



BILLET D'ÉTAT

WEDNESDAY, 16th MAY, 2018

XII
2018

ELECTIONS AND APPOINTMENTS

1. Committee for Home Affairs - Appointment of the Data Protection Authority, P.2018/35
2. Election of Members of The Ladies' College Board of Governors, P.2018/36

LEGISLATIVE BUSINESS

Legislation Laid Before the States

The Post Office (Bailiwick of Guernsey) Law, 2001 (Amendment) Ordinance, 2018

The Health Service (Benefit) (Limited List) (Pharmaceutical Benefit) (Amendment No. 2) Regulations, 2018

The Misuse of Drugs (Modification No. 2) Order, 2018

Legislation for Approval

3. Committee for Home Affairs - The Data Protection (Commencement, Amendment and Transitional) (Bailiwick of Guernsey) Ordinance, 2018, P.2018/32
4. Committee for Home Affairs - The Data Protection (Law Enforcement and Related Matters) (Bailiwick of Guernsey) Ordinance, 2018, P.2018/33

OTHER BUSINESS

5. Requête – Assisted Dying, P.2018/24
6. Schedule for future States' business, P.2018/34

BILLET D'ÉTAT

TO
THE MEMBERS OF THE STATES
OF THE ISLAND OF GUERNSEY

I hereby give notice that a Meeting of the States of Deliberation will be held at **THE ROYAL COURT HOUSE**, on **WEDNESDAY**, the **16th May, 2018** at **9.30 a.m.**, to consider the items listed in this Billet d'État which have been submitted for debate.

R. J. MCMAHON
Deputy Bailiff and Presiding Officer

The Royal Court House
Guernsey

20th April, 2018

THE STATES OF DELIBERATION
of the
ISLAND OF GUERNSEY

COMMITTEE FOR HOME AFFAIRS

APPOINTMENT OF THE DATA PROTECTION AUTHORITY

The States are asked to decide:-

Whether, after consideration of the Policy Letter dated 9th April 2018, of the Committee *for* Home Affairs, they are of the opinion:-

To appoint with effect on and from 25th May 2018 the following persons, as nominated by the Committee, to be voting members of the Data Protection Authority under paragraph 1 of Schedule 6 to the Data Protection (Bailiwick of Guernsey) Law, 2017:

- (a) Mr Richard Thomas CBE as Chairman of the Data Protection Authority for a period of five years,
- (b) Mr Simon Entwisle as a voting member of the Data Protection Authority for a period of five years,
- (c) Mr John Curran as a voting member of the Data Protection Authority for a period of five years,
- (d) Mr Christopher Docksey as a voting member of the Data Protection Authority for a period of four years,
- (e) Mr Mark Lempriere as a voting member of the Data Protection Authority for a period of four years,
- (f) Ms Jennifer Strachan as a voting member of the Data Protection Authority for a period of four years.

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

THE STATES OF DELIBERATION
of the
ISLAND OF GUERNSEY

COMMITTEE FOR HOME AFFAIRS

APPOINTMENT OF THE DATA PROTECTION AUTHORITY

The Presiding Officer
States of Guernsey
Royal Court House
St Peter Port

9th April, 2018

Dear Sir

1 Executive Summary

1.1 The purpose of this Policy Letter is to appoint the Chairman and members of the Data Protection Authority (“the Authority”) established under the Data Protection (Bailiwick of Guernsey) Law, 2017 (“the Law”).

2 Background

2.1 The Law will come into effect on 25th May 2018. Part XI of the Law establishes the Authority. Schedule 6 to the Law sets out the constitution of the Authority and provides that the Chairman and other voting members must be appointed by resolution of the States of Deliberation from individuals nominated by the Committee *for* Home Affairs (“the Committee”).

2.2 This Policy Letter recommends the appointment of the Chairman and five members to the Authority with effect on and from 25th May 2018 in order to ensure that the Authority is constituted when the Law is enacted.

3 Appointment of Chairman and Members of the Authority

3.1 Schedule 6 to the Law states that the Authority comprises a Chairman and no fewer than four and no more than eight other voting members, with the exact number being determined by the Committee, and the Commissioner, as an *ex officio* and non-voting member.

- 3.2 In recommending the individuals to the States, pursuant to paragraph 1(3) of Schedule 6 to the Law, the Committee must have particular regard to the need to “ensure that voting members of the Authority –
- (a) have the qualifications, experience and skills necessary to exercise and perform the functions of a member, in particular relating to the protection of personal data,
 - (b) have a strong sense of integrity, and
 - (c) are able to maintain confidentiality.”
- 3.3 Each voting member is to be appointed for a term of not less than four, and not more than five, years as the Committee thinks fit in a particular case.
- 3.4 It was originally anticipated that there might be a joint Authority with Jersey but in the event the Bailiwicks developed the respective laws which were different in a number of ways. Nonetheless as part of the pan-Island preparation for the new arrangements an executive recruitment agency was engaged to assist with identifying people suitable to fulfil the role as Chairman.
- 3.5 A recruitment campaign for the Authority members was designed to reach as many areas of the population as possible and included advertising locally in the media and further afield through social media.
- 3.6 Following an open and transparent recruitment process the Committee was impressed with the quality and experience of all candidates.
- 3.7 The Committee is pleased to recommend the following individuals for appointment to the Authority.

Chairman – 5 year appointment

- 3.8 Mr Richard Thomas CBE was the UK’s Information Commissioner from 2002 to 2009, responsible for enforcement of the Data Protection and Freedom of Information Acts. He was subsequently the Chairman of the Administrative Justice and Tribunals Council and served as a Member of the Committee on Standards in Public Life from 2012 to 2017. In January 2018, he was appointed by the Prime Minister to the Advisory Committee on Business Appointments.

Voting members – 5 year appointment

- 3.9 Mr Simon Entwisle has recently retired from his role as Deputy Commissioner at the UK Information Commissioner’s Office (ICO), a position he held for over

13 years. He has vast experience of data protection and the ICO management board.

Mr Entwisle has demonstrated a clear analytical mind and the ability to understand and effectively communicate complex legislative issues so as to be understood by all stakeholders. His previous roles have required the ability to react strategically, maintaining high standards and accuracy whilst dealing with competing priorities.

- 3.10 Mr John Curran is a former Chief Executive of the Channel Islands Competition and Regulatory Authorities (CICRA) and currently sits on the Board of the Channel Islands Financial Ombudsman and as a non-voting Member on the States of Guernsey Transport Licensing Authority (TLA).

Mr Curran has experience acting within a regulatory model and proven experience in interpreting and applying complex legislation. Past roles have demonstrated the ability to balance the competing interests of stakeholders, asserting sound judgement and sensitivity.

Voting members – 4 year appointment

- 3.11 Mr Christopher Docksey has recently retired as Director of the Secretariat of the European Data Protection Supervisor and worked as the Legal Adviser on data protection to the European Commission. Mr Docksey has extensive experience in the field of data protection, including facilitating the practical implementation of the General Data Protection Regulation working strategically with multiple legislative institutions and delivering high quality outcomes.

While Mr Docksey is currently based in Brussels, this is not considered to be a barrier to his active participation as a member of the Authority and his practical experience will be an asset to the Authority in meeting the challenges posed by the new legislation.

- 3.12 Mr Mark Lempriere retired as the Chief Secretary to the Committee *for* Home Affairs in April 2018 where he was instrumental in the strategic development of the new Guernsey Data Protection legislation.

Mr Lempriere has considerable experience strategically and operationally in the development, compliance and practical enforcement of statutory regimes and demonstrated a proven ability to maintain accuracy.

- 3.13 Ms Jennifer Strachan is currently the Chief Executive of Startup Guernsey and during her career has held numerous Directorial positions involving regulations and compliance. She has been an adviser in the creation of policies such as the Digital Strategy Framework.

Ms Strachan has demonstrated effective Board governance, has experience in strategic planning and development and is comfortable working with a regulatory framework. She is aware of the importance of identifying opportunities for improved working which will benefit business, the consumer and the community and is committed to delivering high quality, efficient and cost effective services.

4 Compliance with Rule 4 of the Rules of Procedure of the States of Deliberation and their Committees

4.1 Rule 4 of the Rules of Procedure of the States of Deliberation and their Committees sets out the information which must be included in, or appended to, motions laid before the States.

4.2 In accordance with Rule 4(4) of the Rules of Procedure of the States of Deliberation and their Committees, it is confirmed that the propositions above have the unanimous support of the Committee. Please note that Deputy VS Oliver was absent from the Committee meeting when these propositions were considered.

4.3 In accordance with Rule 4(5), the Propositions relate to the duties of the Committee "to advise the States and to develop and implement policies on matters relating to its purpose, including:[...] data protection".

Yours faithfully

M M Lowe
President

R G Prow
Vice-President

R H Graham
M P Leadbeater
V S Oliver

THE STATES OF DELIBERATION
of the
ISLAND OF GUERNSEY

COMMITTEE *FOR* HOME AFFAIRS

APPOINTMENT OF THE DATA PROTECTION AUTHORITY

The President
Policy & Resources Committee
Sir Charles Frossard House
La Charroterie
St Peter Port

10th April 2018

Dear Sir,

Preferred date for consideration by the States of Deliberation

In accordance with Rule 4(2) of the Rules of Procedure of the States of Deliberation and their Committees, the Committee *for* Home Affairs requests that the "Appointment of the Data Protection Authority" Policy Letter be considered at the States' meeting to be held on 16th May 2018.

The above referenced Policy Letter seeks approval of the appointment of the Data Protection Authority established under the Data Protection (Bailiwick of Guernsey) Law 2017 which comes into force on 25th May 2018. In order to meet adequacy with the European Union, Guernsey will need the Chairman and members of the Authority to be endorsed by the States of Deliberation prior to the enactment of the Law. The Committee therefore respectfully requests that arrangements are made for the States of Deliberation to consider this Policy Letter at its meeting on 16th May 2018.

Yours faithfully,

M M Lowe
President

R G Prow
Vice-President

R H Graham
M P Leadbeater
V S Oliver

**ELECTION OF MEMBERS OF THE
LADIES' COLLEGE BOARD OF GOVERNORS**

The States are asked:

- (1) To elect Ms Cathryn Llywella Perkins as a member of the Ladies' College Board of Governors who has been nominated in that behalf by the Chairman, the two States-appointed Governors and the two Governors appointed by the States on the nomination of the Committee *for* Education, Sport & Culture, and whose term of office will expire on the 31st May 2018.

N.B. Nominations cannot be made from the floor of the Assembly.

- (2) To elect Mr Peter Miller as a member of the Ladies' College Board of Governors, who has been nominated in that behalf by the Committee *for* Education, Sport & Culture, to replace Mr John Marren whose term of office will expire on 31st May 2018.

N.B. Nominations cannot be made from the floor of the Assembly.



