for non-compliance with charges regulations

(1) The Information Commissioner may —

(a) produce and publish; or

(b) adopt, with suitable modifications, from another jurisdiction, and publish,

a document specifying the amount of the penalty for a failure to comply with regulations made under regulation 96.

(2) The Information Commissioner may specify different amounts for different types of failure.

(3) The maximum amount that may be specified is 150% of the highest charge payable by a controller or processor in respect of a financial year in accordance with the regulations, disregarding any discount available under the regulations.

(4) The Information Commissioner —

(a) may alter or replace the document; and

(b) must publish any altered or replacement document.

(5) Before publishing a document under this regulation (including any altered or replacement document), the Information Commissioner must consult —

(a) the Council of Ministers; and

(b) such other persons as the Council of Ministers considers appropriate.

(6) The Information Commissioner must arrange for a document published under this regulation (including any altered or replacement document) to be laid before Tynwald.

116 Amount of penalties: supplementary

(1) For the purposes of Article 83 of the applied GDPR and of regulation 114, the Council of Ministers may by regulations, —

(a) provide that a person of a description specified in the regulations is or is not an undertaking; and

(b) make provision about how an undertaking's turnover is to be determined.

Tynwald procedure – approval required.

(2) For the purposes of Article 83 of the applied GDPR, regulation 114 and regulation 115, the Council of Ministers may by regulations provide that a period is or is not a financial year.

Tynwald procedure – approval required.

(3) Before making regulations under this regulation, the Council of Ministers must consult such persons as the Council of Ministers considers appropriate.

117 Failure to comply with notices

(1) The Information Commissioner may certify in writing to the High Court that a controller or processor has, or both have (as the case may be), failed to comply with —

(a) an information notice;

(b) an assessment notice;

(c) an enforcement notice; or

(d) a penalty notice.[19]

(2) The Information Commissioner must not exercise the power under paragraph (1) before the expiry of the period of time specified in the relevant notice.

(3) The High Court must inquire into the matter and, after hearing —

(a) any witness who may be produced against or on behalf of the controller or processor, as the case may be; and

(b) any statement that may be offered in defence,

may deal with the controller or processor, as the case may be, as if it had committed a contempt of court.

(4) This regulation does not confer any right of action in civil proceedings in respect of a failure to comply with a duty imposed by or under these Regulations.

(5) The High Court may for the purposes of securing compliance with data protection legislation make an order requiring the controller (or a processor acting on behalf of that controller), in respect of the processing, —

(a) to take steps specified in the order; or

(b) to refrain from taking steps specified in the Order.

Guidance

118 Guidance about corrective action[20]

(1) The Information Commissioner may produce and publish guidance about how the Information Commissioner proposes to exercise the Information Commissioner's functions in connection with —

(a) information notices;

(b) assessment notices;

(c) enforcement notices; or

(d) penalty notices.[21]

(2) The Information Commissioner may produce and publish guidance about how the Information Commissioner proposes to exercise the Information Commissioner's other functions under this Part.

(3) In relation to assessment notices, the guidance must include —

(a) provision specifying factors to be considered in determining whether to give an assessment notice to a person;

(b) provision specifying descriptions of documents or information that —

(i) are not to be examined or inspected in accordance with an assessment notice; or

(ii) are to be so examined or inspected only by a person of a description specified in the guidance;

(c) provision about the nature of inspections and examinations carried out in accordance with an assessment notice;

(d) provision about the nature of interviews carried out in accordance with an assessment notice; and

(e) provision about the preparation, issuing and publication by the Information Commissioner of assessment reports in respect of controllers and processors that have been given assessment notices.

(4) The guidance prepared in accordance with paragraph (3)(b) must include provisions that relate to —

(a) documents and information concerning a natural person's physical or mental health; and

(b) documents and information concerning the provision of social care for a natural person.

(5) In relation to penalty notices, the guidance must include —

(a) provision about the circumstances in which the Information Commissioner would consider it appropriate to issue a penalty notice;

(b) provision about the circumstances in which the Information Commissioner would consider it appropriate to allow a controller or processor to make oral representations about a notice of intent; and

(c) provision explaining how the Information Commissioner will determine the amount of penalties.

(6) The Information Commissioner —

(a) may alter or replace the guidance; and

(b) must publish any altered or replacement guidance.

(7) Before publishing guidance under this regulation (including any altered or replacement guidance), the Information Commissioner must consult —

(a) the Council of Ministers; and

(b) such other persons as the Council of Ministers considers appropriate.

(8) The Information Commissioner must arrange for guidance under this regulation (including any altered or replacement guidance) to be laid before Tynwald.

(9) In this regulation, "social care" has the same meaning as in section 5 of the *Regulation of Care Act 2013*.

Appeals

119 The Tribunal

(1) For the purposes of these Regulations, there continues to be an Isle of Man Data Protection Tribunal ("**the Tribunal**").

(2) The Tribunal is to consist of a chairman and 2 other members, appointed in accordance with the *Tribunals Act 2006*.

120 Right of appeal

(1) A person who is given any of the following notices may appeal to the Tribunal, —

(a) an information notice;

(b) an assessment notice;

(c) an instruction under regulation 78(2);

(d) an enforcement notice;

(e) a penalty notice; or

(f) a penalty variation notice.

(2) Where a notice listed in paragraph (1) contains a statement under regulation 101(7)(a), 104(8)(a) or 107(8)(a) (urgency), the person given the notice may appeal against, —

(a) the Information Commissioner's decision to include the statement in the notice; or

(b) the effect of its inclusion as respects any part of the notice,

whether or not the person appeals against the notice.

(3) A person who is given an enforcement notice may appeal to the Tribunal against the refusal of an application under regulation 110 for the cancellation or variation of the notice.

(4) A person who is given a penalty notice or a penalty variation notice may appeal against the amount of the penalty specified in the notice, whether or not the person appeals against the notice.

(5) Where a determination is made under regulation 130 in respect of the processing of personal data for the special purposes, the controller or processor may appeal to the Tribunal against the determination.

(6) The requirements of Article 53 of the applied LED are to be regarded as having been, by this regulation, provided for and accordingly, the judicial remedy thereby required is, for the avoidance of doubt, hereby declared to be available in accordance with the relevant Rules of Court and associated substantive and procedural laws of the Island.

(7) Schedule 8 contains additional provisions relevant to appeals.

121 Determination of appeals

(1) Paragraphs (2) to (4) apply where a person appeals to the Tribunal under regulation 120(1) or (4).

(2) The Tribunal may review any determination of fact on which the notice or decision against which the appeal is brought was based.

(3) If the Tribunal considers, —

(a) that the notice or decision against which the appeal is brought is not in accordance with the law; or

(b) to the extent that the notice or decision involved an exercise of discretion by the Information Commissioner, that the Information Commissioner ought to have exercised the discretion differently,

the Tribunal must allow the appeal or substitute another notice or decision which the Information Commissioner could have given or made.

(4) Otherwise, the Tribunal must dismiss the appeal.

(5) On an appeal under regulation 120(2), the Tribunal may direct, —

(a) that the notice against which the appeal is brought is to have effect as if it did not contain the statement under regulation 101(7)(a), 104(8)(a) or 107(8)(a) (urgency); or

(b) that the inclusion of that statement is not to have effect in relation to any part of the notice,

and may make such modifications to the notice as are required to give effect to the direction.

(6) On an appeal under regulation 120(3), if the Tribunal considers that the enforcement notice ought to be cancelled or varied by reason of a change in circumstances, the Tribunal must cancel or vary the notice.

(7) On an appeal under regulation 120(5), the Tribunal may cancel the Information Commissioner's determination.

Complaints

122 Complaints by data subjects

(1) A data subject may make a complaint to the Information Commissioner if the data subject considers that, in connection with personal data relating to him or her, there is an infringement of data protection legislation.

(2) The Information Commissioner must facilitate the making of complaints under paragraph (1) by taking steps such as providing a complaint form which can be completed electronically and by other means.

(3) If the Information Commissioner receives a complaint under paragraph (1), the Information Commissioner must, —

(a) take appropriate steps to respond to the complaint;

(b) inform the complainant of the outcome of the complaint;

(c) inform the complainant of the rights under regulation 123; and

(d) if asked to do so by the complainant, provide the complainant with further information about how to pursue the complaint.

(4) The reference in paragraph (3)(a) to taking appropriate steps in response to a complaint includes, —

(a) investigating the subject matter of the complaint, to the extent appropriate; and

(b) informing the complainant about progress on the complaint, including about whether further investigation or co-ordination with another supervisory authority or foreign designated authority is necessary.

(5) If the Information Commissioner receives a complaint relating to the infringement of a data subject's rights under provisions adopted by a Member State other than the Island pursuant to the applied Law Enforcement Directive, the Information Commissioner must, —

(a) send the complaint to the relevant supervisory authority for the purposes of the applied LED;

(b) inform the complainant that the Information Commissioner has done so; and

(c) if asked to do so by the complainant, provide the complainant with further information about how to pursue the complaint.

(6) The requirements of Article 52 of the applied LED are to be taken as having been, by this regulation, provided for and, accordingly, the enforceable stipulations in that Article have the force of law.

(7) In this regulation, —

"foreign designated authority" means an authority designated for the purposes of Article 13 of the Data Protection Convention by a party, other than the Island, which is bound by that Convention;

"supervisory authority" means a supervisory authority for the purposes of Article 51 of the applied GDPR, or of Article 41 of the applied Law Enforcement Directive, in a member State other than the Island.

123 Orders to progress complaints

(1) This regulation applies where, after a data subject makes a complaint under Article 77 of the applied GDPR or regulation 122, the Information Commissioner, —

(a) fails to take appropriate steps to respond to the complaint;

(b) fails to provide the complainant with information about progress on the complaint, or of the outcome of the complaint, before the end of the period of 3 months beginning with the day on which the Information Commissioner received the complaint; or

(c) if the Information Commissioner's consideration of the complaint is not concluded during that period, fails to provide the complainant with such information during a subsequent period of 3 months.

(2) The Tribunal may, on an application by the data subject, make an order requiring the Information Commissioner, —

(a) to take appropriate steps to respond to the complaint; or

(b) to inform the complainant of progress on the complaint, or of the outcome of the complaint, within a period specified in the order.

(3) An order under paragraph (2)(a) may require the Information Commissioner, —

(a) to take steps specified in the order; or

(b) to conclude the investigation, or take a specified step, within a period specified in the order.

(4) Regulation 122(5) applies for the purposes of paragraphs (1)(a) and (2)(a) as it applies for the purposes of regulation 122(3)(a).

Remedies in the court

124 Compliance orders

(1) This regulation applies if, on an application by a data subject, a court is satisfied that there has been an infringement of the data subject's rights under the data protection legislation in contravention of that legislation.

(2) A court may make an order for the purposes of securing compliance with the data protection legislation which requires the controller in respect of the processing, or a processor acting on behalf of that controller, —

(a) to take steps specified in the order; or

(b) to refrain from taking steps specified in the order.

(3) The order may, in relation to each step, specify the time at which, or the period within which, it must be taken.

(4) In paragraph (1), the reference to an application by a data subject includes an application made in exercise of the right under Article 79(1) of the applied GDPR (right to an effective remedy against a controller or processor).

(5) In relation to a joint controller whose responsibilities are determined in an arrangement under data protection legislation, a court may only make an order under this regulation if the controller is responsible for compliance with the provision of the data protection legislation that is contravened.

(6) The requirements of Articles 54 (right to an effective judicial remedy against a controller or processor) and 55 (representation of data subjects) of the applied LED are to be regarding as having been provided for by this regulation and are accordingly enforceable under this regulation.

125 Compensation for contravention of data protection legislation

(1) In Article 82 of the applied GDPR (right to compensation), "damage" includes financial loss, distress and other adverse effects.

(2) Paragraph (3) applies where, —

(a) in accordance with rules of court, proceedings under Article 82 of the applied GDPR are brought by a representative body on behalf of a person; and

(b) a court orders the payment of compensation.

(3) The court may make an order providing for the compensation to be paid on behalf of the person to, —

(a) the representative body; or

(b) such other person as the court thinks fit.

(4) The requirements of Article 56 of the applied LED (right to compensation) are to be regarded as having been, by this regulation, provided for by law.

(5) A person who suffers damage by reason of a contravention of a requirement of the data protection legislation, other than the applied GDPR, is entitled to compensation for that damage from the controller or the processor, subject to paragraphs (6) and (7).

(6) Under paragraph (5)—

(a) a controller involved in processing of personal data is liable for any damage caused by the processing; and

(b) a processor involved in processing of personal data is liable for damage caused by the processing only if the processor, —

(i) has not complied with an obligation under the data protection legislation specifically directed at processors; or

(ii) has acted outside, or contrary to, the controller's lawful instructions.

(7) A controller or processor is not liable as described in paragraph (6) if the controller or processor proves that the controller or processor is not in any way responsible for the event giving rise to the damage.

(8) A joint controller in respect of the processing of personal data to which Part 3 of the applied LED applies whose responsibilities are determined in an arrangement is only liable as described in paragraph (6) if the controller is responsible for compliance with the provision of the data protection legislation that is contravened.

(9) In this regulation, "damage" includes financial loss, distress and other adverse effects, whether or not material.

Offences relating to personal data

126 Unlawful obtaining etc. of personal data

(1) It is an offence for a person knowingly or recklessly, —

(a) to obtain or disclose personal data without the consent of the controller;

(b) to procure the disclosure of personal data to another person without the consent of the controller; or

(c) after obtaining personal data, to retain them without the consent of the person who was the controller in relation to the personal data when they were obtained.

(2) It is a defence for a person charged with an offence under paragraph (1) to prove that the obtaining, disclosing, procuring or retaining, —

(a) was necessary for the purposes of preventing or detecting crime;

(b) was required or authorised by an enactment, by a rule of law or by the order of a court; or

(c) in the particular circumstances, was justified as being in the public interest.

(3) It is also a defence for a person charged with an offence under paragraph (1) to prove that, —

(a) the person acted in the reasonable belief that the person had a legal right to do the obtaining, disclosing, procuring or retaining; or

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

(4) It is an offence for a person to sell personal data if the person obtained the data in circumstances in which an offence under paragraph (1) was committed.

(5) It is an offence for a person to offer to sell personal data if the person, —

(a) has obtained the data in circumstances in which an offence under paragraph (1) was committed; or

(b) subsequently obtains the data in such circumstances.

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

(7) In this regulation —

(a) references to the consent of a controller do not include the consent of a person who is a controller by virtue of Article 28(10) of the applied GDPR; and

(b) where there is more than one controller, such references are references to the consent of one or more of them.

(See regulation 141(2), which specifies the penalty for offences under this regulation.)

127 Re-identification of de-identified personal data

(1) It is an offence for a person knowingly or recklessly to re-identify information that is de-identified personal data without the consent of the controller responsible for de-identifying the personal data.

(2) For the purposes of this regulation, —

(a) personal data are “de-identified” if they have been processed in such a manner that they can no longer be attributed, without more, to a specific data subject;

(b) a person "re-identifies" information if the person takes steps which result in the information no longer being de-identified within the meaning of subparagraph (a).

(3) It is a defence for a person charged with an offence under paragraph (1) to prove that the re-identification, —

(a) was necessary for the purposes of preventing or detecting crime;

(b) was required or authorised by an enactment, by a rule of law or by the order of a court; or

(c) in the particular circumstances, was justified as being in the public interest.

(4) It is also a defence for a person charged with an offence under paragraph (1) to prove that the person acted in the reasonable belief that —

(a) the person, —

(i) is the data subject to whom the information relates;

(ii) had the consent of that data subject; or

(iii) would have had such consent if the data subject had known about the re-identification and the circumstances of it; or

(b) the person, —

(i) is the controller responsible for de-identifying the personal data;

(ii) had the consent of that controller; or

(iii) would have had such consent if that controller had known about the re-identification and the circumstances of it.

(5) It is an offence for a person knowingly or recklessly to process personal data that are information that has been re-identified where the person does so, —

(a) without the consent of the controller responsible for de-identifying the personal data; and

(b) in circumstances in which the re-identification was an offence under paragraph (1).

(6) It is a defence for a person charged with an offence under paragraph (5) to prove that the processing, —

(a) was necessary for the purposes of preventing or detecting crime;

(b) was required or authorised by an enactment, by a rule of law or by the order of a court; or

(c) in the particular circumstances, was justified as being in the public interest.

(7) It is also a defence for a person charged with an offence under paragraph (5) to prove that the person acted in the reasonable belief that, —

(a) the processing was lawful; or

(b) the person, —

(i) had the consent of the controller responsible for de-identifying the personal data; or

(ii) would have had such consent if that controller had known about the processing and the circumstances of it.

(8) In this regulation, —

(a) references to the consent of a controller do not include the consent of a person who is a controller by virtue of Article 28(10) of the applied GDPR (processor to be treated as controller in certain circumstances); and

(b) where there is more than one controller, such references are references to the consent of one or more of them.

(See regulation 141(2), which specifies the penalty for offences under this regulation.)

128 Alteration of personal data to prevent disclosure

(1) Paragraph (3) applies where, —

(a) a request has been made in exercise of a data subject access right; and

(b) the person making the request would have been entitled to receive information in response to that request.

(2) In this regulation, "data subject access right" means a right under, —

(a) Article 15 (right of access by the data subject) of the applied GDPR; or

(b) Article 20 (right to data portability) of the applied GDPR.

(3) It is an offence for a person listed in paragraph (4) to alter, deface, block, erase, destroy or conceal information with the intention of preventing disclosure of all or part of the information that the person making the request would have been entitled to receive.

(4) Those persons are, —

(a) the controller; and

(b) a person who is employed by the controller, an officer of the controller or subject to the direction of the controller.

(5) It is a defence for a person charged with an offence under paragraph (3) to prove that, —

(a) the alteration, defacing, blocking, erasure, destruction or concealment of the information would have occurred in the absence of a request made in exercise of a data subject access right; or

(b) the person acted in the reasonable belief that the person making the request was not entitled to receive the information in response to the request.

(See regulation 141(1), which specifies the penalty for offences under this regulation.)

129 Record tampering

(1) A person commits an offence if —

(a) the Information Commissioner —

(i) has served an information notice on a controller or processor; or

(ii) has, by means other than serving an information notice, made to the controller or processor a request for information;[22]

(b) the person alters, defaces, erases, destroys or conceals information held by the controller or processor with the intention of preventing the controller or processor from supplying the information to the Information Commissioner; and

(c) the person is —

(i) the controller or processor;

(ii) a member of staff of the controller or processor; or

(iii) a person acting on behalf of the controller or processor, under any arrangement whatsoever and whether or not the person acts at the behest of the controller or processor.

(2) A specified person commits an offence if —

(a) the specified person does any of the things specified in paragraph (1)(b); and

(b) any such action is done to information submitted to the Information Commissioner by a controller or processor in accordance with a request referred to in paragraph 1(a).

(3) Proceedings for an offence under this regulation may not be instituted except —

(a) in the case of an offence under paragraph (1), by the Information Commissioner or by or with the consent of the Attorney General; or

(b) in the case of an offence under paragraph (2), by or with the consent of the Attorney General.

(See regulation 141(1), which specifies the penalty for offences under this regulation.)

(4) In this regulation, a "specified person" is a person employed by the Information Commissioner or otherwise authorised to assist the Information Commissioner in carrying out any of the Information Commissioner's functions.

The special purposes

130 The special purposes

(1) In this Part, "**the special purposes**" means one or more of the following, —

(a) the purposes of journalism;

(b) academic purposes;

(c) artistic purposes; or

(d) literary purposes.

(2) In this Part, **"special purposes proceedings"** means legal proceedings against a controller or processor under regulation 124 (including proceedings on an application under Article 79 of the applied GDPR) which relate, wholly or partly, to personal data processed for the special purposes.

(3) The Information Commissioner may make a written determination, in relation to the processing of personal data, that —

(a) the personal data are not being processed only for the special purposes;

(b) the personal data are not being processed with a view to the publication by a person of journalistic, academic, artistic or literary material which has not previously been published by the controller; or

(c) carrying out the processing in compliance with a provision of the data protection legislation specified in the determination is not incompatible with the special purposes.

(4) The Information Commissioner must give written notice of the determination to the controller and the processor.

(5) The notice must provide information about the rights of appeal under regulation 120(5).

(6) The determination does not take effect unless one of the following conditions is satisfied —

(a) the period for the controller or the processor to appeal against the determination has ended without an appeal having been brought; or

(b) an appeal has been brought against the determination and —

(i) the appeal and any further appeal in relation to the determination has been decided or has otherwise ended; and

(ii) the time for appealing against the result of the appeal or further appeal has ended without another appeal having been brought.

131 [Revoked][23]

132 Staying special purposes proceedings

(1) In any special purposes proceedings before a court or tribunal, if the controller or processor claims, or it appears to the court or tribunal, that any personal data to which the proceedings relate, —

(a) are being processed only for the special purposes;

(b) are being processed with a view to the publication by any person of journalistic, academic, literary or artistic material; and

(c) have not previously been published by the controller,

the court or tribunal must stay the proceedings.

(2) In considering, for the purposes of paragraph (1)(c), whether material has previously been published, publication in the immediately preceding 24 hours is to be ignored.

(3) Under paragraph (1), the court or tribunal must stay the proceedings until either of the following conditions is met, —

(a) a determination of the Information Commissioner under regulation 130 with respect to the personal data or the processing takes effect;[24]

(b) where the proceedings were stayed on the making of a claim, the claim is withdrawn.

Jurisdiction of courts

133 Jurisdiction

(1) The jurisdiction conferred on a court by the provisions listed in paragraph (2) is exercisable only by the High Court.

(2) Those provisions are, —

(a) regulation 109 (enforcement notices and processing for the special purposes);

(b) regulation 113 (penalty notices and processing for the special purposes);

(c) regulation 124, and Article 79 of the applied GDPR (compliance orders);

(d) regulation 125, and Article 82 of the applied GDPR (compensation).

Definitions

134 Interpretation of Part 7

In this Part —

"assessment notice" has the meaning given in regulation 104;

"the data protection principles" means the principles listed in Article 5(1) of the applied GDPR

"enforcement notice" has the meaning given in regulation 106;

"information notice" has the meaning given in regulation 101;

"penalty notice" has the meaning given in regulation 112;

"penalty variation notice" has the meaning given in paragraph 7 of Schedule 5;

"representative", in relation to a controller or processor, means a person designated by the controller or processor under Article 27 of the applied GDPR to represent the controller or processor with regard to the controller's or processor's obligations under the applied GDPR.

PART 8 – SUPPLEMENTARY AND FINAL PROVISIONS

Regulations

135 Regulations and consultation

(1) The Council of Ministers must consult the Information Commissioner before making regulations under these Regulations, other than regulations made under regulation 28.

(2) A requirement under a provision of these Regulations to consult may be satisfied by consultation before, as well as by consultation after, the provision comes into operation.

Changes to the Data Protection Convention

136 Power to reflect changes to the Data Protection Convention

(1) The Council of Ministers may by regulations make such provision as it considers necessary or appropriate in connection with an amendment of, or an instrument replacing, the Data Protection Convention which has effect, or is expected to have effect, in the Island.

Tynwald procedure – approval required.

(2) The power under paragraph (1) includes power, —

(a) to add to or otherwise amend the Information Commissioner's functions; and

(b) to amend these Regulations.

Rights of the data subject

137 Prohibition of requirement to produce relevant records

(1) Subject to paragraph (6), it is an offence for a person ("P1") to require another person to provide P1 with, or give P1 access to, a relevant record in connection with, —

(a) the recruitment of an employee by P1;

(b) the continued employment of a person by P1; or

(c) a contract for the provision of services to P1.

(2) Subject to paragraph (6), it is an offence for a person ("P2") to require another person to provide P2 with, or give P2 access to, a relevant record if, —

(a) P2 is involved in the provision of goods, facilities or services to the public or a section of the public; and

(b) the requirement is a condition of providing or offering to provide goods, facilities or services to the other person or to a third party.

(3) It is a defence for a person charged with an offence under paragraph (1) or (2) to prove that imposing the requirement, —

(a) was required or authorised by an enactment, by a rule of law or by the order of a court; or

(b) in the particular circumstances, was justified as being in the public interest.

(4) The imposition of the requirement referred to in paragraph (1) or (2) is not to be regarded as justified as being in the public interest on the ground that it would assist in the prevention or detection of crime, given Part 5 of the Police Act 1997 (certificates of criminal records etc.) as extended to the Island by SI 2010/764.

(5) In paragraphs (1) and (2), the references to a person who requires another person to provide or give access to a relevant record include a person who asks another person to do so, —

(a) knowing that, in the circumstances, it would be reasonable for the other person to feel obliged to comply with the request; or

(b) being reckless as to whether, in the circumstances, it would be reasonable for the other person to feel obliged to comply with the request,

and the references to a "requirement" in paragraphs (3) and (4) are to be interpreted accordingly.

(6) Paragraphs (1) and (2) do not apply to actions taken to comply with a requirement under —

(a) the *Proceeds of Crime Act 2008*;

(b) the Anti-Money Laundering and Countering the Financing of Terrorism Code 2015[18]; or

(c) the Money Laundering and Terrorist Financing (Online Gambling) Code 2013[19].

(7) In this regulation, —

"employment" means any employment, including —

(a) work under a contract for services or as an office-holder;

(b) work under an apprenticeship;

(c) work experience as part of a training course or in the course of training for employment; and

(d) voluntary work,

and "employee" is to be interpreted accordingly;

"relevant record" has the meaning given in Schedule 6 and references to a relevant record include —

(a) a part of such a record; and

(b) a copy of, or of part of, such a record.

(See regulation 141(2), which specifies the penalty for offences under this regulation.)

138 Avoidance of certain contractual terms relating to health records

(1) A term or condition of a contract is void in so far as it purports to require a natural person to supply another person with a record which, —

(a) consists of the information contained in a health record; and

(b) has been or is to be obtained by a data subject in the exercise of a data subject access right.

(2) A term or condition of a contract is also void in so far as it purports to require a natural person to produce such a record to another person.

(3) The references in paragraphs (1) and (2) to a record include a part of a record and a copy of all or part of a record.

(4) In this regulation, "data subject access right" means a right under, —

(a) Article 15 of the applied GDPR (right of access by the data subject);

(b) Article 20 of the applied GDPR (right to data portability); or

[18] SD 2015/0102

[19] SD 96/13

(c) Article 14 of the applied LED and regulation 43 of these Regulations (law enforcement processing: right of access by the data subject).

139 Representation of data subjects

(1) In relation to the processing of personal data to which the applied GDPR applies, —

(a) Article 80 of the applied GDPR (representation of data subjects) enables a data subject to authorise a body or other organisation which meets the conditions set out in that Article to exercise certain rights on the data subject's behalf; and

(b) a data subject may also authorise such a body or organisation to exercise the data subject's rights under Article 82 of the applied GDPR (right to compensation).

(2) In these Regulations, references to a **"representative body"**, in relation to a right of a data subject, are to a body or other organisation authorised to exercise the right on the data subject's behalf under Article 80 of the applied GDPR or this regulation.

140 Data subject's rights and other prohibitions and restrictions

(1) An enactment or rule of law prohibiting or restricting the disclosure of information, or authorising the withholding of information, does not remove or restrict the obligations and rights provided for in the provisions listed in paragraph (2).

(2) The provisions providing obligations and rights are, —

(a) Chapter III of the applied GDPR (rights of the data subject); and

(b) Chapter 4 of Part 3 of these Regulations (law enforcement processing: rights of the data subject).

Offences

141 Penalties for offences

(1) A person who commits an offence under regulation 82, 128, 129, or paragraph 15 of Schedule 4 is liable on summary conviction to a fine not exceeding level 5 on the standard scale or to custody for a term not exceeding 6 months, or both.

(2) A person who commits an offence under regulation 91, 103, 126, 127 or 137 is liable, —

(a) on summary conviction, to a fine not exceeding level 5 on the standard scale or to custody for a term not exceeding 6 months, or both; or

(b) on conviction on information, to a fine or to custody for a term not exceeding 2 years.

(3) Paragraphs (4) and (5) apply where a person is convicted of an offence under regulation 126 or 137.

(4) The court by or before which the person is convicted may order a document or other material to be forfeited, destroyed or erased if, —

(a) it has been used in connection with the processing of personal data; and

(b) it appears to the court to be connected with the commission of the offence,

subject to paragraph (5).

(5) If a person, other than the offender, who claims to be the owner of the material, or to be otherwise interested in the material, applies to be heard by the court, the court must not make an order under paragraph (4) without giving the person an opportunity to show why the order should not be made.

(6) Additional offences are created, and corresponding penalties prescribed, in paragraph 5 of Schedule 7.[25]

142 Prosecution

(1) Proceedings for an offence under these Regulations may not be instituted except by the Information Commissioner or by or with the consent of the Attorney General.

(2) Subject to paragraph (4), summary proceedings for an offence under regulation 128 (alteration etc. of personal data to prevent disclosure) may be brought within the period of 6 months beginning with the day on which the prosecutor first knew of evidence that, in the prosecutor's opinion, was sufficient to bring the proceedings.

(3) Such proceedings may not be brought after the end of the period of 3 years beginning with the day on which the offence was committed.

(4) A certificate signed by or on behalf of the prosecutor and stating the day on which the 6 month period described in paragraph (2) began is conclusive evidence of that fact.

(5) A certificate purporting to be signed as described in paragraph (4) is to be treated as so signed unless the contrary is proved.

143 Liability of directors etc.

(1) Paragraph (2) applies where, —

(a) an offence under these Regulations has been committed by a body corporate; and

(b) it is proved to have been committed with the consent or connivance of or to be attributable to neglect on the part of, —

(i) a director, manager, secretary or similar officer of the body corporate; or

(ii) a person who was purporting to act in such a capacity.

(2) The director, manager, secretary, officer or person, as well as the body corporate, commits the offence and liable to be proceeded against and punished accordingly.

(3) Where the affairs of a body corporate are managed by its members, paragraphs (1) and (2) apply in relation to the acts and omissions of a member in connection with the member's management functions in relation to the body as if the member were a director of the body corporate.

(4) Paragraph (5) applies where, —

(a) an offence under these Regulations has been committed by a partnership; and

(b) the contravention in question is proved to have occurred with the consent or connivance of, or to be attributable to any neglect on the part of, a partner.

(5) The partner, as well as the partnership, commits the offence and liable to be proceeded against and punished accordingly.

144 Recordable offences

(1) The Police Records (Recordable Offences) Regulations 1999[20] have effect as if the offences under the following provisions were listed in the Schedule to those Regulations, —

(a) regulation 82;

(b) regulation 91;

(c) regulation 103;

(d) regulation 126;

(e) regulation 127;

(f) regulation 128;

(g) regulation 129;

(h) regulation 137;

(i) paragraph 15 of Schedule 4.

(2) Regulations under section 30(4) of the *Police Powers and Procedures Act 1998* may repeal paragraph (1).

[20] SD 22/99

145 Guidance about codes of practice

(1) The Information Commissioner must produce and publish guidance about how the Information Commissioner proposes to perform the duty under section 76(5) of the *Police Powers and Procedures Act 1998* (duty to have regard to codes of practice under that Act when investigating offences and charging offenders) in connection with offences under these Regulations.

(2) The Information Commissioner, —

(a) may alter or replace the guidance; and

(b) must publish any altered or replacement guidance.

(3) The Information Commissioner must consult the Council of Ministers before publishing guidance under this regulation (including any altered or replacement guidance).

(4) The Information Commissioner must arrange for guidance under this regulation (including any altered or replacement guidance) to be laid before Tynwald.

The Tribunal

146 Tribunal Procedure Rules

(1) Tribunal Procedure Rules may make provision for regulating, —

(a) the exercise of the rights of appeal conferred by regulation 120; and

(b) the exercise of the rights of data subjects under regulation 123, including their exercise by a representative body.

(2) In relation to proceedings involving the exercise of those rights, Tribunal Procedure Rules may make provision about, —

(a) securing the production of material used for the processing of personal data; and

(b) the inspection, examination, operation and testing of equipment or material used in connection with the processing of personal data.

(3) Paragraph 5 of Schedule 8 makes additional provisions in respect of Tribunal Procedure Rules.

147 Disclosure of information to Tribunal

No enactment or rule of law prohibiting or restricting the disclosure of information precludes a person from providing the Tribunal with information necessary for the discharge of the Tribunal's functions under data protection legislation.

General

148 Application to Government

(1) Except as provided in paragraph (2), a Department, a Statutory Board and an office of the Government is subject to the same obligations and liabilities under these Regulations as a private person; and for the purposes of these Regulations —

(a) an employee of the Public Services Commission acting under the direction of any Department or Statutory Board must be treated as an employee of that Department or Board;

(b) such employee must be treated as an employee of the Treasury.

(2) For the purposes of this Act a member of the Isle of Man Constabulary must be treated as an employee of the Chief Constable.

149 Application to Tynwald

(1) Parts 1, 2, 5 and 6 to 8 of these Regulations apply to the processing of personal data by or on behalf of Tynwald and its branches.

(2) Where the purposes for which and the manner in which personal data are, or are to be, processed are determined by or on behalf of Tynwald and its branches, the controller in respect of that data for the purposes of the applied GDPR and these Regulations is the Clerk of Tynwald.

(3) Where the purposes for which and the manner in which personal data are, or are to be, processed are determined by or on behalf of the Legislative Council, the controller in respect of that data for the purposes of the applied GDPR and these Regulations is the Clerk of the Legislative Council.

(4) The following provisions apply to a person acting on behalf of Tynwald and its branches as they apply to any other person, —

(a) regulation 126;

(b) regulation 127;

(c) regulation 128;

(d) paragraph 15 of Schedule 4.