Les Gravées, St Peter Port
Guernsey, GY1 IRW

Tel: (01481) 721602
Fax: (01481) 724209

The Bailiff
Bailiff's Chambers
The Royal Court House
St Peter Port
GY1 2NZ



6th April 2018

Dear Sir

I am writing at the request of the Board of Governors of The Ladies' College which would be grateful if you would request the States to appoint Ms Cathy Perkins as a member of the Board for a further three-year term of office. Ms Perkins has served as a member of the Board, nominated by the Board, since January 2017 but her current term of office will end on 31 May 2018.

As you are aware, the Board of Governors has conducted a skills analysis of the Governors in order to ensure that the Board has a suitable range of skills and experience amongst its members. In so doing, the Board were mindful of the guidance of the Association of Governing Bodies in Independent Schools (AGBIS), of which the College is a member, about the range of backgrounds and skills that a Governing Body should ideally encompass.

Ms Perkins brings to the Board a broad range of financial and management experience gained in an operating environment and serves on both the Finance and Development Committees of the Board. Ms Perkins is also an alumna of the College.

Ms Perkins has confirmed her willingness to continue to act in this capacity as a member of the Board of Governors.

Ms Perkins' CV is attached and Deputy Heidi Soulsby has agreed to be her proposer in the States.

Yours faithfully

Elizabeth Bridge
Clerk to the Governors

CV for Ms Cathy Perkins

Ms Perkins is the Group Accounting Technical Manager at Specsavers Optical Group Limited, responsible for the preparation of the financial statements for a large number of entities. She also manages the delivery of training and development for all Chartered Accountants throughout the Specsavers Group. Ms Perkins' previous role as Internal Audit Senior Manager included establishing and managing the group risk matrix and undertaking process reviews. Whilst at Specsavers, Ms Perkins has also been responsible for the management of events.

Ms Perkins has a long association with The Ladies' College having attended the College and currently serving on both the Parents' Association Committee and The College Guild Committee.

Ms Perkins has also contributed to the governance of the College as an Associate Governor from May 2016 and then as a Governor from January 2017 where she has served as a member of the Finance and Development Committees.

Principal
Mrs A Clancy BA (Combined Hons)
Email: principal@ladiescollege.ac.gg

Registrar
Miss R McClean
Email: registrar@ladiescollege.ac.gg

Bursar & Clerk to the Governors
Miss E Bridge MA Oxon, ACA
Email: bursar@ladiescollege.ac.gg



Committee *for*
Education, Sport & Culture

The Presiding Officer
States of Guernsey
Royal Court House
St Peter Port

Sir Charles Frossard House
La Charroterie
St Peter Port
Guernsey
GY11FH
+44 (0) 1481 733000
educationsportandculture@gov.gg
www.gov.gg

12 April 2018

Dear Sir

Election of a Member of The Ladies' College Board of Governors

The Committee *for* Education, Sport & Culture wishes to put forward Mr Peter Miller for election as a Committee nominated member of The Ladies' College Board of Governors with effect from 1 June 2018.

Mr Miller will replace Mr John Marren whose term of office expires on 31 May 2018 and who has confirmed that he does not wish to be considered for a further term of office.

Selecting a Governor with the right skills to complement the other members is vitally important. To this end, a regular skills analysis of the College Governors is undertaken to ensure that the Board has a suitable range of skills and experience amongst its members. One such requirement identified is that there should be Governors with appropriate financial skills and background in order to provide financial advice and guidance to the College. Mr Marren undertook this role and the College has indicated that it would welcome the appointment of a Governor with similar skills to replace Mr Marren; Mr Peter Miller, Associate Partner with Ernst & Young, is considered an appropriate replacement for the following reasons.

Mr Miller is a qualified accountant with 18 years post-qualification experience with Ernst & Young spanning all aspects of the offshore asset management and insurance industries. He has extensive knowledge of auditing and accounting matters. He is part of the leadership team in the Channel Islands, with a primary focus on Guernsey operations, including resourcing and finance and has responsibility for the Channel Islands marketing and business development team. It is considered that Mr Miller would complement the other Governors on the Board to ensure a full range of backgrounds and skills.

I confirm that I have seen Mr Miller's Declaration of Interest and am satisfied that there would be no conflict of interest in his appointment to the Board of Governors. Mr Miller has also confirmed to me his willingness to be elected. Mr Miller's appointment is supported by both the College and the Committee.

Peter was brought up in England, went to university in Scotland and has been in Guernsey ever since. He has 2 children, a daughter who is at The Ladies' College and a son at Elizabeth College. His hobbies are running, golf, squash and reading.

Yours faithfully,

SIGNED

Deputy Matt Fallaize
President,
Committee *for* Education, Sport & Culture

ORDINANCE LAID BEFORE THE STATES

**THE POST OFFICE (BAILIWICK OF GUERNSEY) LAW, 2001 (AMENDMENT)
ORDINANCE, 2018**

In pursuance of the provisions of the proviso to Article 66A(1) of The Reform (Guernsey) Law, 1948, as amended, "The Post Office (Bailiwick of Guernsey) Law, 2001 (Amendment) Ordinance, 2018", made by the Policy & Resources Committee on the 27th March, 2018, is laid before the States.

EXPLANATORY MEMORANDUM

This Ordinance amends section 10(5) of the Post Office (Bailiwick of Guernsey) Law, 2001 to remove the requirement that a scheme made by a universal postal service provider be published in La Gazette Officielle before it comes into force. Instead, pursuant to section 10(8) (which is not amended by this Ordinance), a notice that a scheme has been made or modified will be placed in La Gazette with an explanation of where a written copy of the scheme or modification may be inspected.

The Ordinance was made by the Policy & Resources Committee in exercise of its powers under Article 66A(1) of the Reform (Guernsey) Law, 1948, and came into force on the 27th March, 2018. Under the proviso to Article 66A(1) of the Reform (Guernsey) Law, 1948, the States of Deliberation have the power to annul the Ordinance.

STATUTORY INSTRUMENTS LAID BEFORE THE STATES

No. 9 of 2018

THE HEALTH SERVICE (BENEFIT) (LIMITED LIST) (PHARMACEUTICAL BENEFIT) (AMENDMENT NO.2) REGULATIONS, 2018

In pursuance of section 35 of the Health Service (Benefit) Law, 1990, the Health Service (Benefit) (Limited List) (Pharmaceutical Benefit) (Amendment No.2) Regulations, 2018 made by the Committee *for* Employment & Social Security on 6th March, 2018, are laid before the States.

EXPLANATORY NOTE

These Regulations add to the list of drugs that may be prescribed as pharmaceutical benefit, and extend the prescribing criteria for a medical appliance to allow the appliance to be prescribed to people over the age of 18 if certain conditions are met. These Regulations came into operation on 7th March, 2018.

No. 10 of 2018

THE MISUSE OF DRUGS (MODIFICATION NO. 2) ORDER, 2018

In pursuance of section 30(3) of the Misuse of Drugs (Bailiwick of Guernsey) Law, 1974, as amended, "The Misuse of Drugs (Modification No. 2) Order, 2018" made by the Committee *for* Health & Social Care on the 7th March 2018 is laid before the States.

EXPLANATORY NOTE

This Order amends the Misuse of Drugs (Bailiwick of Guernsey) Ordinance, 1997 ("the Ordinance").

Article 2 of this Order amends the Ordinance by inserting two new paragraphs at the end of Schedule 2 to the Ordinance. This amendment would allow Sativex and any other medicinal cannabinoid products approved for marketing for human use by the Medicines and Healthcare Products Regulatory Agency or the European Medicines Agency to be prescribed, administered, supplied etc. like any other Schedule 2 controlled drug.

Article 3 is the interpretation provision. Articles 4 and 5 are the citation and commencement provisions respectively.

The Misuse of Drugs (Bailiwick of Guernsey) Law, 1974 and the Misuse of Drugs (Amendment) (Bailiwick of Guernsey) Law, 2000 allows the Committee for Health & Social Care to add other cannabinoid products for medicinal use to Schedule 2 to the Ordinance from time to time, as the Committee sees fit.

This Order came into force on the 1st April, 2018.

The full text of the statutory instruments and other legislation included in this document can be found at <http://www.guernseylegalresources.gg/article/163343/2018>

**THE DATA PROTECTION (COMMENCEMENT, AMENDMENT AND TRANSITIONAL)
(BAILIWICK OF GUERNSEY) ORDINANCE, 2018**

The States are asked to decide:-

Whether they are of the opinion to approve the draft Ordinance entitled "The Data Protection (Commencement, Amendment and Transitional) (Bailiwick of Guernsey) Ordinance, 2018", and to direct that the same shall have effect as an Ordinance of the States.

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

EXPLANATORY MEMORANDUM

This Ordinance is made under the Data Protection (Bailiwick of Guernsey) Law, 2017 ("**the Law**"). It amends the Law, makes consequential amendments to Ordinances in Guernsey, Sark and Alderney relating to e-Privacy, and makes transitional and savings provisions. It brings the Law into force on the 25th May, 2018.

PART I
PRELIMINARY

This Part brings the Law and this Ordinance into force on the 25th May, 2018.

PART II
TRANSITION FOR OPERATIVE PROVISIONS

This Part provides for a transitional period of one year before controllers and processors are required to comply with certain duties under the Law or the Data Protection (Law Enforcement and Related Matters) (Bailiwick of Guernsey) Ordinance, 2018 ("**Law Enforcement Ordinance**"). It also allows public authorities to continue processing personal data under the Law based on the legitimate interest of those public authorities during this transitional period. Finally this Part makes provision for notification of a personal data breach occurring before the commencement of the Law.

PART III
SAVING OF CONSENTS, PROCEEDINGS AND OTHER MATTERS

This Part saves the effect of consent to authorisation validly obtained under the Data Protection (Bailiwick of Guernsey) Law, 2001 ("**former Law**") before the commencement of the Law. It also saves designations and notifications of Bailiwick representatives, and authorisations for transfers given by the Data Protection Commissioner under the former Law. Finally, it saves proceedings brought or offences

committed under the former Law, and provides for other things done under the former Law to continue to have effect where there are corresponding provisions for those things under the new Law.

PART IV
TRANSITION OF RIGHTS, RECORDS, ETC

This Part transfers assets, rights, liabilities, obligations, records, etc. of the Data Protection Commissioner to the Authority.

PART V
GENERAL

This Part revokes Orders and Regulations made under the former Law, and makes several amendments to the Law. It also amends the European Communities (Implementation of Privacy Directive) (Guernsey) Ordinance, 2004 and equivalent Ordinances in Alderney and Sark to align those Ordinances with the enforcement provisions under the new Law. Finally it sets out the interpretation and citation provisions.