(5) Subject to paragraph (4), nothing in paragraph (2) or (3) makes the Clerk of Tynwald or the Deputy Clerk of Tynwald liable to prosecution under the applied GDPR or these Regulations.

150 Savings and transitional arrangements

Schedule 11 sets out the savings and transitional arrangements attendant on the coming into operation of these Regulations.

MADE 4 JUNE 2018

SCHEDULE 1

COMPETENT AUTHORITIES

Regulation 28(1)(a)

1. The Cabinet Office.

2. The Department of Education, Sport and Culture.

3. The Department for Enterprise.

4. The Department of Environment, Food and Agriculture.

5. The Department of Home Affairs.

6. The Department of Health and Social Care.

7. The Department of Infrastructure.

8. The Treasury.

9. The Isle of Man Office of Fair Trading.

10. The Isle of Man Financial Services Authority.

11. The Isle of Man Post Office.

12. The Manx Utilities Authority.

13. The Communications Commission.

14. The Isle of Man Gambling Supervision Commission.

15. The Public Sector Pensions Authority.

16. Her Majesty's Attorney General and the Attorney General's Chambers.

17. The Chief Constable of the Isle of Man Constabulary and any other police force established by the Department of Home Affairs pursuant to section 1 of the *Police Act 1993*.

18. Any prison or institution provided pursuant to section 11 of the *Custody Act 1995* or other like authorities whether or not constituting part of a Department or Statutory Board.

19. A provider of probation services acting in pursuance of any statutory authority for the provision of such services.

20. A provider of youth justice services acting in pursuance of any statutory authority for the provision of such services.

21. Any public customs and excise authority whether or not constituting part of a Department or Statutory Board.

22. Any public passport and immigration authority whether or not constituting part of a Department or Statutory Board.

23. Any port authority in the Island, whether or not constituting part of a Department or Statutory Board.

24. The Financial Intelligence Unit established pursuant to the *Financial Intelligence Unit Act 2016.*

25. Local Authorities constituted pursuant to the Local Government Consolidation Act 1916.

26. The General Registry and any other public registry in the Island.

27. All courts in the Island.

28. All tribunals established and operated in accordance with the *Tribunals Act 2006*.

29. The Information Commissioner.

30. A coroner within the meaning of the *Coroners Act 1983.*

31. The Road Transport Licensing Committee established pursuant to section 1 of the *Road Transport Act 2001*.

32. Any person who has entered into a contract with any other competent authority that has responsibility for securing electronic monitoring, parole or bail conditions of a natural person.

SCHEDULE 2

SPECIAL CATEGORIES OF PERSONAL DATA AND CRIMINAL CONVICTIONS ETC. DATA

Regulation 12

PART 1 – CONDITIONS RELATING TO EMPLOYMENT, HEALTH AND RESEARCH ETC

Employment, social security and social protection

1 Employment, social security and social protection[26]

(1) This condition is met if the processing is necessary for the purposes of performing or exercising obligations or rights of the controller or the data subject under employment law, social security law or the law relating to social protection.[27]

(2) See also the additional safeguards in Part 4 of this Schedule.

(3) In this paragraph, —

"social security law" includes any of the branches of social security listed in Article 3(1) of Regulation (EC) No. 883/2004 of the European Parliament and of the Council of 29 April 2004 on the co-ordination of social security systems (as amended from time to time);[28]

"social protection" includes an intervention described in Article 2(b) of Regulation (EC) No. 458/2007 of the European Parliament and of the Council of 25 April 2007 on the European system of integrated social protection statistics (ESSPROS) (as amended from time to time).

2 Health or social care purposes

(1) This condition is met if the processing is necessary for health or social care purposes.

(2) In this paragraph "health or social care purposes" means the purposes of, —

(a) preventive or occupational medicine;

(b) the assessment of the working capacity of an employee;

(c) medical diagnosis;

(d) the provision of health care or treatment;

(e) the provision of social care; or

(f) the management of health care systems or services or social care systems or services.

(3) See also the conditions and safeguards in Article 9(3) of the applied GDPR (obligations of secrecy) and regulation 13(1).

3 Public health

This condition is met if the processing —

(a) is necessary for reasons of public interest in the area of public health; and

(b) is carried out —

(i) by or under the supervision of a health professional; or

(ii) by another person who in the circumstances owes a duty of confidentiality under an enactment or rule of law.

4 Research, etc.

This condition is met if the processing —

(a) is necessary for archiving purposes, scientific or historical research purposes or statistical purposes;

(b) is carried out in accordance with Article 89(1) of the applied GDPR (as supplemented by regulation 18); and

(c) in the public interest.

PART 2 – SUBSTANTIAL PUBLIC INTEREST CONDITIONS

5 Reasons of substantial public interest

(1) A condition in this Part of this Schedule is met only if, in addition to any other requirements specified in respect of each specific condition, the processing is necessary for reasons of substantial public interest.

(2) See also the additional safeguards in Part 4 of this Schedule.

6 Tynwald, statutory and government purposes

(1) This condition is met if the processing is necessary for a purpose listed in subparagraph (2).

(2) Those purposes are —

(a) the administration of justice;

(b) the exercise of a function of Tynwald and its branches;

(c) the exercise of a function conferred on a person by an enactment;

(d) the exercise of a function of the Crown, a Department or a Statutory Board.

7 Equality of opportunity treatment

(1) This condition is met if the processing —

(a) is of a specified category of personal data; and

(b) the existence or absence of equality or opportunity or treatment between groups of people specified in relation to that category with a view to enabling such equality to be promoted or maintained,

subject to the exceptions in subparagraphs (3) to (5).

(2) In subparagraph (1), "specified" means specified in the following table —

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 origins
Personal data revealing religious or philosophical beliefs	People holding different religious or philosophical beliefs
Data concerning health	People with different states of physical or mental health
Personal data concerning a natural person's sexual orientation	People of different sexual orientation

(3) Processing does not meet the condition in subparagraph (1) if —

(a) it is carried out for the purposes of measures or decisions with respect to a particular data subject; and

(b) it is carried out without that data subject's consent.

(4) Processing does not meet the condition in subparagraph (1) if it is likely to cause substantial damage or substantial distress to a natural person.

(5) Processing does not meet the condition in subparagraph (1) if —

(a) a natural person who is the data subject (or one of the data subjects) has given notice in writing to the controller requiring the controller not to process personal data in respect of which the natural person is the data subject (and has not given notice in writing withdrawing that requirement);

(b) the notice gave the controller a reasonable period in which to stop processing such data; and

(c) that period has ended.

8 Preventing or detecting unlawful acts

(1) This condition is met if the processing —

(a) is necessary for the purposes of the prevention or detection of an unlawful act; and

(b) must be carried out without the consent of the data subject so as not to prejudice those purposes.

(2) In this paragraph, **"act"** includes a failure to act.

9 Protecting the public against dishonesty etc.

(1) This condition is met if the processing, —

(a) is necessary for the exercise of a protective function; and

(b) must be carried out without the consent of the data subject so as not to prejudice the exercise of that function.

(2) In this paragraph, "protective function" means a function which is intended to protect members of the public against —

(a) dishonesty, malpractice or other seriously improper conduct;

(b) unfitness or incompetence;

(c) mismanagement in the administration of a body or association; or

(d) failures in services provided by a body or association.

10 Journalism etc. in connection with unlawful acts and dishonesty etc.

(1) This condition is met if, —

(a) the processing consists of the disclosure of personal data for the special purposes;

(b) it is carried out in connection with a matter described in subparagraph (2);

(c) it is carried out with a view to the publication of the personal data by any person; and

(d) the controller reasonably believes that publication of the personal data would be in the public interest.

(2) The matters mentioned in subparagraph (1)(b) are any of the following (whether alleged or established)—

(a) the commission of an unlawful act by a person;

(b) dishonesty, malpractice or other seriously improper conduct of a person;

(c) unfitness or incompetence of a person;

(d) mismanagement in the administration of a body or association;

(e) a failure in services provided by a body or association.

(3) In this paragraph, —

"act" includes a failure to act;

"the special purposes" means —

(a) the purposes of journalism;

(b) academic purposes;

(c) artistic purposes;

(d) literary purposes.

11 Preventing fraud

(1) This condition is met if the processing —

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

(b) consists of, —

(i) the disclosure of personal data by a person as a member of an anti-fraud organisation;

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

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

(2) In this paragraph, "anti-fraud organisation" has the same meaning as in section 68 of the Serious Crime Act 2007 (of Parliament).

12 Suspicion of terrorist financing or money laundering

This condition is met if the processing is necessary —

(a) for the purposes of making a disclosure in good faith; or

(b) in order to comply with the requirements of

(i) the *Proceeds of Crime Act 2008*;

(ii) the Anti-Money Laundering and Countering the Financing of Terrorism Code 2015[21]; or

(iii) the Money Laundering and Terrorist Financing (Online Gambling) Code 2013[22].

[21] SD 2015/0102

[22] SD 96/13

13 Counselling etc.

(1) This condition is met if the processing

(a) is necessary for the provision of confidential counselling, advice or support or of another similar service provided confidentially; and

(b) is carried out without the consent of the data subject for a reason listed in subparagraph (2).

(2) The reasons mentioned in subparagraph (1)(b) are —

(a) in the circumstances, consent to the processing cannot be given by the data subject;

(b) in the circumstances, the controller cannot reasonably be expected to obtain the consent of the data subject to the processing; or

(c) the processing must be carried out without the consent of the data subject because obtaining the consent of the data subject would prejudice the provision of the service mentioned in subparagraph (1)(a).

14 Insurance

(1) This condition is met if the processing —

(a) is necessary for an insurance purpose;

(b) is of personal data revealing racial or ethnic origin, religious or other philosophical beliefs or trade union membership, genetic data or data concerning health; or

(c) is necessary for reasons of substantial public interest, subject to subparagraphs (2) and (3).

(2) Subparagraph (3) applies where —

(a) the processing is not carried out for the purposes of measures or decisions with respect to the data subject; and

(b) the data subject does not have and is not expected to acquire —

(i) rights against, or obligations in relation to, a person who is an insured person under an insurance contract to which the insurance purpose mentioned in subparagraph (1)(a) relates; or

(ii) other rights or obligations in connection with such a contract.

(3) Where this subparagraph applies, the processing does not meet the condition in subparagraph (1) unless, in addition to meeting the requirements in that subparagraph, it can reasonably be carried out without the consent of the data subject.

(4) For the purposes of subparagraph (3), processing can reasonably be carried out without the consent of the data subject only where —

(a) the controller cannot reasonably be expected to obtain the consent of the data subject; and

(b) the controller is not aware of the data subject's withholding consent.

(5) In this paragraph —

"insurance contract" means a contract of general insurance or long term insurance;

"insurance purpose" means —

(a) advising on, arranging, underwriting or administering an insurance contract;

(b) administering a claim under an insurance contract; or

(c) exercising a right, or complying with an obligation, arising in connection with an insurance contract, including a right or obligation arising under an enactment or rule of law;

"listed applied GDPR provisions" means the provisions of the applied GDPR listed in paragraph 9 of Schedule 9.

(6) The reference in subparagraph (4)(b) to a data subject withholding consent does not include a data subject merely failing to respond to a request for consent.

(7) Terms used in the definition of "insurance contract" in subparagraph (5) and also in an order made under section 22 of the Financial Services and Markets Act 2000 (of Parliament) have the same meaning in that definition as they have in that order.[29]

14A Extension of conditions referring to substantial public interest

The condition referred to in paragraph 14 is met if the processing would meet a condition in this Schedule but for an express requirement for the processing to be necessary for reasons of substantial public interest.[30]

15 Third party data processing for group insurance policies and insurance on the life of another

(1) This condition is met if the processing —

(a) is necessary for an insurance purpose;

(b) is of personal data revealing racial or ethnic origin, religious or philosophical beliefs or trade union membership, genetic data or data concerning health; and

(c) is necessary for reasons of substantial public interest,

subject to subparagraphs (2) and (3).

(2) Subparagraph (3) applies where —

(a) the processing is not carried out for the purposes of measures or decisions with respect to the data subject; and

(b) the data subject does not have and is not expected to acquire —

(i) rights against, or obligations in relation to, a person who is an assured person under an insurance contract to which the insurance purpose mentioned in subparagraph (1)(a) relates; or

(ii) other rights or obligations in connection with such a contract.

(3) Where this subparagraph applies, the processing does not meet the condition in subparagraph (1) unless, in addition to meeting the requirements in that subparagraph, it can reasonably be carried out without the consent of the data subject.

(4) For the purposes of subparagraph (3), processing can reasonably be carried out without the consent of the data subject only where —

(a) the controller cannot reasonably be expected to obtain the consent of the data subject; and

(b) the controller is not aware of the data subject withholding consent.

(5) In this paragraph —

"insurance contract" means a contract of general insurance or long-term insurance;

"insurance purpose" means —

(a) advising on, arranging, underwriting or administering an insurance contract;

(b) administering a claim under an insurance contract; or

(c) exercising a right, or complying with an obligation, arising in connection with an insurance contract, including a right or obligation arising under an enactment or rule of law.

(6) The reference in subparagraph (4)(b) to the data subject withholding consent does not include a data subject merely failing to respond to a request for consent.

(7) Terms used in the definition of "long-term insurance contract" in section 54 of the *Insurance Act 2008* have the same meaning, and "insurance contract" must be construed accordingly.

(8) This condition is met if the processing —

(a) would meet the condition in paragraph 14 of this Schedule ("the insurance condition"); or

(b) would meet the condition in paragraph 14A by virtue of the insurance condition,

but for the requirement for the processing to be processing of a category of personal data specified in paragraph 14(2)(b).[31]

16 Occupational pensions

(1) This condition is met if the processing —

(a) is necessary for the purpose of making a determination in connection with eligibility for, or benefits payable under, an occupational pension scheme;

(ab) is of data concerning health, which relates to a data subject who is the parent, grandparent, great grandparent or sibling of a member of the occupational pension scheme;[32]

(b) is not carried out for the purposes of measures or decisions with respect to the data subject; and

(c) can reasonably be carried out without the consent of the data subject.

(2) For the purposes of subparagraph (1)(c), processing can reasonably be carried out without the consent of the data subject only where —

(a) the controller cannot reasonably be expected to obtain the consent of the data subject; and

(b) the controller is not aware of the data subject withholding consent.

(3) In this paragraph —

"member", in relation to an occupational pension scheme, includes an individual who is seeking to become a member of the occupational pension scheme;

"occupational pension scheme" has the meaning given in section 1 of the Pension Schemes Act 1993 (of Parliament) as applied to the Island by SD 531/95.[33]

17 Political parties

(1) This condition is met if the processing —

(a) is of personal data revealing political opinions;

(b) falls within Part IA of the *Representation of the People Act 1995*; and

(c) is necessary for the purposes of the person's or organisation's political activities,

subject to the exceptions in subparagraphs (2) and (3).

(2) Processing does not meet the condition in subparagraph (1) if it is likely to cause substantial damage or substantial distress to a person.

(3) Processing does not meet the condition in subparagraph (1) if —

(a) a natural person who is the data subject (or one of the data subjects) has given notice in writing to the controller requiring the controller not to process personal data in respect of which the natural person is the data subject (and has not given notice in writing withdrawing that requirement);

(b) the notice gave the controller a reasonable period in which to stop processing such data; and

(c) that period has ended.

(4) In this paragraph, "political activities" include campaigning, fund-raising, political surveys and case-work.

18 Elected representatives responding to requests

(1) This condition is met if —

(a) the processing is carried out —

(i) by an elected representative or a person acting with the authority of such a representative;

(ii) in connection with the discharge of the elected representative's functions; and

(iii) in response to a request by a natural person that the elected representative take action on behalf of the natural person; and

(b) the processing is necessary for the purposes of, or in connection with, the action reasonably taken by the elected representative in response to that request,

subject to subparagraph (2).

(2) Where the request is made by a natural person other than the data subject, the condition in subparagraph (1) is met only if the processing must be carried out without the consent of the data subject for one of the following reasons —

(a) in the circumstances, consent to the processing cannot be given by the data subject;

(b) in the circumstances, the elected representative cannot reasonably be expected to obtain the consent of the data subject to the processing;

(c) obtaining the consent of the data subject would prejudice the action taken by the elected representative;

(d) the processing is necessary in the interests of another natural person and the data subject has withheld consent unreasonably.

(3) In this paragraph and paragraph 19, "elected representative" means a Member of the House of Keys or a member elected to a local authority.[34]

(4) For the purposes of subparagraph (3), a person who is a member of the House of Keys immediately before it is dissolved is to be treated as if the person were such a member until the end of the fourth day after the day on which the subsequent general election in relation to the House of Keys is held.

19 Disclosure to elected representatives

(1) This condition is met if —

(a) the processing consists of the disclosure of personal data, —

(i) to an elected representative or a person acting with the authority of such a representative; and

(ii) in response to a communication to the controller from that representative or person which was made in response to a request from a natural person,

(b) the personal data are relevant to the subject matter of that communication; and

(c) the disclosure is necessary for the purpose of responding to that communication,

subject to subparagraph (2).