The Data Protection (Commencement, Amendment and Transitional) (Bailiwick of Guernsey) Ordinance, 2018

ARRANGEMENT OF SECTIONS

PART I PRELIMINARY

1. Commencement of the Data Protection (Bailiwick of Guernsey) Law, 2017 and this Ordinance.

PART II TRANSITION FOR OPERATIVE PROVISIONS

2. Transitional exemption from duty to notify pre-collected personal data.
3. Transitional exemption from duties of joint controllers in relation to continued processing.
4. Transitional exemption from impact assessment duties in relation to continued processing.
5. Transitional exemption from processor-use duties in relation to continued processing.
6. Transitional exemption from processor's duty to establish measures in relation to continued processing.
7. Transitional exemption from processor's duty to obtain controller authorisation for secondary processors.
8. Meaning of "**continued processing**".
9. Transitional provision for processing by public authorities based on legitimate interest.
10. Delayed effect of section 14 (right to data portability) of the Law.
11. Reporting of personal data breaches occurring before commencement.

PART III SAVING OF CONSENTS, PROCEEDINGS AND OTHER MATTERS

12. Validity of consents obtained before commencement.
13. Prior designation and notification of Bailiwick representatives.
14. Saving of authorisation for transfer to unauthorised jurisdictions.
15. Saving of proceedings, etc. under former Law.
16. Offences under former Law.
17. Other things done under former Law.

PART IV
TRANSITION OF RIGHTS, RECORDS, ETC.

18. Rights, liabilities, records, etc.

PART V
GENERAL

19. Revocations.
20. Amendments to the Data Protection (Bailiwick of Guernsey) Law, 2017.
21. Consequential amendments to e-Privacy Ordinances.
22. Interpretation.
23. Citation.

SCHEDULE 1	Orders and regulations revoked
SCHEDULE 2	Amendments to the Data Protection (Bailiwick of Guernsey) Law, 2017
SCHEDULE 3	Consequential amendments to e-Privacy Ordinances

The Data Protection (Commencement, Amendment and Transitional) (Bailiwick of Guernsey) Ordinance, 2018

THE STATES, in pursuance of their Resolution of the 26th April, 2017^a, and in exercise of the powers conferred on them by sections 103, 104, 105, 106, 107, 108 and 115 of the Data Protection (Bailiwick of Guernsey) Law, 2017^b following consultation with the Policy and Finance Committee of the States of Alderney, the Policy and Performance Committee of the Chief Pleas of Sark and the former Commissioner, hereby order:-

PART I PRELIMINARY

Commencement of the Data Protection (Bailiwick of Guernsey) Law, 2017 and this Ordinance.

1. The Data Protection (Bailiwick of Guernsey) Law, 2017 and this Ordinance shall come into force on the 25th May, 2018.

PART II TRANSITION FOR OPERATIVE PROVISIONS

Transitional exemption from duty to notify pre-collected personal data.

2. (1) Until the transition date and subject to subsection (2), a controller is not required to comply with a notification duty in relation to the processing of pre-collected personal data in the context of the controller.

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

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

(2) On request by a data subject, a controller exempt from a notification duty by reason only of subsection (1) must give the data subject any information that the notification duty would otherwise have required the controller to –

- (a) give to the data subject, or
- (b) otherwise publish in relation to the pre-collected personal data relating to the data subject.

(3) In this section –

"notification duty" means any duty imposed on a controller by –

- (a) section 12(2), (3) or (3A) of the Law,
- (b) section 13(1), (2) or (2A) of the Law,
- (c) section 17(3) of the Law,
- (d) section 18(3) of the Law, or
- (e) section 12(2) or (3) of the Law Enforcement Ordinance,
and

"pre-collected personal data" means any personal data processed in the context of a controller, where the personal data was collected before the commencement date –

- (a) by the controller, or a processor acting on the controller's behalf, or
- (b) otherwise for the purposes of the processing.

Transitional exemption from duties of joint controllers in relation to continued processing.

3. (1) Until the transition date, a controller is not required to comply with a joint controller duty in relation to continued processing of personal data in the context of the joint controllers concerned.

(2) In subsection (1), "**joint controller duty**" means any duty imposed on joint controllers by –

- (a) section 33(1) or (3) of the Law, or
- (b) section 28(1) of the Law Enforcement Ordinance.

Transitional exemption from impact assessment duties in relation to continued processing.

4. (1) Until the transition date, a controller is not required to comply with an impact assessment duty in relation to continued processing of personal data in the context of the controller.

(2) In subsection (1), "**an impact assessment duty**" means any duty imposed on a controller –

- (a) to carry out, review or revise an assessment under section 44(1) or (5) of the Law or section 36(1) of the Law Enforcement Ordinance, or
- (b) to consult the Authority under section 45(2) of the Law or section 37(2) of the Law Enforcement Ordinance.

Transitional exemption from processor-use duties in relation to continued processing.

5. (1) Until the transition date, a controller is not required to comply with a processor-use duty where –

- (a) the controller causes or permits a processor to carry out processing of personal data in the context of that controller, and
- (b) the processing is continued processing of the personal data in the context of both the controller and the processor concerned.

(2) In subsection (1), "**processor-use duty**" means any duty imposed on a controller by –

- (a) section 34(1) of the Law, or
- (b) section 29(1) of the Law Enforcement Ordinance.

Transitional exemption from processor's duty to establish measures in relation to continued processing.

6. (1) Until the transition date, a processor is not required to comply with a duty to establish measures in respect of the controller, in relation to continued processing of personal data in the context of both the processor and that controller.

(2) In subsection (1), "**duty to establish measures**" means any duty imposed on a processor by –

- (a) section 35(1)(e) of the Law,
- (b) section 36(3) of the Law, to the extent that it imposes a duty on the processor under section 35(1)(e) of the Law,
or
- (c) section 30(1)(e) of the Law Enforcement Ordinance.

Transitional exemption from processor's duty to obtain controller authorisation for secondary processors.

7. (1) Until the transition date, a processor is not required to comply with a duty to obtain authorisation from the controller in relation to a secondary processor where –

- (a) the processor is carrying out continued processing of personal data in the context of both the processor and that controller, and

- (b) the processor had, before the commencement date, engaged the secondary processor concerned to process that personal data.

(2) In subsection (1) –

"**duty to obtain authorisation**" means any duty imposed on a processor by –

- (a) section 36(1) of the Law, or
- (b) section 31(1) of the Law Enforcement Ordinance, and

"**secondary processor**", in relation to section 36(1) of the Law or section 31(1) of the Law Enforcement Ordinance, has the meaning given by the respective provision.

Meaning of "continued processing".

8. (1) For the purposes of sections 3 to 7, processing of personal data ("**the processing concerned**") is continued processing in the context of a controller or processor where processing of the same kind as the processing concerned –

- (a) was carried out on the personal data in the context of the controller or processor concerned lawfully, in accordance with the former Law, before the commencement date, and
- (b) is continued in the context of the controller or processor concerned after the Law comes into force.

(2) Whether any processing carried out in the context of a controller or processor before the commencement date ("**the previous processing**") is of the same kind as the processing concerned must be determined having regard to the nature, scope, context and purpose of the previous processing in comparison to the processing concerned, including whether or not the processing concerned involves the use or application of a technology, mechanism or procedure that was neither used nor applied in the previous processing.

Transitional provision for processing by public authorities based on legitimate interest.

9. Until the transition date, paragraph 4 of Schedule 2 to the Law has effect as if –

- (a) immediately after "party", a full stop were substituted for the comma, and
- (b) the words "except where the processing is in the context of the exercise or performance by a public authority of a function or task described in paragraph 5" were omitted.

Delayed effect of section 14 (right to data portability) of the Law

10. (1) Until the transition date, neither section 14 of the Law nor any corresponding provision has effect.

(2) In subsection (1), "**any corresponding provision**" means any provision of section 6 of the Law, or of any other section of the Law, so far as the provision corresponds to a right or duty in section 14 of the Law.

Reporting of personal data breaches occurring before commencement.

11. (1) A controller or processor is required to comply with a duty to report a personal data breach regardless whether the breach occurred before or after the Law comes into force.

(2) However, a controller is not required to comply with a duty to report a personal data breach unless the controller first becomes aware of the personal data breach after the Law comes into force.

(3) In this section, "**a duty to report**", in relation to any personal data breach, means a duty to give notice of the breach –

(a) imposed on a controller by any of the following provisions –

(i) section 42(2) or 43(1) of the Law, or

(ii) section 34(2) or 35(1) of the Law Enforcement Ordinance, or

(b) imposed on a processor by any of the following provisions –

(i) section 42(1) of the Law, or

(ii) section 34(1) of the Law Enforcement Ordinance.

PART III
SAVING OF CONSENTS, PROCEEDINGS AND OTHER MATTERS

Validity of consents obtained before commencement.

12. (1) This section applies to consent to the processing of personal data where –

- (a) the consent was given by the data subject before the commencement date,
- (b) the consent had effect as consent for that processing under the former Law immediately before the commencement date,
- (c) the consent was not given on the basis of false, deceptive or misleading information or conduct, knowingly or recklessly provided or perpetrated by –
 - (i) the controller,
 - (ii) the processor, or
 - (iii) any other person who sought the consent or to whom the consent was given, and
- (d) the data subject has not withdrawn the consent –
 - (i) by giving written notice to the controller, or

- (ii) by any other means provided for by the controller.

(2) Where a consent to which this section applies also meets the definition of a consent in section 10(1) and all the other requirements and conditions in section 10 of the Law for consent to be valid for the purposes of the Law, the consent has effect as consent to that processing for the purposes of the Law and the Law Enforcement Ordinance.

(3) In any other case, despite any provision to the contrary in section 10 of the Law, a consent to which this section applies must be regarded as consent to that processing for the purposes of the Law and the Law Enforcement Ordinance until the earlier of –

- (a) the data subject withdrawing the consent –
 - (i) by giving written notice to the controller, or
 - (ii) by any other means provided for by the controller, or
- (b) the occurrence of the transition date.

Prior designation and notification of Bailiwick representatives.

13. A controller is not required under section 38(2)(a) to (c) of the Law to designate a representative, notify the Authority of the name and contact details of the representative or authorise the representative to receive notices and other communications if, before the commencement date, the controller has so designated a representative, so notified the former Commissioner or so authorised the

representative.

Saving of authorisation for transfer to unauthorised jurisdictions.

14. An authorisation by the former Commissioner under paragraph 9 of Schedule 4 to the former Law for the transfer of personal data to an unauthorised jurisdiction in force immediately before the commencement date has effect as if it were an authorisation for the transfer given by the Authority under section 57(1) of the Law until the authorisation is revoked by the Authority.

Saving of proceedings, etc. under former Law.

15. (1) Any proceedings under the former Law not cancelled, withdrawn or finally determined before the commencement date –

- (a) continue to have effect,
- (b) may be cancelled, withdrawn or amended, and
- (c) may otherwise be continued, proceeded upon, completed and finally determined,

in accordance with the provisions of the former Law, as if –

- (i) the former Law had not been repealed, but
- (ii) the former Commissioner were substituted with the Authority.

(2) Subsection (3) applies to any legal proceeding (other than proceedings of the kind saved by subsection (1)), not cancelled, withdrawn or finally

determined before the commencement date –

- (a) in relation to any act or omission of the former Commissioner in the former Commissioner's official capacity or in connection with the discharge of former Commissioner's official functions, and
 - (b) to which the former Commissioner is a party.
- (3) Proceedings to which this subsection applies –
- (a) continue to have effect,
 - (b) may be cancelled, withdrawn or amended, and
 - (c) may otherwise be continued, proceeded upon, completed and finally determined,

as if the Authority were a party to those proceedings instead of the former Commissioner.

- (4) In subsection (1), "**proceedings under the former Law**" includes –
- (a) a request made under section 7 of the former Law,
 - (b) a claim for compensation made under section 13 of the former Law,

- (c) an application for rectification, blocking, erasure or destruction under section 14 of the former Law,
- (d) a request for assessment made under section 42 of the former Law,
- (e) any assessment or determination made by the former Commissioner under the former Law,
- (f) an information notice or a special information notice served under section 43 or 44 of the former Law, respectively,
- (g) an enforcement notice served under section 40 of the former Law, and
- (h) any appeal made under the former Law.

Offences under former Law.

16. (1) Where a person commits an offence under any provision of the former Law wholly or partly before the commencement date, the person may be charged and proceeded against in accordance with the provisions of the former Law, as if –

- (a) the former Law had not been repealed, but
- (b) the former Commissioner were substituted with the Authority.

(2) In section 100(1)(b)(ii)(A) of the Law, the reference to an offence under section 88(2) of the Law is deemed to include a reference to an offence under paragraph 11 of Schedule 8 to the former Law.

(3) In paragraph 10 of Schedule 8 to the Law (including that provision as applied by section 48 of the Law Enforcement Ordinance), the reference to an offence under the Law is deemed to include a reference to an offence under the former Law.

(4) In sections 43(8) and 44(9) of, and paragraph 11(1) and (2) of Schedule 6 to, the former Law to the extent that any of those provisions are saved and continued by any provision of this Ordinance, a reference to an offence under the former Law is deemed to include an offence under the Data Protection (Bailiwick of Guernsey) Law, 2017.

Other things done under former Law.

17. Unless the context requires otherwise, and subject to any provision of this Ordinance to the contrary, anything done or having effect as if done (excluding the making of any Ordinance or subordinate legislation) under or for the purposes of any provision of the former Law has effect as if done under or for the purposes of any corresponding provision of the Law or any Ordinance, Regulations or other subordinate legislation made under the Law.

PART IV
TRANSITION OF RIGHTS, RECORDS, ETC.

Rights, liabilities, records, etc.

18. (1) All assets, rights, liabilities and obligations of the former Commissioner in the former Commissioner's official capacity or arising out of the

discharge of the former Commissioner's official functions are the assets, rights, liabilities and obligations of the Authority.

(2) An agreement entered into by the former Commissioner in the former Commissioner's official capacity or in connection with the discharge of the former Commissioner's official functions has effect as if –

(a) the Authority were a party to it instead of the former Commissioner, and

(b) any reference to the former Commissioner were, in relation to anything to be done after the Law comes into force, a reference to the Authority.

(3) Any record or requirement made by, any information given to, any document deposited with, any record kept by, or any statement made to, the former Commissioner in the former Commissioner's official capacity or in connection with the discharge of the former Commissioner's official functions at any time before the commencement date is taken, on and from that time, to have been made by, given to, deposited with, kept by or made to, the Authority.

(4) Neither subsection (2) nor (3) limits subsection (1).

(5) The Commissioner must do everything necessary to give effect to subsection (1), (2) and (3), including making or amending any registration, notification or transfer requested by the Authority to give effect to those provisions.

(6) This section is subject to section 60A of the Law.

PART V
GENERAL

Revocations.

19. The Orders and Regulations specified in Schedule 1 are revoked.

Amendments to the Data Protection (Bailiwick of Guernsey) Law, 2017.

20. The Law is amended as set out in Schedule 2.

Consequential amendments to e-Privacy Ordinances.

21. The following enactments are amended as set out in Schedule 3 –

- (a) the European Communities (Implementation of Privacy Directive) (Guernsey) Ordinance, 2004^c,
- (b) the European Communities (Implementation of Council Directive on Privacy and Electronic Communications) (Alderney) Ordinance, 2009^d, and
- (c) the European Communities (Implementation of Council Directive on Privacy and Electronic Communications) (Sark) Ordinance, 2004^e.

^c Ordinance No. XXIV of 2004; as amended by Ordinance No. II of 2010; No. XIII of 2012; and No. IX of 2016.

^d Alderney Ordinance No. VIII of 2009; as amended by Alderney Ordinance No. III of 2010; and Ordinance No. XIII of 2012.

^e Sark Ordinance No. 136; as amended by Sark Ordinance No. 184; Sark Ordinance No. VI of 2015; and (Guernsey) Ordinance No. XIII of 2012.

Interpretation.

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

"**commencement date**" means the 25th May, 2018,

"**enactment**" includes –

- (a) an Act of Parliament that extends to the Bailiwick, and
- (b) a Law, an Ordinance and any subordinate legislation and includes any provision or portion of a Law, an Ordinance or any subordinate legislation,

"**the former Commissioner**" means the Data Protection Commissioner under the former Law,

"**the former Law**" –

- (a) means the Data Protection (Bailiwick of Guernsey) Law, 2001^f, and
- (b) includes –
 - (i) any Ordinance repealed by section 113(b), (c) or (d) of the Law, and

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

- (ii) any Order or Regulation revoked by section 19 of this Ordinance,

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

"**the Law Enforcement Ordinance**" means the Data Protection (Law Enforcement and Related Matters) (Bailiwick of Guernsey) Ordinance, 2018⁸,

"**official capacity**", in relation to the former Commissioner, means in the former Commissioner's capacity as, or in respect of the office of, the Data Protection Commissioner under the former Law,

"**official function**", in relation to the former Commissioner, means a function conferred or imposed on the former Commissioner under the former Law,

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

"**the transition date**" means the 25th May, 2019.

(2) A reference in this Ordinance to a provision or Part of the Law or the Law Enforcement Ordinance includes a reference to any regulations made

⁸ Ordinance No. * of 2018.

under, or any Schedule given effect by, the provision or Part of the Law or (as the case may be) the Law Enforcement Ordinance.

(3) An expression used in this Ordinance that is also used in the Law or the Law Enforcement Ordinance has the same meaning as in the Law or (as the case may require) the Law Enforcement Ordinance unless –

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

(b) the context requires otherwise.

(4) The Interpretation (Guernsey) Law, 1948^h applies to the interpretation of this Ordinance throughout the Bailiwick of Guernsey.

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

Citation.

23. This Ordinance may be cited as the Data Protection (Commencement, Amendment and Transitional) (Bailiwick of Guernsey) Ordinance, 2018.

^h Ordres en Conseil Vol. XIII, p. 355.

SCHEDULE 1

Section 19

ORDERS AND REGULATIONS REVOKED

The Data Protection (Bailiwick of Guernsey) Law, 2001 (Commencement) Order, 2002ⁱ.

The Data Protection (Credit Reference Agency) (Statement of Rights) Regulations, 2002^j.

The Data Protection (Miscellaneous Subject Access Exemptions) Order, 2002^k.

The Data Protection (Subject Access Modification) (Education) Order, 2002^l.

The Data Protection (Subject Access Modification) (Health) Order, 2002^m.

The Data Protection (Subject Access Modification) (Social Work) Order, 2002ⁿ.

The Data Protection (Processing of Sensitive Personal Data) Order, 2002^o.

The Data Protection (Further Conditions concerning Fair Processing) Order, 2002^p.

The Data Protection (Non-disclosure Exemption) Order, 2002^q.

The Data Protection (Corporate Finance Exemption) Order, 2002^r.

i G.S.I. No. 10 of 2002.

j G.S.I. No. 12 of 2002.

k G.S.I. No. 13 of 2002.

l G.S.I. No. 14 of 2002.

m G.S.I. No. 15 of 2002.

n G.S.I. No. 16 of 2002.

o G.S.I. No. 17 of 2002.

p G.S.I. No. 18 of 2002.

q G.S.I. No. 19 of 2002.

r G.S.I. No. 20 of 2002.

The Data Protection (Functions of Designated Authority) Order, 2002^s.

The Data Protection (Fees under section 19(7)) Regulations, 2002^t.

The Data Protection (Subject Access) (Fees and Miscellaneous Provisions) Regulations, 2002^u.

The Data Protection (Notification and Notification Fees) Regulations, 2002^v.

The Data Protection (Transfer in the Substantial Public Interest) Order, 2002^w.

The Data Protection (Processing of Sensitive Personal Data) (Elected Representatives) Order, 2004 (signed by M. W. Torode on the 15th December, 2004)^x.

The Data Protection (Notification and Notification Fees) (Amendment) Regulations, 2004^y.

The Data Protection (Notification and Notification Fees) (Amendment) Regulations, 2009^z.

The Data Protection (Processing of Sensitive Personal Data) (Elected Representatives) (Revocation) Order, 2009^{aa}.

The Data Protection (Notification and Notification Fees) (Revocation) Regulations, 2009^{bb}.

^s G.S.I. No. 21 of 2002.

^t G.S.I. No. 22 of 2002.

^u G.S.I. No. 23 of 2002.

^v G.S.I. No. 24 of 2002.

^w G.S.I. No. 28 of 2002.

^x G.S.I. No. 72 of 2009.

^y G.S.I. No. 73 of 2009.

^z G.S.I. No. 38 of 2009.

^{aa} G.S.I. No. 52 of 2009.

The Data Protection (Notification and Notification Fees) (Amendment) Regulations, 2010^{cc}.

The Data Protection (References to Committees of the States) (Miscellaneous Amendments) Order, 2010^{dd}.

The Data Protection (Bailiwick of Guernsey) Law, 2001 (Commencement) Order, 2010^{ee}.

The Data Protection (Crown Appointments) Order, 2010^{ff}.

The Data Protection (Processing of Personal Data) Order, 2010^{gg}.

The Data Protection (Subject Access) (Fees and Miscellaneous Provisions) (Amendment) Regulations, 2010^{hh}.

The Data Protection (Processing of Personal Data) (STSC) Order, 2012ⁱⁱ.

The Data Protection (Subject Access Exemptions) (Guernsey) Order, 2015^{jj}.

The Data Protection (Public Information Designation) (Revocation) Order, 2015^{kk}.

The Data Protection (Notification and Notification Fees) (Amendment) Regulations, 2016^{ll}.

bb G.S.I. No. 53 of 2009.

cc G.S.I. No. 7 of 2010.

dd G.S.I. No. 8 of 2010.

ee G.S.I. No. 9 of 2010.

ff G.S.I. No. 10 of 2010.

gg G.S.I. No. 51 of 2010.

hh G.S.I. No. 59 of 2010.

ii G.S.I. No. 36 of 2012.

jj G.S.I. No. 99 of 2015.

kk G.S.I. No. 100 of 2015.