(2) Where the request to the elected representative came from a natural person other than the data subject, the condition in subparagraph (1) is met only if the disclosure must be made without the consent of the data subject for one of the following reasons, —

(a) in the circumstances, consent to the processing cannot be given by the data subject;

(b) in the circumstances, the elected representative cannot reasonably be expected to obtain the consent of the data subject to the processing;

(c) obtaining the consent of the data subject would prejudice the action taken by the elected representative;

(d) the processing is necessary in the interests of another natural person and the data subject has withheld consent unreasonably.

(3) In this paragraph, "elected representative" has the same meaning as in paragraph 18.

20 Informing elected representatives about prisoners

(1) This condition is met if, —

(a) the processing consists of the processing of personal data about a prisoner for the purpose of informing a member of the House of Keys; and

(b) the member is under an obligation not to further disclose the personal data.

(2) The references in subparagraph (1) to personal data about, and to informing someone about, a prisoner include personal data about, and informing someone about, arrangements for the prisoner's release.

(3) In this paragraph, —

"prison" includes a young offender institution;

"prisoner" means a person detained in a prison.

21 Standards of behaviour in sport

(1) This condition is met if the processing —

(a) is necessary for the purposes of measures designed to protect the integrity of a sport or a sporting event;

(b) must be carried out without the consent of the data subject so as not to prejudice those purposes; and

(c) is necessary for reasons of substantial public interest.

(2) In subparagraph (1)(a), the reference to measures designed to protect the integrity of a sport or a sporting event is a reference to measures designed to protect a sport or a sporting event against —

(a) dishonesty, malpractice or other seriously improper conduct; or

(b) failure by a person participating in the sport or event in any capacity to comply with standards of behaviour set by a body or association with responsibility for the sport or event.[35]

22 Safeguarding of children and of natural persons at risk

(1) This condition is met if —

(a) the processing is necessary for the purposes of —

(i) protecting a natural person from neglect or physical, mental or emotional harm; or

(ii) protecting the physical, mental or emotional wellbeing of a natural person;

(b) the natural person is —

(i) aged under 18; or

(ii) aged 18 or over and at risk; and

(c) the processing is carried out without the consent of the data subject for one of the reasons listed in subparagraph (2).

(2) The reasons mentioned in subparagraph (1)(c) are —

(a) in the circumstances, consent to the processing cannot be given by the data subject;

(b) in the circumstances, the controller cannot reasonably be expected to obtain the consent of the data subject to the processing;

(c) the processing must be carried out without the consent of the data subject because obtaining the consent of the data subject would prejudice the provision of the protection mentioned in subparagraph (1)(a).

(3) For the purposes of this paragraph, a natural person aged 18 or over is "at risk" if the controller has reasonable cause to suspect that the natural person —

(a) has needs for care and support;

(b) is experiencing or is at risk of —

(i) neglect; or

(ii) physical, mental or emotional harm; and

(c) as a result of those needs is unable to protect himself or herself against the neglect or harm or the risk of it.

(4) In subparagraph (1)(a), the reference to the protection of a natural person or of the wellbeing of a natural person includes both protection relating to a particular natural person and protection relating to a type of natural person.

23 Safeguarding of economic wellbeing of certain natural persons

(1) This condition is met if the processing —

(a) is necessary for the purposes of protecting the economic wellbeing of a natural person at economic risk who is aged 18 or over;

(b) is of data concerning health;

(c) is carried our without the consent of the data subject for one of the reasons listed in subparagraph (2); and

(d) is necessary for reasons of substantial public interest.

(2) The reasons mentioned in subparagraph (1)(c) are —

(a) in the circumstances, consent to the processing cannot be given by the data subject;

(b) in the circumstances, the controller cannot reasonably be expected to obtain the consent of the data subject to the processing;

(c) the processing must be carried out without the consent of the data subject because obtaining the consent of the data subject would prejudice the provision of the protection mentioned in subparagraph (1)(a).

(3) In this paragraph, "natural person at economic risk" means a natural person who is less able to protect his or her economic wellbeing by reason of physical or mental injury, illness or disability.

PART 3 – ADDITIONAL CONDITIONS RELATING TO CRIMINAL CONVICTIONS ETC

24 Consent

This condition is met if the data subject has given consent to the processing.

25 Protecting natural person's vital interests

This condition is met if —

(a) the processing is necessary to protect the vital interests of a natural person; and

(b) the data subject is physically or legally incapable of giving consent.

26 Processing by not-for-profit bodies

This condition is met if the processing is carried out, —

(a) in the course of its legitimate activities with appropriate safeguards by a foundation, association or other not-for-profit body with a political, philosophical, religious or trade union aim, and

(b) on condition that, —

(i) the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes, and

(ii) the personal data are not disclosed outside that body without the consent of the data subjects.

27 Personal data in the public domain

This condition is met if the processing relates to personal data which —

(a) are manifestly made public by the data subject; or

(b) necessarily falls within the scope of the screening obligations imposed on controllers or processors under —

(i) the *Proceeds of Crime Act 2008*;

(ii) the Anti-Money Laundering and Countering the Financing of Terrorism Code 2015[23]; or

(iii) the Money Laundering and Terrorist Financing (Online Gambling) Code 2013[24].

28 Legal claims and judicial acts

(1) This condition is met if the processing —

(a) is necessary for the purpose of, or in connection with, any legal proceedings (including prospective legal proceedings);

(b) is necessary for the purpose of obtaining legal advice; or

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

(2) This condition is met if the processing is necessary when a court or tribunal is acting in its judicial capacity.[36]

28A Publication of legal judgments

This condition is met if the processing —

(a) consists of the publication of a judgment or other decision of a court or tribunal; or

(b) is necessary for the purposes of publishing such a judgment or decision.[37]

29 Administration of accounts used in commission of offences involving children

(1) This condition is met if, —

(a) the processing is of personal data about a conviction or caution for an offence listed in subparagraph (2); and

(b) the processing is necessary for the purpose of administering an account relating to the payment card used in the commission of the offence or cancelling that payment card.

(2) Those offences are an offence —

(a) under the *Adoption Act 1984*;

(b) under the *Child Custody Act 1987*;

(c) under the *Children and Young Persons Act 1966*;

(d) under the *Children and Young Persons Act 2001*; or

[23] SD 2015/0102

[24] SD 96/13

(e) against a child under the *Sexual Offences Act 1992*,

or incitement to commit an offence under any of those enactments.

(3) See also the additional safeguards in Part 4 of this Schedule.

(4) In this paragraph —

"caution" means a caution given to any person in the Island in respect of an offence which, at the time when the caution is given, is admitted;

"conviction" has the same meaning as in the *Rehabilitation of Offenders Act 2001*;

"payment card" includes a credit card, a charge card and a debit card.

PART 4 –ADDITIONAL SAFEGUARDS

30 Additional safeguard: record of processing

A record maintained by the controller, or the controller's representative, under Article 30 of the applied GDPR in respect of the processing of personal data must include the following information —

(a) which condition is relied on; and

(b) how the processing satisfies Article 6 of the applied GDPR (lawfulness of processing).

SCHEDULE 3

CO-OPERATION AND MUTUAL ASSISTANCE WITH RESPECT TO THE DATA PROTECTION CONVENTION

Regulation 81(3)

1 Co-operation between the Information Commissioner and foreign designated authorities

(1) The Information Commissioner must, at the request of a foreign designated authority, —

(a) provide that authority with such information referred to in Article 13(3)(a) of the Data Protection Convention (information on law and administrative practice in the field of data protection) as is the subject of the request, and

(b) take appropriate measures in accordance with Article 13(3)(b) of the Data Protection Convention for providing that authority with information relating to the processing of personal data in the Island.

(2) The Information Commissioner may ask a foreign designated authority, —

(a) to provide the Information Commissioner with information referred to in Article 13(3)(a) of the Data Protection Convention, or

(b) to take appropriate measures to provide such information.

2 Assisting persons resident outside the Island with requests under Article 14 of the Convention

(1) This paragraph applies where a request for assistance in exercising any of the rights referred to in Article 8 of the Data Protection Convention in the Island is made by a person resident outside the Island, including where the request is forwarded to the Information Commissioner through the Council of Ministers or a foreign designated authority.

(2) The Information Commissioner must take appropriate measures to assist the person to exercise those rights.

3 Assisting Island residents with requests under Article 8 of the Convention

(1) This paragraph applies where a request for assistance in exercising any of the rights referred to in Article 8 of the Data Protection Convention in a country or territory (other than the Island) specified in the request is, —

(a) made by a person resident in the Island, and

(b) submitted through the Information Commissioner under Article 14(2) of the Data Protection Convention.

(2) If the Information Commissioner is satisfied that the request contains all necessary particulars referred to in Article 14(3) of the Data Protection Convention, the Information Commissioner must send the request to the foreign designated authority in the specified country or territory.

(3) Otherwise, the Information Commissioner must, where practicable, notify the person making the request of the reasons why the Information Commissioner is not required to assist.

4 Restrictions on use of information

Where the Information Commissioner receives information from a foreign designated authority as a result of a request made or received by the Information Commissioner, the Information Commissioner may use the information only for the purposes specified in the request.

5 Foreign designated authority

In this Part of this Schedule, "foreign designated authority" means an authority designated for the purposes of Article 13 of the Data Protection Convention by a party, other than the Island, which is bound by that Data Protection Convention.

SCHEDULE 4

POWERS OF ENTRY AND INSPECTION

Regulations 104 and 111

1 Issue of warrants in connection with non-compliance and offences

(1) Subparagraph (2) applies if a Deemster or the High Bailiff is satisfied by information on oath supplied by the Information Commissioner that, —

(a) there are reasonable grounds for suspecting that, —

(i) a controller or processor has failed or is failing as described in regulation 106(2); or

(ii) an offence under these Regulations has been or is being committed; and

(b) there are reasonable grounds for suspecting that evidence of the failure or of the commission of the offence is to be found on premises specified in the information.

(2) The Deemster or High Bailiff may grant a warrant to the Information Commissioner.

2 Issue of warrants in connection with assessment notices

(1) This paragraph applies if a Deemster or the High Bailiff is satisfied by information on oath supplied by the Information Commissioner that a controller or processor has failed to comply with a requirement imposed by an assessment notice.

(2) The Deemster or High Bailiff may, for the purpose of enabling the Information Commissioner to determine whether the controller or processor has complied or is complying with the data protection legislation, grant a warrant to the Information Commissioner in relation to premises that were specified in the assessment notice.

(3) The grant of a warrant under this paragraph is subject to the right of the controller or processor to appeal to the Staff of Government Division in accordance with the relevant rules of court.

3 Restrictions on issuing warrants: processing for the special purposes

The Deemster or High Bailiff must not issue a warrant under this Schedule in respect of personal data processed for the special purposes unless a determination under regulation 130 with respect to the data or the processing has taken effect.

4 Restriction on issuing warrants: procedural requirements

(1) The Deemster or High Bailiff must not issue a warrant under this Schedule unless satisfied that, —

(a) the conditions in subparagraphs (2) to (4) are met;

(b) compliance with those conditions would defeat the object of entry to the premises in question; or

(c) the Information Commissioner requires access to the premises in question urgently.

(2) The first condition is that the Information Commissioner has given 7 days' notice in writing to the occupier of the premises in question demanding access to the premises.

(3) The second condition is that, —

(a) access to the premises was demanded at a reasonable hour and was unreasonably refused; or

(b) entry to the premises was granted but the occupier unreasonably refused to comply with a request by the Information Commissioner or the Information Commissioner's officers or staff to be allowed to do any of the things referred to in paragraph 5.

(4) The third condition is that, since the refusal, the occupier of the premises, —

(a) has been notified by the Information Commissioner of the application for the warrant; and

(b) has had an opportunity to be heard by the judge on the question of whether or not the warrant should be issued.

(5) In determining whether the first condition is met, an assessment notice given to the occupier is to be disregarded.

5 Content of warrants

(1) A warrant issued under this Schedule must authorise the Information Commissioner or any of the Information Commissioner's officers or staff, —

(a) to enter the premises;

(b) to search the premises; and

(c) to inspect, examine, operate and test any equipment found on the premises which is used or intended to be used for the processing of personal data.

(2) A warrant issued under paragraph 1 must authorise the Information Commissioner or any of the Information Commissioner's officers or staff, —

(a) to inspect and seize any documents or other material found on the premises which may be evidence of the failure or offence mentioned in that paragraph;

(b) to require any person on the premises to provide an explanation of any document or other material found on the premises; and

(c) to require any person on the premises to provide such other information as may reasonably be required for the purpose of determining whether the controller or processor has failed or is failing as described in regulation 106(2).

(3) A warrant issued under paragraph 2 must authorise the Information Commissioner or any of the Information Commissioner's officers or staff, —

(a) to inspect and seize any documents or other material found on the premises which may enable the Information Commissioner to determine whether the controller or processor has complied or is complying with the data protection legislation;

(b) to require any person on the premises to provide an explanation of any document or other material found on the premises; and

(c) to require any person on the premises to provide such other information as may reasonably be required for the purpose of determining whether the controller or processor has complied or is complying with the data protection legislation.

(4) A warrant issued under this Schedule must authorise the Information Commissioner or any of the Information Commissioner's officers or staff to do the things described in subparagraphs (1) to (3) at any time in the period of 7 days beginning with the day on which the warrant is issued.

6 Copies of warrants

The Deemster or High Bailiff who issues a warrant under this Schedule must, —

(a) issue two copies of it; and

(b) certify them clearly as copies.

7 Execution of warrants: reasonable force

A person executing a warrant issued under this Schedule may use such reasonable force as may be necessary.

8 Execution of warrants: time when executed

A warrant issued under this Schedule may be executed only at a reasonable, hour, unless it appears to the person executing it that there are grounds for suspecting that exercising it at a reasonable hour would defeat the object of the warrant.

9 Execution of warrants: occupier of premises

(1) If an occupier of the premises in respect of which a warrant is issued under this Schedule is present when the warrant is executed, the person executing the warrant must, —

(a) show the occupier the warrant; and

(b) give the occupier a copy of it.

(2) Otherwise, a copy of the warrant must be left in a prominent place on the premises.

10 Execution of warrants: seizure of documents

(1) This paragraph applies where a person executing a warrant under this Schedule seizes something.

(2) The person must, on request —

(a) give a receipt for it; and

(b) give an occupier of the premises a copy of it.

(3) Subparagraph (2)(b) does not apply if the person executing the warrant considers that providing a copy would result in undue delay.

(4) Anything seized may be retained for so long as is necessary in all the circumstances.

11 Matters exempt from inspection and seizure: privileged communications

(1) The powers of inspection and seizure conferred by a warrant issued under this Schedule are not exercisable in respect of a communication which is made, —

(a) between a professional legal adviser and the adviser's client; and

(b) in connection with the giving of legal advice to the client with respect to obligations, liabilities or rights under the data protection legislation.

(2) The powers of inspection and seizure conferred by a warrant issued under this Schedule are not exercisable in respect of a communication which is made, —

(a) between a professional legal adviser and the adviser's client or between such an adviser or client and another person;

(b) in connection with or in contemplation of proceedings under or arising out of the data protection legislation; and

(c) for the purposes of such proceedings.

(3) Subparagraphs (1) and (2) do not prevent the exercise of powers conferred by a warrant issued under this Schedule in respect of, —

(a) anything in the possession of a person other than the professional legal adviser or the adviser's client; or

(b) anything held with the intention of furthering a criminal purpose.

(4) The references to a communication in subparagraphs (1) and (2) include, —

(a) a copy or other record of the communication; and

(b) anything enclosed with or referred to in the communication, if made as described in subparagraph (1)(b) or in subparagraph (2)(b) and (c).

(5) In subparagraphs (1) to (3), the references to the client of a professional legal adviser include a person acting on behalf of such a client.

12 Matters exempt from inspection and seizure: Tynwald privilege

The powers of inspection and seizure conferred by a warrant issued under this Schedule are not exercisable where their exercise would involve an infringement of the privileges of either the House of Keys or the Legislative Council.

13 Partially exempt material

(1) This paragraph applies if a person in occupation of premises in respect of which a warrant is issued under this Schedule objects to the inspection or seizure of any material under the warrant on the grounds that it consists partly of matters in respect of which those powers are not exercisable.

(2) The person must, if the person executing the warrant so requests, provide that person with a copy of so much of the material as is not exempt from those powers.

14 Return of warrants

(1) Where a warrant issued under this Schedule is executed, —

(a) it must be returned to the court from which it was issued after being executed; and

(b) the person by whom it is executed must write on the warrant a statement of the powers that have been exercised under the warrant.

(2) Where a warrant issued under this Schedule is not executed, it must be returned to the court from which it was issued within the time authorised for its execution.

15 Offences

(1) It is an offence for a person, —

(a) intentionally to obstruct a person in the execution of a warrant issued under this Schedule; or

(b) to fail without reasonable excuse to give a person executing such a warrant such assistance as the person may reasonably require for the execution of the warrant.