The Data Protection (Processing of Sensitive Personal Data) (Ofsted) Order, 2017^{mm}.

The Data Protection (Transfer in the Substantial Public Interest) (Amendment)

Order, 2017ⁿⁿ.

ll G.S.I. No. 13 of 2016.

mm G.S.I. No. 61 of 2017.

nn G.S.I. No. 92 of 2017.

SCHEDULE 2

Section 20

AMENDMENTS TO THE DATA PROTECTION (BAILIWICK OF GUERNSEY)
LAW, 2017

Provision or part amended	Amendment
Section 7	<p>Re-number this section "7(1)".</p> <p>Immediately after the new subsection (1), insert the following subsection –</p> <p>"(2) Despite anything to the contrary in subsection (1), the keeping of a comprehensive register of criminal convictions by any person other than a competent authority (within the meaning of section 50(1) of the Law Enforcement Ordinance) is not lawful for the purposes of the data protection principle of Lawfulness, Fairness and Transparency."</p>
Section 12	<p>Immediately after subsection (3), insert –</p> <p>"(3A) Where the controller intends to further process the personal data for a purpose other than that for which the data was collected, the controller must give the data subject prior to the further processing –</p> <ul style="list-style-type: none"> (a) information on the other purpose, and (b) any relevant further information specified in Schedule 3." <p>Immediately after subsection (4), insert –</p> <p>"(5) Nothing in subsection (2), (3) or (3A) requires the controller to give the data subject any information that the data subject already has."</p>
Section 13	<p>Immediately after subsection (2), insert –</p> <p>"(2A) Where the controller intends to further process the personal data for a purpose other than that for which the controller originally processed the personal data, the controller must give the data subject prior to the further processing –</p> <ul style="list-style-type: none"> (a) information on the other purpose, and (b) any relevant further information specified in Schedule 3." <p>In subsection (4), for "or (2)", substitute ", (2) or (2A)".</p>

Provision or part amended	Amendment
Section 17	<p>In subsection (5), for "Where", substitute "Despite any provision in an e-Privacy Ordinance to the contrary, where".</p> <p>Immediately after subsection (5), insert –</p> <p style="padding-left: 40px;">"(6) In subsection (5), "e-Privacy Ordinance" means any Ordinance specified in section 104(2)(b)."</p>
Section 21(6)	For "or 13", substitute "13 or 13A".
Section 24(2)(b) and (4)(b)	Omit "who is a third party" in each place it occurs.
Section 29(3)	Immediately after "proof", insert "on the balance of probabilities".
Section 35(3)	Immediately after (" the authorised person ")", insert ", other than an employee of the controller or (as the case may be) processor,".
Section 35(4)	Omit this subsection.
Section 45(7)	For "latter", substitute "later".
Section 47(1)(a)	Immediately after "authority", insert ", other than a court or tribunal acting in its judicial capacity".
Section 49(1)	For "a staff member", substitute "an employee".
Section 52(3)(c)	For "a", substitute "more than one".
Section 57	<p>In the heading of this section, omit "specific".</p> <p>In subsection (1), immediately after "has", insert "generally or".</p>
Section 61(6)	Immediately after "proof", insert "on the balance of probabilities".
Part XI	<p>Immediately after section 60 of this Part, insert –</p> <p><u>Former Commissioner and employees deemed to be employed by the Authority.</u></p> <p style="padding-left: 40px;">60A. (1) On the commencement of this Law, subject to the provisions of Schedule 6A –</p> <p style="padding-left: 80px;">(a) the former Commissioner is deemed to have been duly appointed and employed as the Commissioner by the Authority in accordance with Schedule 6, and</p>

Provision or part amended	Amendment
	<p>(b) any other individual holding any office or position in the office of the Data Protection Commissioner immediately before the commencement of this Law is deemed to have been duly employed by the Authority in the office or position concerned in accordance with Schedule 6.</p> <p>(2) For the purposes of Schedule 6A, the individual who is the former Commissioner is deemed to have been employed by the States of Guernsey immediately before the commencement of this Law under a contract of employment containing the terms and conditions of that individual's appointment as the Data Protection Commissioner under the Data Protection (Bailiwick of Guernsey) Law, 2001.</p> <p>(3) Schedule 6A has effect.</p> <p>(4) In this section and Schedule 6A, "the former Commissioner" means the Data Protection Commissioner under Data Protection (Bailiwick of Guernsey) Law, 2001."</p>
Section 73	<p>Immediately after subsection (7), insert –</p> <p>"(7A) In determining what, if any, order to make under section 73(2) where a controller or processor has breached an operative provision, the Authority must have regard to the matters specified in section 74(2)(a) to (j)."</p>
Section 74(1)	<p>Immediately after paragraph (f), insert –</p> <p>"(fa) failure to comply with an order under section 73(2) within the time specified in the order for compliance".</p>
Part XVI	<p>Immediately after section 100, insert –</p> <p><u>Saving of international agreements.</u></p> <p>100A. Nothing in this Law affects the validity or effect of any international agreement imposing an international obligation on the Bailiwick in relation to the transfer of personal data to an unauthorised jurisdiction, to the extent that the agreement –</p> <p>(a) was concluded before the commencement of this Law, and</p> <p>(b) is consistent with the Data Protection (Bailiwick of Guernsey) Law, 2001."</p>
Section 111(1)	<p>For the definition of "adequacy decision", substitute the following definition –</p> <p>" "adequacy decision" in respect of any country, sector within</p>

Provision or part amended	Amendment
	<p>a country or international organisation –</p> <ul style="list-style-type: none"> (a) means a decision made by the European Commission that the country, sector or international organisation concerned ensures an adequate level of protection within the meaning of Article 45(2) of the GDPR, and (b) includes a finding of the European Commission under Article 31(2) of the former Directive, in force immediately before the commencement date, that the country, sector or international organisation concerned ensures an adequate level of protection within the meaning of Article 25(2) of that former Directive, unless and until the European Commission revokes the finding or decides that the country, sector or international organisation concerned does not ensure an adequate level of protection within the meaning of Article 45(2) of the GDPR,". <p>In the definition of "controller", immediately after paragraph (b), insert –</p> <p>"but</p> <ul style="list-style-type: none"> (c) excludes an employee of a controller (within the meaning of paragraph (a) or (b) of this definition), who determines the purposes and means of the processing of the personal data on behalf of the controller,". <p>In the definition of "designated jurisdiction" –</p> <ul style="list-style-type: none"> (a) in paragraph (c), for "other country within the British Islands", substitute "Crown Dependency", and (b) in paragraph (d) – <ul style="list-style-type: none"> (i) immediately after "sector", insert "(within the meaning of the GDPR)", and (ii) immediately after "country, insert "or dependency". <p>In the definition of "law enforcement purpose" –</p> <ul style="list-style-type: none"> (a) at the end of paragraph (b), omit "or", and (b) immediately after paragraph (c), insert – <p>"or</p> <ul style="list-style-type: none"> (d) exercising or performing any power or duty conferred

Provision or part amended	Amendment
	<p style="text-align: center;">or imposed on a public authority by a criminal proceeds enactment,</p> <p>In the definition of "processor", immediately after paragraph (b), insert –</p> <p style="padding-left: 40px;">"but</p> <p style="padding-left: 40px;">(c) excludes –</p> <p style="padding-left: 80px;">(i) an employee of a controller, who processes personal data on behalf of the controller, and</p> <p style="padding-left: 80px;">(ii) an employee of a processor (within the meaning of paragraph (a) or (b) of this definition), who processes personal data on behalf of the processor,".</p> <p>In the definition of "public security", immediately after "Islands", insert "or any country outside the British Islands".</p> <p>For the definition of "standard data protection clause", substitute the following definition –</p> <p style="padding-left: 40px;">" "standard data protection clauses" –</p> <p style="padding-left: 80px;">(a) means standard contractual clauses for data protection</p> <p style="padding-left: 120px;">(i) approved or adopted by the European Commission for the purposes of Article 28 of the GDPR, or</p> <p style="padding-left: 120px;">(ii) approved by the Authority for the purposes of this Law, and</p> <p style="padding-left: 80px;">(b) includes standard contractual clauses that the European Commission decided under Article 26(4) of the former Directive offer sufficient safeguards for the purposes of Article 26(2) of that Directive, unless and until the European Commission revokes that decision or otherwise determines not to approve or adopt those clauses as standard data protection clauses for the purposes of Article 28 of the GDPR,".</p> <p>Insert in the appropriate alphabetical order, the following definitions–</p> <p style="padding-left: 40px;">" "criminal proceeds enactment" means –</p> <p style="padding-left: 80px;">(a) any of the following enactments, including any</p>

Provision or part amended	Amendment
	<p>Ordinance or subordinate legislation made under any of them –</p> <ul style="list-style-type: none"> (i) the Criminal Justice (Proceeds of Crime) (Bailiwick of Guernsey) Law, 1999, (ii) the Drug Trafficking (Bailiwick of Guernsey) Law, 2000, (iii) the Terrorism and Crime (Bailiwick of Guernsey) Law, 2002, (iv) the Criminal Justice (Fraud Investigation) (Bailiwick of Guernsey) Law, 1991, (v) the Criminal Justice (International Cooperation) (Bailiwick of Guernsey) Law, 2001, (vi) the Forfeiture of Money etc. in Civil Proceedings (Bailiwick of Guernsey) Law, 2007, (vii) the Disclosure (Bailiwick of Guernsey) Law, 2007, (viii) the Beneficial Ownership of Legal Persons (Guernsey) Law, 2017, or (ix) the Beneficial Ownership of Legal Persons (Alderney) Law, 2017, or <p>(b) any enactment, in any country outside the Bailiwick, that is similar or comparable in purpose or effect to an enactment mentioned in paragraph (a),"</p> <p>" "employee" includes a servant within the meaning of Schedule 1," and</p> <p>" "tribunal" means an office-holder or a body of persons, other than a court, that judges, adjudicates on or otherwise determines claims, disputes or other contentious matters following legal proceedings,".</p>
Section 111	Immediately after subsection (1), insert the following subsection – “(1A) The Committee may by regulations amend the definition of "criminal proceeds enactment" in subsection (1).”.
Schedule 2	Immediately after paragraph 13, insert the following paragraph – "13A. The processing is necessary for a law enforcement purpose.”.
Paragraphs 3 and 19 of	Omit "who is a third party" in each place it occurs.

Provision or part amended	Amendment
Schedule 2	
Paragraph 1(5) of Schedule 6	For "five years or any shorter period that", substitute "not less than four, and not more than five, years as".
The Schedules	<p>Immediately after Schedule 6, insert the following schedule –</p> <p style="text-align: center;">"SCHEDULE 6A EFFECT OF TRANSFER ON CONTRACTS OF EMPLOYMENT, ETC. Section 60A</p> <p>1. <u>Effect of deemed employment by Authority on contract of employment.</u></p> <p>(1) Subject to subparagraph (4), the deemed employment of an individual under section 60A(1) does not terminate the contract of employment of the former Commissioner or any other individual employed by the States of Guernsey in the office of the Data Protection Commissioner in force immediately before the commencement of this Law; on the commencement of this Law, any such contract has effect as if originally made between the individual so employed and the Authority.</p> <p>(2) Without prejudice to subparagraph (1), but subject to subparagraph (4), on the commencement of this Law –</p> <p>(a) all the rights, powers, duties and liabilities of the States of Guernsey under or in connection with any contract of employment described in subparagraph (1) are transferred by virtue of this Schedule to the Authority, and</p> <p>(b) anything done before the commencement of this Law by or in relation to the States of Guernsey in respect of that contract or an individual employed under that contract is deemed to have been done by or in relation to the Authority.</p> <p>(3) Subparagraph (2) does not transfer or otherwise affect the liability of any person to be prosecuted for, convicted of and sentenced for any offence.</p> <p>(4) If, within the period of 3 months after the commencement of this Law, the employee gives the Authority written notice that the employee objects to becoming employed by the Authority, upon the Authority's receipt of the notice –</p>

Provision or part amended	Amendment
	<p>(a) the employee's deemed employment by the Authority is deemed to be terminated,</p> <p>(b) the employee is deemed to revert to being employed by the States of Guernsey, instead of the Authority, and</p> <p>(c) the employee must not be treated for any purpose as having been dismissed by either the Authority or the States of Guernsey.</p> <p>(5) Subparagraphs (1) and (4) are without prejudice to any right of an employee (arising apart from subparagraph (4)) to terminate the employee's contract of employment without notice if a substantial change is made in the employee's working conditions to the employee's detriment; but no such right arises by reason only that, under those subparagraphs, the identity of the employer changes unless the employee shows that, in all the circumstances, the change is a significant change and is to the employee's detriment.</p> <p>2. <u>Effect of deemed employment by the Authority on collective agreements.</u> Where immediately before the commencement of this Law there exists a collective agreement made by or on behalf of the States of Guernsey with a trade union recognised by the States of Guernsey in respect of any employee whose contract of employment is preserved by paragraph 1(1), then on and after the commencement of this Law –</p> <p>(a) that agreement, in its application in relation to the employee, has effect as if made by or on behalf of the Authority with that trade union; and accordingly anything done under or in connection with it in its application as aforesaid by or in relation to the States of Guernsey before the commencement of this Law is deemed to have been done by or in relation to the Authority, and</p> <p>(b) any order made in respect of that agreement, in its application in relation to the employee, has effect as if the Authority were a party to the agreement.</p> <p>3. <u>Non-application of paragraphs 1 and 2 to occupational pension schemes.</u></p> <p>(1) Neither paragraph 1 nor 2 applies –</p>

Provision or part amended	Amendment
	<p>(a) to any part of a contract of employment or collective agreement that relates to an occupational pension scheme of a description set out in section 157C(1)(e) of the Income Tax (Guernsey) Law, 1975, or</p> <p>(b) to any rights, powers, duties or liabilities under or in connection with any such contract or subsisting by virtue of any such agreement and relating to such a scheme or otherwise arising in connection with a person's employment and relating to such a scheme.</p> <p>(2) For the purposes of subparagraphs (1) and (3), any provisions of an occupational pension scheme which do not relate to benefits for old age, invalidity or survivors must not be treated as part of the scheme.</p> <p>(3) An employee whose contract of employment is transferred by virtue of paragraph 1(1) is not entitled to bring a claim against either the Authority or the States of Guernsey for –</p> <p>(a) breach of contract, or</p> <p>(b) constructive unfair dismissal under Part II of the Employment Protection (Guernsey) Law, 1998, arising out of a loss or reduction in the employee's rights under an occupational pension scheme described in subparagraph (1)(a) in consequence of the transfer, save insofar as the alleged breach of contract or dismissal (as the case may be) occurred before the commencement of this Law.</p> <p>4. <u>Dismissal of employee because of transfer of employment contract.</u></p> <p>(1) If any individual deemed to be employed by the Authority under section 60A(1) is dismissed at any time before or after the commencement of this Law, the dismissal of the employee must be regarded for the purposes of Part II of the Employment Protection (Guernsey) Law, 1998 as having been unfair if the reason for the dismissal (or, if more than one, the principal reason) was the transfer of the employment contract under paragraph 1(1) and (2) or a reason connected with it; and the provisions of that Law apply accordingly.</p> <p>(2) Subparagraph (1) is subject to the provisions of the Employment Protection (Guernsey) Law, 1998.</p> <p>5. <u>The Law to prevail in case of conflict.</u></p>

Provision or part amended	Amendment
	<p>If there is any conflict between the terms and conditions of an employment contract having effect in accordance with this Schedule on the one hand, and a provision of this Law or any Ordinance or subordinate legislation made under this Law on the other hand, the Law, Ordinance or (as the case may be) subordinate legislation prevails.</p> <p>6. <u>Interpretation of this Schedule.</u> In this Schedule, unless the context requires otherwise –</p> <p>"collective agreement" means any agreement or arrangement made by or on behalf of a trade union and an employer or employers' association and relating to any of the following matters –</p> <ul style="list-style-type: none"> (a) terms and conditions of employment, or the physical conditions in which employees are required to work, (b) engagement or non-engagement, or termination or suspension of employment or the duties of employment, of any employee, (c) allocation of work or the duties of employment as between employees or groups of employees, (d) matters of discipline, (e) the membership or non-membership of trade unions on the part of an employee, (f) facilities for officials of trade unions, and (g) machinery for negotiation or consultation, and other procedures, relating to any of the foregoing matters, including the recognition by employers or employers' associations of the right of a trade union to represent workers in any such negotiation or consultation or in the carrying out of any such procedures, <p>"collective bargaining" means negotiations relating to or connected with any of the matters specified in the definition of the expression "collective agreement",</p> <p>"contract" includes any agreement, transaction, arrangement or understanding, whether or not conditional or in writing and governed by the law of the Bailiwick or any part thereof,</p> <p>"contract of employment" means any agreement,</p>

Provision or part amended	Amendment
	<p>whether express or implied and whether written or oral, between an employee and the employee's employer, determining the terms and conditions of the employment of the employee,</p> <p>"employee" means an individual who has entered into or who works under a contract of service or apprenticeship (whether express or implied and whether written or oral), but does not include an individual engaged under a contract for services or on a consultancy or secondment basis, and cognate expressions shall be construed accordingly,</p> <p>"employers' association" has the meaning given by section 34 of the Employment Protection (Guernsey) Law, 1998,</p> <p>"independent trade union" has the meaning given by section 34 of the Employment Protection (Guernsey) Law, 1998,</p> <p>"liability" includes a debt, a duty and an obligation of any description (whether present or future, actual, contingent or prospective),</p> <p>"occupational pension scheme" means any scheme or arrangement which is comprised in one or more instruments or agreements and which has, or is capable of having, effect in relation to one or more descriptions or categories of employments so as to provide benefits, in the form of pensions or otherwise, payable on termination of service or on death or retirement, to or in respect of earners with qualifying service in an employment of any such description or category,</p> <p>"recognised", in relation to a trade union, means recognised to any extent by an employer, or two or more associated employers (within the meaning of section 34 of the Employment Protection (Guernsey) Law, 1998), for the purpose of collective bargaining,</p> <p>"trade union" has the meaning given by section 34 of the Employment Protection (Guernsey) Law, 1998, and</p> <p>"working conditions" includes terms and conditions of employment and physical working conditions."</p>
Paragraph 19 of Schedule 8	<p>Renumber this paragraph "19(1)".</p> <p>In the new subparagraph (1)(b), for "paragraph", substitute "item".</p>

Provision or part amended	Amendment																
	<p>Immediately after the new subparagraph (1), insert the following subparagraph –</p> <p>"(2) The modifications, exceptions and exemptions provided for by regulations under subparagraph (1) may be in addition to, or in substitution of, any modifications, exceptions or exemptions specified in this Schedule before those regulations are made."</p>																
<p>Paragraph 20 of Schedule 8</p>	<p>In the definition of "a provision of Part III", for paragraph (b), substitute –</p> <p style="padding-left: 40px;">"(b) any provision of section 6 of this Law corresponding to a right or duty in Part III of this Law,".</p> <p>In the definition of "designated provision", for paragraphs (b) and (c), substitute –</p> <p style="padding-left: 40px;">"(b) any provision of section 6 of this Law corresponding to a right or duty in Part III of this Law, or</p> <p style="padding-left: 40px;">(c) section 43 of this Law,".</p>																
<p>Schedule 10</p>	<p>In that table in this schedule, insert each of the following rows in the appropriate alphabetical order –</p> <table border="1" data-bbox="432 1099 1350 1424"> <tbody> <tr> <td data-bbox="432 1099 890 1137">Approval date</td> <td data-bbox="890 1099 1350 1137">Section 108(8)</td> </tr> <tr> <td data-bbox="432 1137 890 1176">The Constable</td> <td data-bbox="890 1137 1350 1176">Paragraph 3(3) of Schedule 1</td> </tr> <tr> <td data-bbox="432 1176 890 1214">Criminal proceeds enactment</td> <td data-bbox="890 1176 1350 1214">Section 111(1)</td> </tr> <tr> <td data-bbox="432 1214 890 1252">The former Commissioner</td> <td data-bbox="890 1214 1350 1252">Section 60A(4)</td> </tr> <tr> <td data-bbox="432 1252 890 1290">Employee</td> <td data-bbox="890 1252 1350 1290">Section 111(1)</td> </tr> <tr> <td data-bbox="432 1290 890 1328">e-Privacy Ordinance</td> <td data-bbox="890 1290 1350 1328">Section 17(6)</td> </tr> <tr> <td data-bbox="432 1328 890 1366">Relevant date</td> <td data-bbox="890 1328 1350 1366">Section 109(8)</td> </tr> <tr> <td data-bbox="432 1366 890 1424">Tribunal</td> <td data-bbox="890 1366 1350 1424">Section 111(1)</td> </tr> </tbody> </table>	Approval date	Section 108(8)	The Constable	Paragraph 3(3) of Schedule 1	Criminal proceeds enactment	Section 111(1)	The former Commissioner	Section 60A(4)	Employee	Section 111(1)	e-Privacy Ordinance	Section 17(6)	Relevant date	Section 109(8)	Tribunal	Section 111(1)
Approval date	Section 108(8)																
The Constable	Paragraph 3(3) of Schedule 1																
Criminal proceeds enactment	Section 111(1)																
The former Commissioner	Section 60A(4)																
Employee	Section 111(1)																
e-Privacy Ordinance	Section 17(6)																
Relevant date	Section 109(8)																
Tribunal	Section 111(1)																