(2) It is an offence for a person, —

(a) to make a statement in response to a requirement under paragraph 5(2)(b) or (c) or paragraph 5(3)(b) or (c) which the person knows to be false in a material respect; or

(b) recklessly to make a statement in response to such a requirement which is false in a material respect.

(See regulation 141(1), which specifies the penalty for offences under this paragraph.)

16 Self-incrimination

(1) An explanation given, or information provided, by a person in response to a requirement under paragraph 5(2)(b) or (c) or paragraph 5(3)(b) or (c) may only be used in evidence against that person —

(a) on a prosecution for an offence under a provision listed in subparagraph (2); or

(b) on a prosecution for any other offence where —

(i) in giving evidence, that person makes a statement inconsistent with that explanation or information; and

(ii) evidence relating to that explanation or information is adduced, or a question relating to it is asked, by that person or on that person's behalf.

(2) Those provisions are —

(a) paragraph 15;

(b) section 5 of the *Perjury Act 1952* (false statements made otherwise than on oath).

17 Vessels, vehicles etc.

In this Schedule, —

(a) **"premises"** includes a vehicle, vessel or other means of transport; and

(b) references to the occupier of premises include the person in charge of a vehicle, vessel or other means of transport.

SCHEDULE 5

PENALTIES

Regulation 112(4)

1 Meaning of "penalty"

In this Schedule, "penalty" means a penalty imposed by a penalty notice.

2 Notice of intent to impose penalty

(1) Before giving a person a penalty notice, the Information Commissioner must, by written notice (a **"notice of intent"**) inform the person that the Information Commissioner intends to give a penalty notice.

(2) The Information Commissioner may not give a penalty notice in reliance on a notice of intent after the end of the period of 6 months beginning with the day after the notice of intent is given.

3 Contents of notice of intent

(1) A notice of intent must contain the following information, —

(a) the name and address of the person to whom the Information Commissioner proposes to give a penalty notice;

(b) the reasons why the Information Commissioner proposes to give a penalty notice (see subparagraph (2));

(c) an indication of the amount of the penalty the Information Commissioner proposes to impose, including any aggravating or mitigating factors that the Information Commissioner proposes to take into account;

(d) the date on which the Information Commissioner proposes to give the penalty notice.

(2) The information required under subparagraph (1)(b) includes, —

(a) a description of the circumstances of the failure, and

(b) where the notice if given in respect of a failure described in regulation 106(2), the nature of the personal data involved in the failure.

(3) A notice of intent must also, —

(a) state that the person may make written representations about the Information Commissioner's intention to give a penalty notice, and

(b) specify the period within which such representations may be made.

(4) The period specified for making written representations must be a period of not less than 21 days beginning with the day on which the notice of intent is given.

(5) If the Information Commissioner considers that it is appropriate for the person to have an opportunity to make oral representations about the Information Commissioner's intention to give a penalty notice, the notice of intent must also, —

(a) state that the person may make such representations, and

(b) specify the arrangements for making such representations and the time at which, or the period within which, they may be made.

4 Giving an penalty notice

(1) The Information Commissioner may not give a penalty notice before a time, or before the end of a period, specified in the notice of intent for making oral or written representations.

(2) When deciding whether to give a penalty notice to a person and determining the amount of the penalty, the Information Commissioner must consider any oral or written representations made by the person in accordance with the notice of intent.

5 Contents of penalty notice

(1) A penalty notice must contain the following information, —

(a) the name and address of the person to whom it is addressed;

(b) details of the notice of intent given to the person;

(c) whether the Information Commissioner received oral or written representations in accordance with the notice of intent;

(d) the reasons why the Information Commissioner proposes to impose the penalty (see subparagraph (2));

(e) the reasons for the amount of the penalty, including any aggravating or mitigating factors that the Information Commissioner has taken into account;

(f) details of how the penalty is to be paid;

(g) details of the rights of appeal under regulation 120; and

(h) details of the Information Commissioner's enforcement powers under this Schedule.

(2) The information required under subparagraph (1)(d) includes, —

(a) a description of the circumstances of the failure, and

(b) where the notice is given in respect of a failure described in regulation 106(2), the nature of the personal data involved in the failure.

6 Period for payment of penalty

(1) A penalty must be paid to the Information Commissioner within the period specified in the penalty notice.

(2) The period specified must be a period of not less than 28 days beginning with the day after the day on which the penalty notice is given.

7 Variation of penalty

(1) The Information Commissioner may vary a penalty notice by giving written notice (a **"penalty variation notice"**) to the person to whom it was given.

(2) A penalty variation notice must specify, —

(a) the penalty notice concerned, and

(b) how it is varied.

(3) A penalty variation notice may not, —

(a) reduce the period for payment of the penalty;

(b) increase the amount of the penalty;

(c) otherwise vary the penalty notice to the detriment of the person to whom it was given.

(4) If, —

(a) a penalty variation notice reduces the amount of the penalty, and

(b) when that notice is given, an amount has already been paid that exceeds the amount of the reduced penalty,

the Information Commissioner must repay the excess.

8 Cancellation of penalty

(1) The Information Commissioner may cancel a penalty notice by giving written notice to the person to whom it was given.

(2) If a penalty notice is cancelled, the Information Commissioner, —

(a) may not take any further action under regulation 112 or this Schedule in relation to the failure to which that notice relates; and

(b) must repay any amount that has been paid in accordance with that notice.

9 Enforcement of payment

(1) The Information Commissioner must not take action to recover a penalty unless, —

(a) the period specified in accordance with paragraph 6 has ended,

(b) any appeals against the penalty notice have been decided or otherwise ended,

(c) if the penalty notice has been varied, any appeals against the penalty variation notice have been decided or otherwise ended, and

(d) the period for the controller or processor to appeal against the penalty, and any variation of it, has ended.

(2) A penalty is recoverable if the court so orders in accordance with proceedings taken under regulation 117, as if it were payable under an order of that court.

SCHEDULE 6

RELEVANT RECORDS

Regulation 137

1 Relevant records

(1) In regulation 137, "relevant record" means —

(a) a health record,

(b) a relevant record relating to a conviction or caution (see paragraph 2), or

(c) a relevant record relating to statutory functions (see paragraph 3).

(2) A record is not a "relevant record" to the extent that it relates, or is to relate, only to manual unstructured personal data held by FOI public authorities.

(3) In this Schedule, "FOI public authority" means a public authority as defined in section 6(1) of the *Freedom of Information Act 2015*.

2 Relevant records relating to a conviction or caution

(1) "Relevant record relating to a conviction or caution" means a record which —

(a) has been or is to be obtained by a data subject in the exercise of a data subject access right from a person listed in subparagraph (2), and

(b) contains information relating to a conviction or caution.

(2) Those persons are, —

(a) the Chief Constable of the Isle of Man Constabulary; and

(b) the ACRO Criminal Records Office.

(3) In this paragraph, —

"caution" means a caution given to a person in respect of an offence which, at the time when the caution is given, is admitted;

"conviction" has the same meaning as in the *Rehabilitation of Offenders Act 2001.*

3 Relevant records relating to statutory functions

(1) "Relevant record relating to statutory functions" means a record which —

(a) has been or is to be obtained by a data subject in the exercise of a data subject access right from a person listed in subparagraph (2); and

(b) contains information relating to a relevant function in relation to that person.

(2) That person is the Treasury.

(3) In relation to the Treasury, the "relevant functions" are its functions under

(a) the Social Security Contributions and Benefits Act 1992 (of Parliament)[25]; or

(b) the Jobseekers Act 1995 (of Parliament)[26],

as applied to the Island.

4 Data subject access right

In this Schedule, "data subject access right" means a right under —

(a) Article 15 of the applied GDPR (right of access by the data subject);

(b) Article 20 of the applied GDPR (right to data portability); or

(c) regulation 43 of these Regulations (law enforcement processing: right of access by the data subject).

5 Records stating that personal data are not processed

For the purposes of this Schedule, a record which states that a controller is not processing personal data relating to a particular matter is to be taken to be a record containing information relating to that matter.

6 Power to amend

The Council of Ministers may by regulations amend this Schedule.

Tynwald procedure – approval required.

[25] Applied to the Island by SD 505/94.
[26] Applied to the Island by SD 008/96.

SCHEDULE 7

REGISTRATION WITH THE INFORMATION COMMISSIONER

Regulations 9(4) and 141(6)

PART 1 – REGISTRATION

1 Preliminary

(1) In this Schedule "**the registrable particulars**", in relation to controller or processor, means —

(a) the controller or processor's name;

(b) the controller or processor's address;

(c) other contact details as may be prescribed in registration regulations;

(d) where applicable, the controller or processor's company registration number;

(e) where applicable, the country in which the company is incorporated, if not the Isle of Man;

(f) the nature of the controller or processor's business or trade;

(g) the address of any website of the controller or processor;

(h) any trading names or business names used by the controller or processor;

(i) where in accordance with Article 27 of the applied GDPR the controller or processor has designated a representative, the name, address and contact details of that representative;

(j) where a controller or processor has not designated a Data Protection Officer, the name, address and contact details of the person who will act as a point of contact for the Information Commissioner; and

(k) where, in accordance with Article 37 of the applied GDPR or Article 32 of the applied LED, the controller or processor has designated a Data Protection Officer —

(i) the name;

(ii) the address; and

(iii) the contact details,

of that Data Protection Officer.

(2) For the purposes of this paragraph —

(a) the address of a registered company is that of its registered office;

(b) the address of a person (other than a registered company) carrying on a business is that of his or her principal place of business in the Island; and

(c) the nature of business is the principal trade recorded with the relevant Companies Registry or, if not so recorded, a brief description of that trade.

(3) The Council of Ministers may by regulations (in this Schedule referred to as **"registration regulations"**) add to or amend the registrable particulars.

Tynwald procedure – approval required.

2 Prohibition on processing without registration

(1) Subject to the following provisions of this Schedule and any transitional provisions provided for by Schedule 11, personal data must not be processed unless an entry in respect of that controller or processor is included in the register maintained by the Information Commissioner under paragraph 4 of this Schedule (or is treated, by registration regulations, as being so included).

(2) Subparagraph (1) does not apply to personal data processed other than wholly or partly by automated means.

(3) If it appears to the Council of Ministers that processing of a particular description is unlikely to prejudice the rights and freedoms of data subjects, registration regulations may provide that, in such cases as may be prescribed, subparagraph (1) is not to apply in relation to processing of that description.

(4) Subparagraph (1) does not apply in relation to any processing whose sole purpose is the maintenance of a public register.

3 Application for registration

(1) A controller or processor must, in order to be included in the register maintained by the Information Commissioner under paragraph 4, submit to the Information Commissioner an application in the form the Information Commissioner determines in accordance with paragraph 7 of this Schedule.

(2) Registration regulations may make provision as to registration —

(a) by partnerships; or

(b) in other cases where 2 or more persons are controllers in respect of any personal data.

(3) An application must be accompanied by such fee as may be prescribed in fees regulations made by the Treasury after consultation with the Information Commissioner.

Tynwald procedure – approval required.

4 Register of controllers and processors

(1) The Information Commissioner must —

(a) maintain a register of persons who have applied for registration under paragraph 3; and

(b) make an entry in the register in pursuance of each application received by the Information Commissioner under that paragraph from a person in respect of whom no entry as a controller or processor was for the time being included in the register.

(2) Each entry in the register must consist of —

(a) the registrable particulars or, as the case requires, those particulars as amended in pursuance of paragraph 12; and

(b) such other information as the Information Commissioner may be authorised or required by registration regulations to include in the register.

(3) The time from which an entry in respect of a controller or processor who has made an application for registration under paragraph 3 of this Schedule is to be treated as having been made in the register, is the day on which the application is received by the Information Commissioner.

(4) No entry is permitted to be retained in the register for more than the relevant time except on payment of such fee as may be prescribed by fees regulations.

(5) In subparagraph (4) "the relevant time" means 12 months or such other period as may be prescribed by registration regulations.

(6) The Information Commissioner must, with the exception of the registrable particulars provided to the Information Commissioner pursuant to paragraphs 1(1)(i), (j) or (k), publish the information contained in the register by electronic means for inspection by members of the public free of charge. [38]

5 Offences

(1) If paragraph 2(1) is contravened, the controller or processor commits an offence and is liable on summary conviction to a fine not exceeding level 5 on the standard scale.

(2) Any person who fails to comply with the duty imposed by paragraph 12(1) and (2) commits an offence and is liable on summary conviction to a fine not exceeding level 5 on the standard scale.

(3) It is a defence for a person charged with an offence under subparagraph (2) to show that he or she exercised all due diligence to comply with the duty.

PART 2 – EXEMPTIONS AND OTHER PROCEDURAL MATTERS

6 Exemptions from registration

Paragraph 2(1) of this Schedule does not apply to processing, —

(a) which —

(i) falls within one or more of the descriptions of processing set out in Part 3 of this Schedule; or

(ii) is specified in registration regulations as permitted by paragraph 2(3) of this Schedule (being processing appearing to the Council of Ministers to be unlikely to prejudice the rights and freedoms of data subjects);

(b) which does not fall within one or more of those descriptions solely by virtue of the fact that disclosure of the personal data is to a person other than those specified in the descriptions; or

(c) which is required by or under any statutory provision, by any rule of law or by the order of a court.

7 Form of application for registration

(1) Subject to paragraphs 8 and 9 of this Schedule, the Information Commissioner must determine the form in which the registrable particulars are to be provided in an application for registration under paragraph 3 of this Schedule.

(2) Subject to paragraphs 8 and 9 of this Schedule, the Information Commissioner must determine the form in which an application to notify changes to the registrable particulars under paragraph 10 of this Schedule (including that regulation as modified by paragraph 13 of this Schedule) is to be specified.

8 Registration in respect of partnerships

(1) In any case in which two or more persons carrying on a business in partnership are controllers in respect of any personal data for purposes of that business, an application for registration under paragraph 3 of this Schedule may be given in respect of those persons in the name of the firm.

(2) Where an application is made in the name of a firm under paragraph (1) —

(a) the name to be specified for the purposes of paragraph 1(1)(a) of this Schedule is the name of the firm; and

(b) the address to be specified for the purposes of paragraph 1(1)(b) of this Schedule is the address of the firm's principal place of business.[39]

9 Registration in respect of the governing body or, and head teacher at, any school

(1) In any case in which a governing body of, and a head teacher at, any school are, in those capacities, the controllers in respect of any personal data, an application for registration under paragraph 3 of this Schedule may be made in respect of that governing body and head teacher in the name of the school.

(2) Where an application is made in the name of a school under subparagraph (1), the name and address to be specified for the purposes of paragraph 1(1) of this Schedule are those of the school.[40]

10 Confirmation of register entry

(1) The Information Commissioner must, as soon as practicable and in any event within a period of 28 days after making an entry in the register in accordance with paragraph 4 of this Schedule or amending an entry in the register in accordance with paragraph 12 of this Schedule, give the controller or processor to whom the register entry relates notice confirming the register entry.

(2) A notice under subparagraph (1) must include a statement of —

(a) the date on which —

(i) in the case of an entry made under paragraph 4 of this Schedule, the entry is treated as having been included by virtue of paragraph 4(3) of this Schedule; or

(ii) in any case of an entry made under paragraph 12 of this Schedule, the notification of changes was received by the Information Commissioner;

(b) the registrable particulars entered in the register, or the amendments made; and

(c) the date by which the fee (if any) prescribed in fees regulations, made under paragraph 3(3) of this Schedule, must be paid in order for the entry to be retained in the register as provided for by paragraph 4(4) of this Schedule.

11 Additional information contained in a register entry

In addition to the matters mentioned in paragraph 1 of this Schedule, the Information Commissioner may include in a register entry —

(a) a registration number issued by the Information Commissioner in respect of that entry;

(b) the date on which the entry is treated, by virtue of paragraph 4(3) of this Schedule, as having been included in pursuance of an application for registration; or

(c) the date on which the entry falls or may fall to be removed by virtue of paragraph 4(4) of this Schedule.

12 Duty to notify changes

(1) Subject to paragraph 13 of this Schedule, every person in respect of whom an entry is for the time being included in the register is under a duty to inform the Information Commissioner when the registrable particulars in that entry become inaccurate or incomplete, setting out the changes which need to be made to that entry in order to make it accurate and complete.

(2) Notification of such changes must be given as soon as practicable and in any event within a period of 28 days from the date on which the entry becomes inaccurate or incomplete.

(3) On receiving any notification referred to in subparagraph (1), the Information Commissioner must make such amendments of the relevant entry in the register maintained under paragraph 4 as are necessary to take account of the notification.

13 Duty to notify changes – transitional modifications

(1) This paragraph applies to persons in respect of whom an entry for the time being is maintained by the Information Commissioner in the Register of notifications under section 16 of the *Data Protection Act 2002*.

(2) In the case of a person to whom this regulation applies, the duty imposed by paragraph 12 of this Schedule is modified so as to have effect as set out in subparagraph (3) below.