SCHEDULE 3

Section 21

CONSEQUENTIAL AMENDMENTS TO E-PRIVACY ORDINANCES

Amendments to the European Communities (Implementation of Privacy Directive) (Guernsey) Ordinance, 2004

Provision or part amended	Amendment
Section 2	For "Data Protection (Bailiwick of Guernsey) Law, 2001", substitute "Data Protection (Bailiwick of Guernsey) Law, 2017, including any Ordinance or regulation made under it,".
Section 24	Immediately after subsection (7), insert – <p style="margin-left: 40px;">"(7A) The Royal Court's power under this section to make rules includes power to vary or revoke any such rules by subsequent rules.</p> <p style="margin-left: 40px;">(7B) Any rules made by the Royal Court under this section may–</p> <p style="margin-left: 80px;">(a) make different provision for different cases, and</p> <p style="margin-left: 80px;">(b) make such supplemental, incidental, consequential or transitional provision or savings as the Royal Court considers appropriate."</p>
Section 24(8)	In paragraph (a) – <p style="margin-left: 20px;">(a) For "(8), (9), (10), (11), (12) and (13) of section 28 of", substitute "paragraph 18(9), (10) and (11) of Schedule 8 to", and</p> <p style="margin-left: 20px;">(b) for "section 28 of that Law", substitute "paragraph 18 of Schedule 8 to that Law; and for the purposes of this subsection "Royal Court" has the meaning given by section 111(1) of that Law".</p> <p>In paragraph (b), for "58", substitute "100A".</p> <p>Repeal paragraph (c).</p>
Section 27	For subsection (1), substitute – <p style="margin-left: 40px;">"(1) The provisions of the Data Protection Law specified in the left-hand column of Schedule 1 are extended for the purposes of this Ordinance and, for those purposes have effect subject to the modifications set out in the right-hand column of that schedule."</p> <p>In subsection (2), for "Commissioner", substitute "Authority".</p>
Section 28	In paragraph (b), for "Authority", substitute "Guernsey Competition and

Provision or part amended	Amendment				
	<p>Regulatory Authority".</p> <p>For "Data Protection Commissioner" or "Commissioner" in each place it occurs (including the heading of this section), substitute "Data Protection Authority".</p> <p>For "his" or "he" in each place either expression occurs (including the heading of this section), substitute "its" and "it" respectively.</p>				
Section 29	<p>For "Authority", substitute "Guernsey Competition and Regulatory Authority".</p> <p>For "Data Protection Commissioner" or "Commissioner" in each place it occurs (including the heading of this section), substitute "Data Protection Authority".</p> <p>For "his", substitute "its".</p>				
Section 31(1)	<p>Repeal the definition of "the Commissioner".</p> <p>In the definition of "Data Protection Law", for "2001", substitute "2017".</p> <p>In the appropriate alphabetical order, insert – " Data Protection Authority" means the Data Protection Authority established by the Data Protection Law,".</p>				
Schedule 1	<p>Repeal this schedule and substitute in its place –</p> <p style="text-align: center;">"SCHEDULE 1 <u>Section 27</u> EXTENSION OF PROVISIONS OF THE DATA PROTECTION (BAILIWICK OF GUERNSEY) LAW, 2017 SUBJECT TO MODIFICATIONS, FOR THE PURPOSES OF THIS ORDINANCE</p> <table border="1" data-bbox="408 1534 1353 1964"> <thead> <tr> <th data-bbox="408 1534 788 1655">Provision of the Data Protection (Bailiwick of Guernsey) Law, 2017</th> <th data-bbox="796 1534 1353 1655">Modifications</th> </tr> </thead> <tbody> <tr> <td data-bbox="408 1655 788 1964">Section 69</td> <td data-bbox="796 1655 1353 1964"> <p>For "controller or processor" in each place it occurs, substitute "person".</p> <p>For "operative provision" in each place it occurs, substitute "e-Privacy requirement".</p> <p>In subsection (1), for "this Law",</p> </td> </tr> </tbody> </table>	Provision of the Data Protection (Bailiwick of Guernsey) Law, 2017	Modifications	Section 69	<p>For "controller or processor" in each place it occurs, substitute "person".</p> <p>For "operative provision" in each place it occurs, substitute "e-Privacy requirement".</p> <p>In subsection (1), for "this Law",</p>
Provision of the Data Protection (Bailiwick of Guernsey) Law, 2017	Modifications				
Section 69	<p>For "controller or processor" in each place it occurs, substitute "person".</p> <p>For "operative provision" in each place it occurs, substitute "e-Privacy requirement".</p> <p>In subsection (1), for "this Law",</p>				

Provision or part amended	Amendment	
		substitute "the 2004 Ordinance".
	Section 70	-
	Section 72	<p>Omit paragraph (a) of subsection (1).</p> <p>For "controller or processor" in each place it occurs, substitute "person".</p> <p>For "operative provision" in each place it occurs, substitute "e-Privacy requirement".</p>
	Section 73(1)	For "operative provision", substitute "e-Privacy requirement".
	Section 73(2)(a), (e)(i) and (ii)	<p>For "operative provision", substitute "e-Privacy requirement".</p> <p>For "this Law", substitute "the 2004 Ordinance".</p>
	Section 73(4), (5), (6), (7A) and (8)	-
	Section 74(2)(a) to (j)	Extended only for the purposes of section 73(7A), as extended above.
	Sections 76(1) to (5), 77, 81, 84, 88(1), (2)(d) and (e) and items (i) to (iv) and (3), 89, 90	-
	Section 91	Immediately after "this Law" in each place it occurs, insert "or the 2004 Ordinance".
	Sections 92, 93, 94 and 95	-
	Section 111 (any definition necessary to give meaning to any of the provisions of the Data Protection (Bailiwick of Guernsey) Law, 2017 extended above)	<p>Extended to the extent necessary to give meaning to those provisions extended above. This extension is subject to the following modifications –</p> <p>(a) for "controller or processor" in each place it occurs, substitute "person",</p> <p>(b) for "operative provision" in each place it occurs, substitute "e-Privacy requirement",</p>

Provision or part amended	Amendment	
		<p>(c) in the definition of "breach determination", omit "section 71(1)(a)",</p> <p>(d) for the definition of "this Law", substitute – " this Law" means this Law as extended for the purposes of the 2004 Ordinance and includes any Ordinance or regulations made under or for the purposes of this Law as so extended,"</p> <p>(e) in the definition of "privileged items", in paragraph (b), for "this Law", substitute "this Law or the 2004 Ordinance", and</p> <p>(f) insert in the appropriate alphabetical order the following definitions – " the 2004 Ordinance" means the European Communities (Implementation of Privacy Directive) (Guernsey) Ordinance, 2004", and " e-Privacy requirement" means any requirement of the 2004 Ordinance,".</p>
	Schedule 7	<p>For "controller or processor" in each place it occurs, substitute "person".</p> <p>For "operative provision" in each place it occurs, substitute "e-Privacy requirement".</p>
		<p>In paragraph 1(2) –</p> <p>(a) in item (a), omit "investigate a complaint," and</p> <p>(b) in item (b), omit "investigation or".".</p>

Amendments to the European Communities (Implementation of Council Directive on Privacy and Electronic Communications) (Alderney) Ordinance, 2009

Provision or part amended	Amendment
Section 2	For "Data Protection (Bailiwick of Guernsey) Law, 2001", substitute "Data Protection (Bailiwick of Guernsey) Law, 2017, including any Ordinance or regulation made under it,".
Section 24	Immediately after subsection (7), insert – <p align="center">"(7A) The Royal Court's power under this section to make rules includes power to vary or revoke any such rules by subsequent rules.</p> <p align="center">(7B) Any rules made by the Royal Court under this section may–</p> <p align="center">(a) make different provision for different cases, and</p> <p align="center">(b) make such supplemental, incidental, consequential or transitional provision or savings as the Royal Court considers appropriate."</p>
Section 24(8)	In paragraph (a) – <p>(a) For "(8), (9), (10), (11), (12) and (13) of section 28 of", substitute "paragraph 18(9), (10) and (11) of Schedule 8 to", and</p> <p>(b) for "section 28 of that Law", substitute "paragraph 18 of Schedule 8 to that Law; and for the purposes of this subsection "Royal Court" has the meaning given by section 111(1) of that Law".</p> <p>In paragraph (b), for "58", substitute "100A".</p> <p>Repeal paragraph (c).</p>
Section 27	For subsection (1), substitute – <p align="center">"(1) The provisions of the Data Protection Law specified in the left-hand column of Schedule 1 are extended for the purposes of this Ordinance and, for those purposes have effect subject to the modifications set out in the right-hand column of that schedule."</p> <p>In subsection (2), for "Commissioner", substitute "Authority".</p>
Section 28	In paragraph (b), for "Authority", substitute "Guernsey Competition and Regulatory Authority". <p>For "Data Protection Commissioner" or "Commissioner" in each place it occurs (including the heading of this section), substitute "Data Protection Authority".</p>

Provision or part amended	Amendment								
	For "his" or "he" in each place either expression occurs (including the heading of this section), substitute "its" and "it" respectively.								
Section 29	<p>For "Authority", substitute "Guernsey Competition and Regulatory Authority".</p> <p>For "Data Protection Commissioner" or "Commissioner" in each place it occurs (including the heading of this section), substitute "Data Protection Authority".</p> <p>For "his", substitute "its".</p>								
Section 31(1)	<p>Repeal the definition of "the Commissioner".</p> <p>In the definition of "Data Protection Law", for "2001", substitute "2017".</p> <p>In the appropriate alphabetical order, insert – " "Data Protection Authority" means the Data Protection Authority established by the Data Protection Law,".</p>								
Schedule 1	<p>Repeal this schedule and substitute in its place –</p> <p style="text-align: center;">"SCHEDULE 1 <u>Section 27</u> EXTENSION OF PROVISIONS OF THE DATA PROTECTION (BAILIWICK OF GUERNSEY) LAW, 2017 SUBJECT TO MODIFICATIONS, FOR THE PURPOSES OF THIS ORDINANCE</p> <table border="1" data-bbox="405 1339 1351 1937"> <thead> <tr> <th data-bbox="405 1339 783 1460">Provision of the Data Protection (Bailiwick of Guernsey) Law, 2017</th> <th data-bbox="783 1339 1351 1460">Modifications</th> </tr> </thead> <tbody> <tr> <td data-bbox="405 1460 783 1816">Section 69</td> <td data-bbox="783 1460 1351 1816"> <p>For "controller or processor" in each place it occurs, substitute "person".</p> <p>For "operative provision" in each place it occurs, substitute "e-Privacy requirement".</p> <p>In subsection (1), for "this Law", substitute "the 2009 Ordinance".</p> </td> </tr> <tr> <td data-bbox="405 1816 783 1854">Section 70</td> <td data-bbox="783 1816 1351 1854">-</td> </tr> <tr> <td data-bbox="405 1854 783 1937">Section 72</td> <td data-bbox="783 1854 1351 1937">Omit paragraph (a) of subsection (1).</td> </tr> </tbody> </table>	Provision of the Data Protection (Bailiwick of Guernsey) Law, 2017	Modifications	Section 69	<p>For "controller or processor" in each place it occurs, substitute "person".</p> <p>For "operative provision" in each place it occurs, substitute "e-Privacy requirement".</p> <p>In subsection (1), for "this Law", substitute "the 2009 Ordinance".</p>	Section 70	-	Section 72	Omit paragraph (a) of subsection (1).
Provision of the Data Protection (Bailiwick of Guernsey) Law, 2017	Modifications								
Section 69	<p>For "controller or processor" in each place it occurs, substitute "person".</p> <p>For "operative provision" in each place it occurs, substitute "e-Privacy requirement".</p> <p>In subsection (1), for "this Law", substitute "the 2009 Ordinance".</p>								
Section 70	-								
Section 72	Omit paragraph (a) of subsection (1).								