(3) Every person in respect of whom an entry is for the time being included in the register of notifications is under a duty to give the Information Commissioner a notification specifying his current registrable particulars and setting out the changes which need to be made to that entry in order to make it accurate and complete in those respects.

14 Retention of register entries – transitional provisions

(1) This regulation applies to any entry in respect of a person that is maintained by the Information Commissioner in the Register of notifications under section 16 of the *Data Protection Act 2002*.

(2) An entry must be immediately erased from the register upon the happening of the first of the following to occur —

(a) the expiration of that entry's current registration period; or

(b) the date on which the controller makes an application for registration under paragraph 3 of this Schedule.

PART 3 – PROCESSING TO WHICH PART 2 OF THIS SCHEDULE DOES NOT APPLY

15 Interpretation

In this Part of this Schedule —

"exempt purposes" in paragraphs 16 and 17 of this Schedule means the purposes specified in sub-subparagraph (a) and in paragraph 18 of this Schedule means the purposes specified in sub-subparagraph (b) of paragraph 18 of this Schedule;

"staff" includes —

(a) employees or office holders;

(b) workers within the meaning of the *Minimum Wage Act 2001*;

(c) persons working under any contract for services; and

(d) volunteers.

16 Staff administration exemption

The processing —

(a) is for the purposes of appointments or removals, pay, discipline, superannuation, work management or other personnel matters in relation to the staff of the controller or processor;[41]

(b) is of personal data in respect of which the data subject is —

(i) a past, existing or prospective member of staff of the controller or processor; or [42]

(ii) any person the processing of whose personal data is necessary for the exempt purposes;

(c) is of personal data consisting of the name, address and other identifiers of the data subject or information as to —

(iv) qualifications, work experience or pay; or

(v) other matters the processing of which is necessary for the exempt purposes;

(d) does not involve disclosure of the personal data to any third party other than —

(i) with the consent of the data subject;

(ii) where it is necessary to make such disclosure for the exempt purposes; and

(e) does not involve keeping the personal data after the relationship between the controller or processor and staff member ends, unless and for so long as it is necessary to do so for the exempt purposes.[43]

17 Accounts and records exemption

(1) The processing —

(a) is for the purposes of —

(i) keeping accounts relating to any business or other activity carried on by the controller or processor;[44]

(ii) deciding whether to accept any person as a customer or supplier;

(iii) keeping records of purchases, sales or other transactions, in order to ensure that the requisite payments and deliveries are made or services provided by or to the controller or processor in respect of those transactions; or[45]

(iv) making financial or management forecasts to assist the controller or processor in the conduct of any such business or activity;

(b) is of personal data in respect of which the data subject is —

(i) a past, existing or prospective customer or supplier; or

(ii) any person the processing of whose personal data is necessary for the exempt purposes; [46]

(c) is of personal data consisting of the name, address and other identifiers of the data subject or information as to —

(i) financial standing; or

(ii) other matters the processing of which is necessary for the exempt purposes;

(d) does not involve disclosure of the personal data to any third party other than —

(i) with the consent of the data subject;

(ii) where it is necessary to make such disclosure for the exempt purposes; and

(e) does not involve keeping the personal data after the relationship between the controller or processor and customer or supplier ends, unless and for so long as it is necessary to do so for the exempt purposes.[47]

(2) Subparagraph (1)(c) does not apply to personal data processed by or obtained from a credit reference agency.

18 Non profit-making organisations exemptions

The processing —

(a) is carried out by a controller which is a body or association which is not established or conducted for profit;

(b) is for the purposes of establishing or maintaining membership of or support for the body or association, or providing or administering activities for individuals who are either members of the body or association or have regular contact with it;

(c) is of personal data in respect of which the data subject is —

(i) a past, existing or prospective member of the body or organisation;

(ii) any person who has regular contact with the body or organisation in connection with the exempt purposes; or

(iii) any person the processing of whose data is necessary for the exempt purposes;

(d) is of personal data consisting of the name, address and other identifiers of the data subject or information as to —

(i) eligibility for membership of the body or association; or

(ii) other matters the processing of which is necessary for the exempt purposes;

(e) does not involve disclosure of the personal data of any third party other than —

(i) with the consent of the data subject;

(ii) where it is necessary to make such disclosure for the exempt purposes; and

(f) does not involve keeping the personal data after the relationship between the controller and data subject ends, unless and for so long as it is necessary to do so for the exempt purposes.

SCHEDULE 8

APPEALS

Regulations 120 and 146(3)

Interpretation

1. In this Schedule, "appeal" means an appeal under regulation 120.

Hearing of appeals

2. For the purposes of hearing and determining appeals or any matter preliminary or incidental to an appeal, the Tribunal must sit at such times and in such places as the chairman or deputy chairman may direct.

Constitution of Tribunal

3. Subject to paragraph 4 and any rules under paragraph 5, the Tribunal is duly constituted for the purpose of any proceedings if it consists of —

   (a) the chairman or deputy chairman (who must preside); and

   (b) one or more other members.

Ex parte proceedings

4. Subject to any rules under paragraph 5, the jurisdiction of the Tribunal in respect of an appeal under regulation 120 may be exercised ex parte by the chairman or deputy chairman sitting alone.

Rules of procedure

5. (1) The Council of Ministers may make rules for regulating the exercise of the rights of appeal under these Regulations.

   (2) Rules under this paragraph may in particular make provision —

   (a) with respect to the period within which an appeal can be brought and the burden of proof on an appeal;

   (b) for summoning of witnesses and the administration of oaths;

   (c) for securing the production of documents and materials used for the processing of personal data;

   (d) for the inspection, examination, operation and testing of any equipment or material used in connection with the processing of personal data;

   (e) for the hearing of an appeal or reference wholly or partly in camera;

   (f) for hearing an appeal in the absence of the appellant or for determining an appeal without a hearing;

(g) for enabling an appeal to the Tribunal against an information notice to be determined by the chairman or deputy chairman;

(h) for enabling any matter preliminary or incidental to an appeal to be dealt with by the chairman or deputy chairman;

(i) for the awarding of costs;

(j) for the publication of reports of the Tribunal's decisions; and

(k) for conferring on the Tribunal such ancillary powers as the Council of Ministers thinks necessary for the proper discharge of its functions.

(3) In making rules under this paragraph which relate to appeals under regulation 126, the Council of Ministers must have regard, in particular, to the need to secure that information is not disclosed contrary to the public interest.

Obstruction etc.

6. (1) If any person commits an act or omission in relation to proceedings before the Tribunal which, if those proceedings were proceedings before the High Court, would constitute contempt of court, the Tribunal may certify the matter to the High Court.

(2) Where a matter is so certified, the High Court may inquire into it and, after hearing any witness who may be produced against or on behalf of the person charged with the matter, and after hearing any statement that may be offered in defence, deal with him or her in any manner in which it could deal with him or her if the act or omission had occurred in relation to the court.

SCHEDULE 9

RESTRICTIONS AND EXEMPTIONS

Regulations 9(5) and 24

PART 1: ADAPTATIONS, RESTRICTIONS AND EXEMPTIONS BASED ON ARTICLE 23(1) OF THE APPLIED GDPR

Crime and taxation: general

1. (1) Personal data processed for any of the following purposes —

(a) the prevention or detection of crime;

(b) the apprehension or prosecution of offenders; or

(c) the assessment or collection of any tax or duty or of any imposition of a similar nature,

are, to the extent that the application of those provisions would be likely to prejudice any of the matters mentioned in sub-subparagraphs (a) to (c), exempt from the provisions of the applied GDPR listed in subparagraph (2).

(2) Those provisions of the applied GDPR are —

(a) Article 13(1) to (3) (personal data collected from data subject);

(b) Article 14(1) to (4) (personal data collected other than from data subject);

(c) Article 15(1) to (3) (confirmation of processing, access to data and safeguards for third country transfers);

(d) Article 16 (right to rectification);

(e) Article 17(1) and (2) (right to erasure);

(f) Article 18(1) (restriction of processing);

(g) Article 19 (notification obligations regarding rectification or erasure of personal data or restriction of processing);

(h) Article 20(1) and (2) (right to data portability);

(i) Article 21(1) (objections to processing);

(j) Article 5 (general principles), so far as its provisions correspond to the rights and obligations provided for in the provisions mentioned in heads (a) to (i).

Data processed for the purpose of discharging statutory functions[48]

2. (1) Personal data which —

(a) are processed for the purpose of discharging statutory functions; and

(b) consist of information obtained for such a purpose from a person who possessed that information for any of the purposes mentioned in paragraph 1(1),

are exempt from the provisions of the applied GDPR listed in subparagraph (2).

(2) The provisions of the applied GDPR referred to in subparagraph (1) are —

(a) Article 13(1) to (3) (personal data collected from data subject);

(b) Article 14(1) to (4) (personal data collected other than from data subject);

(c) Article 15(1) to (3) (confirmation of processing, access to data and safeguards for third country transfers); and

(d) Article 5 (general principles), so far as its provisions correspond to the rights and obligations provided for in the provisions mentioned in heads (a) to (c).[49]

Crime and taxation: risk assessment systems

3. (1) Personal data which are processed by a relevant authority and consist of a classification applied to the data subject as part of a system of risk assessment which is operated by that relevant authority for either of the following purposes —

(a) the assessment or collection of any tax due or duty or any imposition of a similar nature; or

(b) the prevention or detection of crime, or the apprehension or prosecution of offenders, where the offence concerned involves any unlawful claim for any payment out of, or any unlawful application of, public funds,

and are processed for either of those purposes, are, to the extent that the application of those provisions would prevent the system from operating effectively, exempt from the provisions of the applied GDPR that are listed in subparagraph (2).

(2) Those provisions of the applied GDPR are —

(a) Article 13(1) to (3) (personal data collected from data subject: information to be provided);

(b) Article 14(1) to (4) (personal data collected other than from data subject: information to be provided);

(c) Article 15(1) to (3) (confirmation of processing, access to data and safeguards for third country transfers);

(d) Article 5 (general principles), so far as its provisions correspond to the rights and obligations provided for in the provisions mentioned in heads (a) to (c).

(3) In this paragraph, "relevant authority" means a Department, Statutory Board, local authority or joint board.

4. [Revoked][50]

5. [Revoked][51]

Information required to be disclosed by law etc. or in connection with legal proceedings

6. (1) Where —

(a) an enactment (other than the *Freedom of Information Act 2015*) requires personal data to be made available to the public whether by publishing it, making it available for inspection, or otherwise, and whether gratuitously or on payment of a fee;

(b) disclosure of personal data is required by an enactment, a rule of law, an order of a court or tribunal; or

(c) disclosure of personal data is —

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

(ii) necessary for the purpose of obtaining legal advice; or

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

such disclosures are, to the extent that the application of those provisions would prevent the disclosure, exempt from the provisions of the applied GDPR set out in subparagraph (2).

(1) Those provisions of the applied GDPR are —

(a) Article 13(1) to (3) (personal data collected from data subject);

(b) Article 14(1) to (4) (personal data collected other than from data subject);

(c) Article 15(1) to (3) (confirmation of processing, access to data and safeguards for third country transfers);

(d) Article 16 (right to rectification);

(e) Article 17(1) and (2) (right to erasure);

(f) Article 18(1) (restriction of processing);

(g) Article 19 (notification obligation regarding rectification or erasure of personal data or restriction of processing);

(h) Article 20(1) and (2) (right to data portability);

(i) Article 21(1) (objections to processing);

(j) Article 5 (general principles) so far as its provisions correspond to the rights and obligations provided for in the provisions mentioned in heads (a) to (i).

PART 2 –EXEMPTIONS AND RESTRICTIONS BASED ON ARTICLE 23(1) OF THE APPLIED GDPR: EXEMPTIONS AND RESTRICTIONS RELATING TO ARTICLES 13 TO 21

Tynwald privilege

7. If required for the purpose of avoiding an infringement of the privileges of Tynwald, the processing of personal data is exempt from the following provisions of the applied GDPR —

(a) Article 13(1) to (3) (personal data collected from data subject: information to be provided);

(b) Article 14(1) to (4) (personal data collected other than from data subject: information to be provided);

(c) Article 15(1) to (3) (confirmation of processing: access to data and safeguards for third country transfers);

(d) Article 16 (right to rectification);

(e) Article 17(1) and (2) (right to erasure);

(f) Article 18(1) (restriction of processing);

(g) Article 19 (notification obligation regarding rectification or erasure of personal data or restriction of processing);

(h) Article 20(1) and (2) (right to data portability);

(i) Article 21(1) (objections to processing);

(j) Article 5 (general principles) so far as its provisions correspond to the rights and obligations provided for in the provisions mentioned in heads (a) to (i).

PART 3 – EXEMPTIONS AND RESTRICTIONS BASED ON ARTICLE 23(1): PROTECTION OF RIGHTS OF OTHERS

Protection of the rights of others: general

8. (1) Article 15(1) to (3) of the applied GDPR (confirmation of processing, access to data and safeguards for third country transfers), and Article 5 of the applied GDPR so far as its provisions correspond to the rights and

obligations provided for in Article 15(1) to (3), do not oblige a controller or processor to disclose information to the data subject to the extent that doing so would involve disclosing information relating to another individual who can be identified from the information.[52]

(2) Subparagraph (1) does not remove the controller's or processor's obligation where —

(a) the other individual has consented to the disclosure of the information to the data subject; or

(b) it is reasonable to disclose the information to the data subject without the consent of the other individual.[53]

(3) In determining whether it is reasonable to disclose the information without consent, the controller or processor must have regard to all the relevant circumstances, including —

(a) the type of information that would be disclosed;

(b) any duty of confidentiality owed to the other individual;

(c) any steps taken by the controller or processor with a view to seeking the consent of the other individual; [54]

(d) whether the other individual is capable of giving consent; and

(e) any express refusal of consent by the other individual. [55]

(4) For the purposes of this paragraph —

(a) "information relating to another individual" includes information identifying the other individual as the source of information;

(b) an individual can be identified from information to be provided to a data subject by a controller or processor if the individual can be identified from —

(i) that information; or

(ii) that information and any other information that the controller or processor reasonably believes the data subject is likely to possess or obtain.[56] [57]

(5) This paragraph is not to be construed as excusing a controller or processor from communicating so much of the information sought by the request as can be communicated without disclosing the identity of the other individual concerned, whether by the omission of names or other identifying particulars or otherwise.[58]

PART 4 – EXEMPTIONS AND RESTRICTIONS BASED ON ARTICLE 23(1) OF THE APPLIED GDPR: EXEMPTIONS AND RESTRICTIONS RELATING TO ARTICLES 13 TO 15

Applied GDPR provisions to be exempted or restricted: "the listed applied GDPR provisions"

9. In this Part of this Schedule, "**the listed applied GDPR provisions**" means the following provisions of the applied GDPR (the rights and obligations in which may be restricted by virtue of Article 23(1) of the applied GDPR) —

(a) Article 13(1) to (3) (personal data collected from data subject: information to be provided);

(b) Article 14(1) to (4) (personal data collected other than from data subject: information to be provided);

(c) Article 15(1) to (3) (confirmation of processing, access to data and safeguards for third country transfers);

(d) Article 5 (general principles) so far as its provisions correspond to the rights and obligations provided for in the provisions mentioned in subparagraphs (a) to (c)

Legal professional privilege

10. The listed applied GDPR provisions do not apply to personal data that consist of information in respect of which a claim to legal professional privilege could be maintained in legal proceedings.

Judicial appointments, judicial independence and judicial proceedings

11. (1) The listed applied GDPR provisions do not apply to personal data processed for the purposes of assessing a person's suitability for judicial office or the office of Queen's Counsel.

(2) The listed applied GDPR provisions do not apply to personal data processed by —

(a) an individual acting in a judicial capacity; or

(b) a court or tribunal acting in its judicial capacity.

(3) As regards personal data not falling within subparagraph (1) or (2), the listed applied GDPR provisions do not apply to the extent that the application of those provisions would be likely to prejudice judicial independence or judicial proceedings.

(4) Personal data processed for the purposes of —

(a) assessing any person's suitability for judicial office; or

(b) the conferring by the Crown of any honour or dignity,

are exempt from the listed applied GDPR provisions.

Crown employment and appointments

12. (1) Personal data are exempted from the of the listed applied GDPR provisions if they are processed for the purpose of assessing any person's suitability for any of the following offices —

(a) offices to which appointments are made by Her Majesty, namely —

(i) Lieutenant Governor;

(ii) Bishop of Sodor and Man;

(iii) First Deemster and Clerk of the Rolls;

(iv) Second Deemster;

(v) Attorney General;

(vi) Incumbent of a Benefice;

(vii) Judge of Appeal;

(viii) Solicitor General;[59]

(b) acting judges, being offices to which appointments are made under the High Court Act 1991;[60]

(c) offices to which appointments are made by the Lieutenant Governor.[61]

(2) The Council of Ministers may make further regulations to exempt from the provisions of the applied GDPR listed in paragraph 9 personal data processed for the purposes of assessing any person's suitability for —

(a) employment by or under the Crown; or

(b) any office of which appointments are made by Her Majesty, the Governor in Council or the Council of Ministers.

Self-incrimination

13. (1) A person need not comply with the listed applied GDPR provisions to the extent that compliance would, by revealing evidence of the commission of an offence other than an offence under these Regulations, expose the person to criminal proceedings for that offence.

(2) Information disclosed by any person in compliance with any request, made in accordance with any of the listed applied GDPR provisions, in respect of granting access to personal data is inadmissible against the person in proceedings for an offence under these Regulations.

Armed forces

14. Personal data are exempt from the listed applied GDPR provisions in any case to the extent to which the application of that requirement would be likely to prejudice the combat effectiveness of any of the armed forces of the Crown.

Management forecasts

15. The listed applied GDPR provisions do not apply to personal data processed for the purposes of management forecasting or management planning in relation to a business or other activity, to the extent that the application of those provisions would be likely to prejudice the conduct of the business or activity concerned.

Negotiations

16. The listed applied GDPR provisions do not apply to personal data that consist of records of the intentions of the controller in relation to any negotiations with the data subject to the extent that the application of those provisions would be likely to prejudice those negotiations.

Confidential references

17. The listed applied GDPR provisions do not apply to personal data consisting of a reference given (or to be given) in confidence for the purposes of —

(a) the education, training or employment (or prospective education, training or employment) of the data subject;

(b) the placement (or prospective placement) of the data subject as a volunteer;

(c) the appointment (or prospective appointment) of the data subject to any office; or

(d) the provision (or prospective provision) by the data subject of any service.[62]

Exam scripts and exam marks

18. (1) The listed applied GDPR provisions do not apply to personal data consisting of information recorded by candidates during an exam.

(2) Where personal data consist of marks or other information processed by a controller —

(a) for the purposes of determining the results of an exam; or

(b) in consequence of the determination of the results of an exam,

the duty in Article 12(3) or (4) of the applied GDPR for the controller to provide information requested by the data subject within a certain time period, as it applies to Article 15 of the applied GDPR (confirmation of processing, access to data and safeguards for third country transfers), is modified as set out in subparagraph (3).

(3) Where a question arises as to whether the controller is obliged by Article 15 of the applied GDPR to disclose personal data, and the question arises before the day on which the exam results are announced, the controller must provide the information mentioned in Article 12(3) or (4) —

(a) before the end of the period of 5 months beginning when the question arises; or

(b) if earlier, before the end of the period of 40 days beginning with the announcement of the results.

(4) In this paragraph, "exam" means an academic, professional or other examination used for determining the knowledge, intelligence, skill or ability of a candidate and may include an exam consisting of an assessment of the candidate's performance while undertaking work or any other activity.

(5) For the purposes of this paragraph, the results of an exam are treated as announced when they are first published or, if not published, first communicated to the candidate.

Corporate finance

19. (1) Where personal data are processed for the purposes of, or in connection with, a corporate finance service provided by any person —

(a) the data are exempt from the listed applied GDPR provisions in any case to the extent to which either —

(i) the application of that requirement to the data could affect the price of any securities which are already in existence or are to be or may be created; or

(ii) the controller reasonably believes that the application of that requirement to the data could affect the price of any such securities; and

(b) to the extent that the data are not exempt from the listed applied GDPR provisions by virtue of paragraph (a), they are exempt from that requirement if the exemption is required for the purpose of safeguarding an important economic or financial interest of the Island.

(2) For the purposes of subparagraph (1)(b) the Council of Ministers may by order specify —

(a) matters to be taken into account in determining whether exemption from the listed applied GDPR provisions is required for the purpose of safeguarding an important economic or financial interest in the Island; or

(b) circumstances in which exemption from that requirement is, or is not, to be taken to be required for that purpose.

(3) In this paragraph —

"corporate finance service" means a service consisting in —

(a) underwriting in respect of issues of, or the placing of issues of, any securities;

(b) advice to undertakings on capital structure, industrial strategy and related matters and advice and service relating to mergers and the purchase of undertakings; or

(c) services relating to such underwriting as is mentioned in paragraph (a);

"price" includes value;

"securities" means —

(a) shares or debentures;

(b) securities of the government or any country or territory; or

(c) rights or interests (described whether as units or otherwise) in any such shares, debentures or securities.

Regulatory activity

20. (1) Personal data processed for the purposes of discharging functions to which this paragraph applies are exempt from the listed applied GDPR provisions in any case to the extent to which the application of those provisions to the data would be likely to prejudice the proper discharge of those functions

(2) Subparagraph (1) applies to any relevant function which is designed for —

(a) protecting members of the public against —

(i) financial loss due to dishonesty, malpractice or other seriously improper conduct by, or the unfitness or incompetence of, persons concerned in the provision of banking, insurance, investment or other financial services or in the management of bodies corporate;

(ii) financial loss due to the conduct of discharged or undischarged bankrupts; or

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

(b) protecting charities against misconduct or mismanagement (whether by trustees or other persons) in their administration, protecting the property of charities from loss or misapplication, or the recovery of the property of charities;

(c) securing the health, safety and welfare of persons at work, or protecting persons other than persons at work against risk to health or safety arising out of or in connection with the actions of persons at work.

(3) In subparagraph (2), "relevant function" means —

(a) any function conferred on any person by or under any statutory provision; or

(b) any other function which is of a public nature and is exercised in the public interest.

(2) Personal data processed for the purposes of discharging any function of the Isle of Man Office of Fair Trading under the *Fair Trading Act 1996* are exempt from the listed applied GDPR provisions in any case to the extent to which the application of those provisions to the data would be likely to prejudice the proper discharge of that function.

(3) Personal data processed for the purpose of considering a complaint under section 26 of the *Social Services Act 2011* are exempt from the listed applied GDPR provisions in any case to the extent to which the application of those provisions to the data would be likely to prejudice the proper application of that function.

Trusts

21. (1) Personal data processed in connection with a trust (regardless of which jurisdiction's law is the proper law of the trust) are exempt from the listed applied GDPR provisions to the extent that those personal data consist of any information —

(a) which discloses the trustee's deliberations as to the manner in which the trustee has —

(i) exercised a power or discretion conferred; or

(ii) performed a duty imposed,

upon the trustee;

(b) which discloses —

(i) the reason for any particular exercise of such power or discretion, or performance of duty; or

(ii) the material upon which such reason is likely to be or might have been based;

(c) which relates to —

(i) the exercise or proposed exercise of such power or discretion; or

(ii) the performance or proposed performance of such a duty; or

(d) the disclosure, erasure or rectification of which, if done by the relevant controller, would be contrary to the law referred to in subparagraph (2).

(2) The law referred to in subparagraph (1)(d) is a prohibition or restriction under —

(a) any enactment or other rule of law of the Island; or

(b) in the case of a trust the proper law of which is the law of any other jurisdiction, any enactment or other rule of law of that jurisdiction.

Insurance Purposes[63]

21A. (1) The listed applied GDPR provisions do not apply to personal data processed for an insurance purpose to the extent that the application of those provisions would be likely to prejudice that insurance purpose by the provision of information, or disclosure of personal data, to a data subject who is a beneficiary of an insurance contract prior to the occurrence of the triggering event for that contract.

(2) In this paragraph, "insurance contract" and "insurance purpose" have the same meaning as set out in paragraph 14 of Schedule 2.[64]

PART 5 – EXEMPTIONS AND RESTRICTIONS BASED ON ARTICLE 85(2) OF THE APPLIED GDPR FOR REASONS OF FREEDOM OF EXPRESSION AND INFORMATION

Journalistic, academic and literary purposes

22. (1) In this paragraph, "the special purposes" means one or more of the following —

(a) the purposes of journalism;

(b) academic purposes;

(c) artistic purposes;

(d) literary purposes.

(2) Subparagraph (3) applies to the processing of personal data carried out for the special purposes if —

(a) the processing is being carried out with a view to the publication by a person of journalistic, academic, artistic or literary material; and

(b) the controller reasonably believes that the publication of the material would be in the public interest.

(3) The listed applied GDPR provisions do not apply to the extent that the controller reasonably believes that the application of those provisions would be incompatible with the special purposes.

(4) In determining whether publication would be in the public interest, the controller must take into account the special importance of the public interest in the freedom of expression and information.

(5) In determining whether it is reasonable to believe that publication would be in the public interest, the controller must have regard to any of

the codes of practice or guidelines listed in subparagraph (6) that is relevant to the publication in question.

(6) The codes of practice and guidelines are those issued under the following legislation —

(a) the Broadcasting Act 1996 (of Parliament);

(b) the Broadcasting Act 1990 (of Parliament);

(c) the *Broadcasting Act 1993*.

(7) The Council of Ministers may by regulations amend subparagraph (6).

Tynwald procedure – approval required.

(8) For the purposes of this paragraph, "**the listed applied GDPR provisions**" are the following provisions of the applied GDPR (which may be exempted or derogated from by virtue of Article 85(2) of the applied GDPR) —

(a) in Chapter II of the applied GDPR (principles) —

(i) Article 5(1)(a) to (f) (principles relating to processing);

(ii) Article 6 (lawfulness);

(i) Article 7 (conditions for consent);

(ii) Article 8(1) and (2) (child's consent);

(iii) Article 9 (processing of special categories of data);

(iv) Article 10 (data relating to criminal convictions etc.);

(v) Article 11(2) (processing not requiring identification);

(b) in Chapter III of the applied GDPR (rights of the data subject) —

(i) Article 13(1) to (3) (personal data collected other than from data subject: information to be provided);

(ii) Article 14(1) to (4) (personal data collected other than from data subject: information to be provided);

(iii) Article 15(1) to (3) (confirmation of processing, access to data and safeguards for third country transfers);

(iv) Article 16 (right to rectification);

(v) Article 17(1) and (2) (right to erasure);

(vi) Article 18(1)(a), (b) and (d) (restriction of processing);

(vii) Article 19 (notification obligation regarding rectification or erasure of personal data or restriction of processing);

(viii) Article 20(1) and (2) (right to data portability);

(ix) Article 21(1) (objections to processing);

(e) in Chapter IV of the applied GDPR (controller and processor) —

(i) Article 34(1) and (4) (communication of personal data breach to the data subject;

(ii) Article 36 (requirement for controller to consult Information Commissioner prior to high risk processing);

(f) in Chapter V of the applied GDPR (transfers of data to third countries etc), Article 44 (general principles for transfers).

PART 6 – DEROGATIONS ETC BASED ON ARTICLE 89 OF THE APPLIED GDPR FOR RESEARCH, STATISTICS AND ARCHIVING

Research and statistics

23. (1) The listed applied GDPR provisions do not apply to personal data processed for —

(a) scientific or historical research purposes; or

(b) statistical purposes,

to the extent that the application of those provisions would prevent or seriously impair achievement of the purposes in question.

This is subject to subparagraph (3).

(2) For the purposes of this paragraph, "**the listed applied GDPR provisions**" are the following provisions of the applied GDPR (the rights in which may be derogated from by virtue of Article 89(2) of the applied GDPR) —

(a) Article 15(1) to (3) (confirmation of processing, access to data and safeguards for third country transfers);

(b) Article 16 (right to rectification);

(c) Article 18(1) (restriction of processing);

(d) Article 21(1) (objections to processing).

(3) The exemption in subparagraph (1) is available only where —

(a) the personal data are processed in accordance with Article 89(1) of the applied GDPR (as supplemented by regulation 18); and [65]

(b) as regards the disapplication of Article 15(1) to (3), the results of the research or any resulting statistics are not made available in a form which identifies a data subject.

Archiving in the public interest

24. (1) The listed applied GDPR provisions do not apply to personal data processed for archiving purposes in the public interest to the extent that the application of those provisions would prevent or seriously impair the achievement of the purposes.

(2) For the purposes of this paragraph, "the listed applied GDPR provisions" are the following provisions of the applied GDPR (rights in which may be derogated from by virtue of Article 89(3) of the applied GDPR) —

(a) Article 15(1) to (3) (confirmation of processing, access to data and safeguards for third country transfers);

(b) Article 16 (right to rectification);

(c) Article 18(1) (restriction of processing);

(d) Article 19 (notification obligation regarding rectification or erasure of personal data or restriction of processing);

(e) Article 20(1) and (2) (right to data portability);

(f) Article 21(1) (objections to processing).

(3) The exemption in subparagraph (1) is available only where the personal data are processed in accordance with Article 89(1) of the applied GDPR.

PART 7 – APPLIED GDPR PROVISIONS TO BE RESTRICTED OR EXEMPTED: "THE LISTED APPLIED GDPR PROVISIONS"

Provisions in respect of health, social work and education data

25. In this Part of this Schedule "**the listed applied GDPR provisions**" means the following provisions of the applied GDPR (the rights and obligations in which may be restricted by virtue of Article 23(1) of the applied GDPR) —

(a) Article 13(1) to (3) (personal data collected from data subject: information to be provided);

(b) Article 14(1) to (4) (personal data collected other than from data subject: information to be provided);

(c) Article 15(1) to (3) (confirmation of processing, access to data and safeguards for third country transfers);

(d) Article 16 (right to rectification);

(e) Article 17(1) and (2) (right to erasure);

(f) Article 18(1) (restriction of processing);

(g) Article 20(1) and (2) (right to data portability);

(h) Article 21(1) (objections to processing);

(i) Article 5 (general principles) so far as its provisions correspond to the rights and obligations provided for in the provisions mentioned in subparagraphs (a) to (h).

Data concerning health

26. (1) The listed applied GDPR provisions do not apply to data concerning health to the extent that the serious harm test is met with respect to those data.

(2) The "serious harm test" in subparagraph (1) is met with respect to data concerning health to the extent that the application of the listed applied GDPR provisions would be likely to cause serious harm to the physical or mental health of the data subject or another individual.

(3) A controller who is not a health professional may not rely on subparagraph (1) to withhold data concerning health unless the controller has obtained an opinion from the person who appears to the controller to be the appropriate health professional to the effect that the serious harm test is met with respect to the data.

(4) An opinion does not count for the purposes of subparagraph (2) if —

(a) it is obtained before the beginning of the relevant period; or

(b) it is obtained during that period but it was reasonable in all the circumstances to re-consult the appropriate health professional.

(5) In this paragraph —

"appropriate health professional", in relation to a question as to whether the serious harm test is met with respect to data concerning health, means —

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

(b) where there is more than one such health professional, the health professional who is the most suitable to provide an opinion on the question; or

(c) a health professional who has the necessary experience and qualifications to provide an opinion on the question, where —

(i) there is no health professional available falling within sub-subparagraph (a) or (b); or

(ii) the controller is the Department of Health and Social Care and data are processed in connection with the exercise of the functions conferred on the Department of Health and Social Care by or under the *Children and Young Persons Act 2001*; or the Department of Health and Social Care's functions in relation to social security or war pensions;

"relevant period" means the period of 6 months ending with the day on which the opinion would be relied upon;[66]

"war pension" has the same meaning as in section 25(4) of the Social Security Act 1989 (of Parliament)[27], as it applies in the Island.

Social work data

27. (1) The listed GDPR provisions do not apply to social work data to the extent that the serious harm test is met with respect to those data.

(2) The "serious harm test" in subparagraph (1) is met with respect to social work to the extent that the application of the listed applied GDPR provisions to the data would be likely to prejudice the carrying out of social work, because it would be likely to cause serious harm to the physical or mental health of the data subject or another individual.[67]

(3) In this paragraph —

"social work data" means personal data falling within any of the following descriptions —

(a) data processed by the Department of Health and Social Care —

(i) in connection with its functions under the *National Assistance (Isle of Man) Act 1951* or the *Children and Young Persons Act 2001*; or

(ii) in the exercise of other functions but obtained or consisting of information obtained in connection with any of those functions;

(b) data processed by the Probation Liaison Committee established by section 30 of the *Criminal Justice Act 1963*;

(c) data processed by the Department of Education, Sport and Culture in the exercise of its functions under section 30 of and Schedule 5 to the *Education Act 2001*;

(d) data processed by any voluntary organisation or other body designated under this sub-subparagraph by the Department of Health and Social Care and appearing to the Department to be processed for the purposes of the provision of any service similar to a service provided in the exercise of any functions specified in sub-subparagraph (a);

(e) data processed by a guardian ad litem appointed under section 51 of the *Adoption Act 1984*;

(f) data processed by an advocate appointed under section 96 of the *Children and Young Person Act 2001* or any person

[27] Applied to the Island by GC422/89, GC131/92 & SD589/95.

engaged by him to take any steps in the proceedings to which the appointment relates.

Education data

28. (1) The listed applied GDPR provisions do not apply to education data to the extent that the serious harm test is met with respect to those data.

(2) The "serious harm test" in subparagraph (1) is met with respect to education data to the extent the application of the listed applied GDPR provisions to the data would be likely to cause serious harm to the physical or mental health or condition of the data subject or any other person.

(3) In this paragraph —

"educational record" means any record of information which —

(a) relates to any person who is or has been a pupil at a school or college maintained by the Department of Education, Sport and Culture;

(b) is processed by or on behalf of that Department or the governing body of, or a teacher at, that school or college; and

(c) originated from or was supplied by or on behalf of any of the following —

(i) an employee of the Department of Education, Sport and Culture;

(ii) in the case of a maintained school (within the meaning of the *Education Act 2001*), a teacher or other employee at the school;

(iii) the pupil to whom the record relates; and

(iv) a parent (within the meaning of the *Education Act 2001*) of that pupil;

other than information which is processed by a teacher solely for the teacher's own use.

(4) In circumstances where the exemption in subparagraph (1) does not apply, where any person falling within subparagraph (5) is enabled by or under any enactment or rule of law to make a request on behalf of a data subject and has made such a request, personal data consisting of information as to whether the data subject is or has been the subject of, or may be at risk of, child abuse are exempt from Articles 15(1) to (3) of the applied GDPR in any case to the extent to which the application of that section would not be in the best interests of that data subject.

(5) A person falls within this paragraph if —

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

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

(6) For the purposes of subparagraph (4), "child abuse" includes physical injury (other than accidental injury) to, and physical and emotional neglect, ill-treatment and sexual abuse of, a minor.

(7) For the purposes of this paragraph, "a minor" is a natural person under the age of 18 years.[68]

Data subject's expectations and wishes

29. (1) Articles 15(1) to (3) of the applied GDPR (confirmation of processing, access to data and safeguards for third country transfers) do not apply to data concerning health, social work or education data (as defined in this Part of this Schedule) to the extent that complying with the request would disclose information which —

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

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

(c) the data subject has expressly indicated should not be so disclosed, and —

(i) the data subject is an individual aged under 16 years and the person making the request has parental responsibilities for the data subject; or

(ii) the data subject is incapable of managing his or her own affairs and the person making the request has been appointed by the court to manage those affairs.

(2) This paragraph does not apply if the data subject has expressly indicated that the data subject no longer has the expectation mentioned there.

PART 8 – APPLIED LED PROVISIONS TO BE RESTRICTED OR EXEMPTED

30. (1) Personal data processed for the purposes set out in Article 1(1) of the applied LED are, to the extent that the application of those provisions would be likely to prejudice any of the matters mentioned in Article 1(1), exempt from the following provisions of the applied LED and the associated, specified provisions of these Regulations —

(a) Article 4(1)(a), except to the extent to which the processing requires compliance with Article 8 of the applied LED;

(b) Article 13 and regulation 42 (information to be made available or given to the data subject);

(c) Article 14 and regulation 43 (right of access by the data subject);

(d) Article 16 and regulation 45 (right to rectification or erasure and restriction of processing);

(e) Article 18 and regulation 47 (rights of the data subject in criminal investigations and proceedings).

(2) Personal data which —

(a) are processed for the purpose of discharging statutory functions; and

(b) consist of information obtained for such a purpose from a person who possessed that information for any of the purposes mentioned in Article 1(1) of the applied LED,

are exempt from the provisions of the applied LED (and the associated, specified provisions of these Regulations) set out in subparagraph (1) to the same extent that the person from whom the personal data were obtained is exempt from those provisions.

(3) Where a controller applies an exemption under subparagraph (1)(iii), the controller, in accordance with regulation 44(4) of these Regulations and Article 15 of the applied LED, must document the factual or legal reasons on which its decision is based and make that information available to the Information Commissioner.

SCHEDULE 10

EXCEPTIONS TO ADEQUACY REQUIREMENTS

Regulation 68(2)(c)

1. Order of court, public authorities etc.

The transfer is specifically required by —

(a) an order or judgment of a court or tribunal having the force of law in the Island;

(b) an order or judgment of a court or tribunal of a country other than the Island or a decision of a public authority of such a country having the force of law in the Island that is based on an international agreement imposing an international obligation on the Island; or

(c) a decision of a public authority in the Island that is based on such an international agreement.

2. Consent

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 under Article 45 of the applied GDPR and appropriate safeguards.

3. Contract between data subject and controller

The transfer is necessary for —

(a) the performance of a contract between the data subject and the controller; or

(b) the implementation of pre-contractual measures taken at the data subject's request.

4. Third-party contract in interest of data subject

The transfer is necessary for the conclusion or performance of a contract between the controller and a person other than the data subject.

5. Transfers necessary for reasons of substantial public interest

The transfer is necessary for reasons of substantial public interest, which is taken to be the case if all the following circumstances apply —

(a) the transfer is a disclosure that is permitted or required under an enactment in operation in the Island;

(b) the transfer is made by or on behalf of the Isle of Man Financial Services Authority; and

(c) the European Commission has taken reasonable steps to ensure that the transferee will not transfer the personal data to another person except —

(i) with the consent of the European Commission; or

(ii) in order to comply with an order of a court (whether or not a court in the Island) that directs the transferee to transfer the personal data to the other person.

6. Legal proceedings etc.

The transfer —

(a) is necessary for the purpose of, or in connection with, any legal proceedings (including prospective legal proceedings);

(b) is necessary for the purpose of obtaining legal advice; or

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

7. Vital interests

The transfer is necessary in order to protect the vital interests of the data subject or of other persons, where —

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

(b) the data subject has unreasonably withheld consent; or

(c) the controller or processor cannot reasonably be expected to obtain the explicit consent of the data subject.

8. Public register

(1) The transfer is made from a register that —

(a) according to the relevant law is intended to provide information to the public; and

(b) is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest.

(2) However, a transfer under this paragraph —

(a) may take place only to the extent that the conditions laid down by the relevant law for consultation are fulfilled in the particular case;

(b) must not involve the entirety of the personal data or entire categories of personal data contained in the register; and

(c) where the register is intended for consultation by persons having a legitimate interest, may be made only at the request of those persons or where they are to be recipients of the data.

9. Other exceptions

(1) Where a transfer cannot be based on any other provision of these Regulations, a transfer to a third country or an international organisation may take place only if —

(a) the transfer is not repetitive;

(b) the transfer concerns only a limited number of data subjects;

(c) the transfer is necessary for the purposes of compelling legitimate interests pursued by the controller which are not overridden by the interests or rights and freedoms of the data subject; and

(d) the controller has assessed all the circumstances surrounding the data transfer and has on the basis of that assessment provided suitable safeguards with regard to the protection of personal data.

(2) Where a transfer is to take place under this paragraph, the controller must —

(a) inform the Information Commissioner of the transfer as soon as practicable; and

(b) in addition to providing any information required by Part 5 of these Regulations, inform the data subject of the transfer and on the compelling legitimate interests pursued.

(3) The controller or processor must document the assessment as well as the suitable safeguards referred to in paragraph 9(1)(d) in the records maintained under these Regulations.

10. Public authorities

Paragraphs 2, 3, 4 and 9 do not apply to activities carried out by public authorities in the exercise of their public powers.

SCHEDULE 11

SAVINGS AND TRANSITIONAL ARRANGEMENTS

Regulation 150

1. "The 2002 Act"

In this Schedule, **"the 2002 Act"** means the *Data Protection Act 2002*.

2. Processing underway at time of commencement of these Regulations

(1) Where, at the time of commencement of Article 5 of the Data Protection (Application of GDPR) Order 2018[28], consent to the processing of personal data was obtained in compliance with the requirements of the 2002 Act, that consent, to the extent that it was not given in a manner that complies with the applied GDPR, has effect until 25 May 2019.

(2) Where, at the time of the commencement of Article 5 of the Data Protection (Application of GDPR) Order 2018, the information to be provided to the data subject under Chapter III of the applied GDPR was provided by the controller to the data subject in compliance with the requirements of the 2002 Act, to the extent that such compliance is not compliance with the applied GDPR, the controller is nevertheless treated as complying with it until 25 May 2019.

3. Request for information and copy of personal data

A request for information and a copy of personal data under the 2002 Act that has not been complied with on the commencement of these Regulations is treated as a request under Article 15 of the applied GDPR or regulation 42 of these Regulations, save that no fee paid is refundable.

4. Right to compensation for inaccuracy, loss or unauthorised disclosure

A claim for compensation under the 2002 Act that remains outstanding on the coming into operation of these Regulations is, despite regulation 125 of these Regulations, treated as if the relevant provision of the 2002 Act continued in operation.

5. Application for rectification and erasure

An application for rectification and disclosure under the 2002 Act that remains outstanding on the coming into operation of these regulations is treated as if the relevant provisions of the 2002 Act continued in operation.

6. Self-incrimination, etc.

[28] SD 2018/0143

Any reference in these Regulations to an offence includes a reference to an offence committed under the 2002 Act before the coming into operation of Article 5 of the Data Protection (Application of GDPR) Order 2018[29].

7. Effect of notification under the 2002 Act

Where, under Part 3 of the 2002 Act, an entry in respect of the controller is included in the register maintained by the Information Commissioner, that controller is not required to register in accordance with the provisions of Schedule 7 to these Regulations until the expiration of that entry.

8. Enforcement notices

If, immediately before the coming into operation of these Regulations, an enforcement notice is served under section 36 of the 2002 Act, that notice has effect after such coming into operation as if it were an enforcement notice made under regulation 106 of these Regulations.

9. Information notices

If, immediately before the coming into operation of these Regulations, an information notice is served under section 39 of the 2002 Act, that notice has effect after such coming into operation as if it were an information notice made under regulation 101 of these Regulations.

10. Requests for assessment

(1) Any request for assessment under section 38 of the 2002 Act that the Information Commissioner has not dealt with before the coming into operation of these Regulations has effect as if it were a complaint under regulation 122.

(2) The repeal of the 2002 Act by the Data Protection (Application of GDPR) Order 2018 does not affect the application of the relevant provisions of that Act in any case where the request for assessment was received by the Information Commissioner before the commencement of the repeal.

(3) In dealing with a request for assessment under the 2002 Act or a request for an assessment under that Act, the Information Commissioner must have regard to the provisions from time to time applicable to the processing, and accordingly —

(a) in the 2002 Act, the reference to the old principles and provisions of these Regulations includes, in relation to any time when the new principles and the provisions of these Regulations have effect, those principles and provisions; and

(b) in these Regulations, the reference to the provisions of these Regulations includes, in relation to any time when the old

[29] SD 2018/0143

principles and the provisions of the 2002 Act had effect, those provisions.

11. General saving

Except as provided otherwise in this Schedule, anything made or done by any person under any provision of the 2002 Act (being a thing that still had force or effect immediately before the repeal of the 2002 Act), if there is a provision under these Regulations that gives power to make or do such a thing, is taken to have been made or done under the latter provision.

SCHEDULE 12

CONDITIONS FOR SPECIAL CATEGORY PROCESSING UNDER PART 3

Regulation 37(3)

1. Statutory etc. purposes

This condition is met if the processing —

(a) is necessary for the exercise of a function conferred on a person by an enactment or rule of law; and

(b) is necessary for reasons of substantial public interest.

2. Administration of justice

This condition is met if the processing is necessary for the administration of justice.

3. Protecting natural person's vital interests

This condition is met if the processing is necessary to protect the vital interests of the data subject or another natural person.

4. Safeguarding of children and of individuals at risk

(1) This condition is met if —

(a) the processing is necessary for the purposes of —

(i) protecting a natural person from neglect or physical, mental or emotional harm; or

(ii) protecting the physical, mental or emotional well-being of a natural person;

(b) the natural person is —

(i) aged under 18; or

(ii) aged 18 or over and at risk;

(c) the processing is carried out without the consent of the data subject for one of the reasons listed in subparagraph (2); and

(d) the processing is necessary for reasons of substantial public interest.

(2) The reasons mentioned in subparagraph (1)(c) are —

(a) in the circumstances, consent to the processing cannot be given by the data subject;

(b) in the circumstances, the controller cannot reasonably be expected to obtain the consent of the data subject to the processing;

(c) the processing must be carried out without the consent of the data subject because obtaining the consent of the data subject would prejudice the provision of the protection mentioned in subparagraph (1)(a).

(3) For the purposes of this paragraph, a natural person aged 18 or over is "at risk" if the controller has reasonable cause to suspect that the natural person —

(a) has needs for care and support;

(b) is experiencing, or at risk of, neglect or physical, mental or emotional harm; and

(c) as a result of those needs is unable to protect himself or herself against the neglect or harm or the risk of it.

(4) In subparagraph (1)(a), the reference to the protection of a natural person or of the well-being of a natural person includes both protection relating to a particular natural person and protection relating to a type of natural person.

5. Personal data already in the public domain

This condition is met if the processing relates to personal data which are manifestly made public by the data subject.

6. Legal claims

This condition is met if the processing —

(a) is necessary for the purpose of, or in connection with, any legal proceedings (including prospective legal proceedings);

(b) is necessary for the purpose of obtaining legal advice; or

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

7. Judicial Acts

This condition is met if the processing is necessary when a court or other judicial authority is acting in its judicial capacity.

8. Preventing fraud

(1) This condition is met if the processing —

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

(b) consists of —

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

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

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

(2) In this paragraph, "anti-fraud organisation" has the same meaning as in section 68 of the Serious Crime Act 2007 (of Parliament).

9. Archiving

This condition is met if the processing is necessary —

(a) for archiving purposes in the public interest;

(b) for scientific or historical research purposes; or

(c) for statistical purposes.

ENDNOTES

Table of Endnote References

[1] The format of this legislation has been changed as provided for under section 75 of, and paragraph 2 of Schedule 1 to, the Legislation Act 2015. The changes have been approved by the Attorney General after consultation with the Clerk of Tynwald as required by section 76 of the Legislation Act 2015.
[2] Para (1) substituted by SD2018/0309.
[3] Para (1) substituted by SD2018/0309.
[4] Para (1) substituted by SD2018/0309.
[5] Para (4) amended by SD2018/0309.
[6] Para (1) amended by SD2018/0309.
[7] Para (1) amended by SD2018/0309.
[8] Para (2) amended by SD2018/0309.
[9] Para (4) amended by SD2018/0309.
[10] Reg 77 substituted by SD2018/0309.
[11] Reg 78 substituted by SD2018/0309.
[12] Reg 96 heading amended by SD2018/0309.
[13] Reg 101 substituted by SD2018/0309.
[14] Reg 103 substituted by SD2018/0309.
[15] Reg 104 substituted by SD2018/0309.
[16] Para (5) amended by SD2018/0309.
[17] Subpara (b) amended by SD2018/0309.
[18] Para (1) substituted by SD2018/0309.
[19] Para (1) substituted by SD2018/0309.
[20] Reg 118 heading amended by SD2018/0309.
[21] Para (1) substituted by SD2018/0309.
[22] Subpara (a) substituted by SD2018/0309.
[23] Reg 131 revoked by SD2018/0309.
[24] Subpara (a) amended by SD2018/0309.
[25] Para (6) amended by SD2018/0309.
[26] Para 1 heading amended by SD2018/0309.
[27] Subpara (1) amended by SD2018/0309.
[28] Definition of "social security law" amended by SD2018/0309.
[29] Para 14 substituted by SD2018/0309.
[30] Para 14A inserted by SD2018/0309.
[31] Subpara (8) inserted by SD2018/0309.
[32] Item (ab) inserted by SD2018/0309.
[33] Subpara (3) substituted by SD2018/0309.
[34] Subpara (3) amended by SD2018/0309.
[35] Para 21 substituted by SD2018/0309.

[36] Para 28 substituted by SD2018/0309.
[37] Para 28A inserted by SD2018/0309.
[38] Subpara (6) amended by SD2018/0309.
[39] Subpara (2) amended by SD2018/0309.
[40] Subpara (2) amended by SD2018/0309.
[41] Item (a) amended by SD2018/0309.
[42] Sub-item (i) amended by SD2018/0309.
[43] Item (e) amended by SD2018/0309.
[44] Sub-item (i) amended by SD2018/0309.
[45] Sub-item (iii) amended by SD2018/0309.
[46] Sub-item (ii) amended by SD2018/0309.
[47] Item (e) amended by SD2018/0309.
[48] Cross-heading inserted by SD2018/0309.
[49] Subpara (2) amended by SD2018/0309.
[50] Para 4 (and associated cross-heading) revoked by SD2018/0309.
[51] Para 5 (and associated cross-heading) revoked by SD2018/0309.
[52] Subpara (1) amended by SD2018/0309.
[53] Subpara (2) amended by SD2018/0309.
[54] Item (c) amended by SD2018/0309.
[55] Subpara (3) amended by SD2018/0309.
[56] Sub-item (ii) amended by SD2018/0309.
[57] Item (b) amended by SD2018/0309.
[58] Subpara (5) amended by SD2018/0309.
[59] Item (a) substituted by SD2018/0309.
[60] Item (b) substituted by SD2018/0309.
[61] Item (c) inserted by SD2018/0309.
[62] Para 17 amended by SD2018/0309.
[63] Cross-heading inserted by SD2018/0309.
[64] Para 21A inserted by SD2018/0309.
[65] Item (a) amended by SD2018/0309.
[66] Definition of "relevant period" inserted by SD2018/0309.
[67] Subpara (2) amended by SD2018/0309.
[68] Subpara (7) inserted by SD2018/0309.