Provision or part amended	Amendment	
		<p>For "controller or processor" in each place it occurs, substitute "person".</p> <p>For "operative provision" in each place it occurs, substitute "e-Privacy requirement".</p>
	Section 73(1)	For "operative provision", substitute "e-Privacy requirement".
	Section 73(2)(a), (e)(i) and (ii)	<p>For "operative provision", substitute "e-Privacy requirement".</p> <p>For "this Law", substitute "the 2009 Ordinance".</p>
	Section 73(4), (5), (6), (7A) and (8)	-
	Section 74(2)(a) to (j)	Extended only for the purposes of section 73(7A), as extended above.
	Sections 76(1) to (5), 77, 81, 84, 88(1), (2)(d) and (e) and items (i) to (iv) and (3), 89, 90	-
	Section 91	Immediately after "this Law" in each place it occurs, insert "or the 2009 Ordinance".
	Sections 92, 93, 94 and 95	-
	Section 111 (any definition necessary to give meaning to any of the provisions of the Data Protection (Bailiwick of Guernsey) Law, 2017 extended above)	<p>Extended to the extent necessary to give meaning to those provisions extended above. This extension is subject to the following modifications –</p> <p>(a) for "controller or processor" in each place it occurs, substitute "person",</p> <p>(b) for "operative provision" in each place it occurs, substitute "e-Privacy requirement",</p> <p>(c) in the definition of "breach determination", omit "section 71(1)(a)",</p> <p>(d) for the definition of "this Law",</p>

Provision or part amended	Amendment	
		<p>substitute –</p> <p>" this Law" means this Law as extended for the purposes of the 2009 Ordinance and includes any Ordinance or regulations made under or for the purposes of this Law as so extended,"</p> <p>(e) in the definition of "privileged items", in paragraph (b), for "this Law", substitute "this Law or the 2009 Ordinance", and</p> <p>(f) insert in the appropriate alphabetical order the following definitions –</p> <p>" the 2009 Ordinance" means the European Communities (Implementation of Council Directive on Privacy and Electronic Communications) (Alderney) Ordinance, 2009," and</p> <p>" e-Privacy requirement" means any requirement of the 2009 Ordinance,".</p>
	Schedule 7	<p>For "controller or processor" in each place it occurs, substitute "person".</p> <p>For "operative provision" in each place it occurs, substitute "e-Privacy requirement".</p>
		<p>In paragraph 1(2) –</p> <p>(a) in item (a), omit "investigate a complaint," and</p> <p>(b) in item (b), omit "investigation or".".</p>

Amendments to the European Communities (Implementation of Council Directive on Privacy and Electronic Communications) (Sark) Ordinance, 2004

Provision or part amended	Amendment
Section 2	For "Data Protection (Bailiwick of Guernsey) Law, 2001", substitute "Data Protection (Bailiwick of Guernsey) Law, 2017, including any Ordinance or regulation made under it".
Section 24	<p>Immediately after subsection (7), insert –</p> <p style="padding-left: 40px;">"(7A) The Royal Court's power under this section to make rules includes power to vary or revoke any such rules by subsequent rules.</p> <p style="padding-left: 40px;">(7B) Any rules made by the Royal Court under this section may–</p> <p style="padding-left: 80px;">(a) make different provision for different cases, and</p> <p style="padding-left: 80px;">(b) make such supplemental, incidental, consequential or transitional provision or savings as the Royal Court considers appropriate."</p>
Section 24(8)	<p>In paragraph (a) –</p> <p>(a) For "(8), (9), (10), (11), (12) and (13) of section 28 of", substitute "paragraph 18(9), (10) and (11) of Schedule 8 to", and</p> <p>(b) for "section 28 of that Law", substitute "paragraph 18 of Schedule 8 to that Law; and for the purposes of this subsection "Royal Court" has the meaning given by section 111(1) of that Law".</p> <p>In paragraph (b), referring to section 58 of the Data Protection Law, for "58", substitute "100A".</p> <p>Repeal paragraph (c) (mistakenly numbered as paragraph (b)), referring to section 66 of the Data Protection Law.</p>
Section 27	<p>For subsection (1), substitute –</p> <p style="padding-left: 40px;">"(1) The provisions of the Data Protection Law specified in the left-hand column of Schedule 1 are extended for the purposes of this Ordinance and, for those purposes have effect subject to the modifications set out in the right-hand column of that schedule."</p> <p>In subsection (2), for "Commissioner", substitute "Authority".</p>
Section 28	<p>In paragraph (b), for "Authority", substitute "Guernsey Competition and Regulatory Authority".</p> <p>For "Data Protection Commissioner" or "Commissioner" in each place it occurs (including the heading of this section), substitute "Data Protection Authority".</p>

Provision or part amended	Amendment								
	For "his" or "he" in each place either expression occurs (including the heading of this section), substitute "its" and "it" respectively.								
Section 29	<p>For "Authority", substitute "Guernsey Competition and Regulatory Authority".</p> <p>For "Data Protection Commissioner" or "Commissioner" in each place it occurs (including the heading of this section), substitute "Data Protection Authority".</p> <p>For "his", substitute "its".</p>								
Section 31(1)	<p>Repeal the definition of "the Commissioner".</p> <p>In the definition of "Data Protection Law", for "2001", substitute "2017".</p> <p>In the appropriate alphabetical order, insert – " "Data Protection Authority" means the Data Protection Authority established by the Data Protection Law,".</p>								
Schedule 1	<p>Repeal this schedule and substitute in its place –</p> <p style="text-align: center;">"SCHEDULE 1 <u>Section 27</u> EXTENSION OF PROVISIONS OF THE DATA PROTECTION (BAILIWICK OF GUERNSEY) LAW, 2017 SUBJECT TO MODIFICATIONS, FOR THE PURPOSES OF THIS ORDINANCE</p> <table border="1" data-bbox="405 1375 1350 1928"> <thead> <tr> <th data-bbox="405 1375 778 1494">Provision of the Data Protection (Bailiwick of Guernsey) Law, 2017</th> <th data-bbox="778 1375 1350 1494">Modifications</th> </tr> </thead> <tbody> <tr> <td data-bbox="405 1494 778 1854">Section 69</td> <td data-bbox="778 1494 1350 1854"> <p>For "controller or processor" in each place it occurs, substitute "person".</p> <p>For "operative provision" in each place it occurs, substitute "e-Privacy requirement".</p> <p>In subsection (1), for "this Law", substitute "the 2004 Ordinance".</p> </td> </tr> <tr> <td data-bbox="405 1854 778 1895">Section 70</td> <td data-bbox="778 1854 1350 1895">-</td> </tr> <tr> <td data-bbox="405 1895 778 1928">Section 72</td> <td data-bbox="778 1895 1350 1928">Omit paragraph (a) of subsection (1).</td> </tr> </tbody> </table>	Provision of the Data Protection (Bailiwick of Guernsey) Law, 2017	Modifications	Section 69	<p>For "controller or processor" in each place it occurs, substitute "person".</p> <p>For "operative provision" in each place it occurs, substitute "e-Privacy requirement".</p> <p>In subsection (1), for "this Law", substitute "the 2004 Ordinance".</p>	Section 70	-	Section 72	Omit paragraph (a) of subsection (1).
Provision of the Data Protection (Bailiwick of Guernsey) Law, 2017	Modifications								
Section 69	<p>For "controller or processor" in each place it occurs, substitute "person".</p> <p>For "operative provision" in each place it occurs, substitute "e-Privacy requirement".</p> <p>In subsection (1), for "this Law", substitute "the 2004 Ordinance".</p>								
Section 70	-								
Section 72	Omit paragraph (a) of subsection (1).								

Provision or part amended	Amendment	
		<p>For "controller or processor" in each place it occurs, substitute "person".</p> <p>For "operative provision" in each place it occurs, substitute "e-Privacy requirement".</p>
	Section 73(1)	For "operative provision", substitute "e-Privacy requirement".
	Section 73(2)(a), (e)(i) and (ii)	<p>For "operative provision", substitute "e-Privacy requirement".</p> <p>For "this Law", substitute "the 2004 Ordinance".</p>
	Section 73(4), (5), (6), (7A) and (8)	-
	Section 74(2)(a) to (j)	Extended only for the purposes of section 73(7A), as extended above.
	Sections 76(1) to (5), 77, 81, 84, 88(1), (2)(d) and (e) and items (i) to (iv) and (3), 89, 90	-
	Section 91	Immediately after "this Law" in each place it occurs, insert "or the 2004 Ordinance".
	Sections 92, 93, 94 and 95	-
	Section 111 (any definition necessary to give meaning to any of the provisions of the Data Protection (Bailiwick of Guernsey) Law, 2017 extended above)	<p>Extended to the extent necessary to give meaning to those provisions extended above. This extension is subject to the following modifications –</p> <p>(a) for "controller or processor" in each place it occurs, substitute "person",</p> <p>(b) for "operative provision" in each place it occurs, substitute "e-Privacy requirement",</p> <p>(c) in the definition of "breach determination", omit "section 71(1)(a)",</p>

Provision or part amended	Amendment	
		<p>(d) for the definition of "this Law", substitute – " "this Law" means this Law as extended for the purposes of the 2004 Ordinance and includes any Ordinance or regulations made under or for the purposes of this Law as so extended,"</p> <p>(e) in the definition of "privileged items", in paragraph (b), for "this Law", substitute "this Law or the 2004 Ordinance", and</p> <p>(f) insert in the appropriate alphabetical order the following definitions – " "the 2004 Ordinance" means the European Communities (Implementation of Council Directive on Privacy and Electronic Communications) (Sark) Ordinance, 2004," and " "e-Privacy requirement" means any requirement of the 2004 Ordinance,".</p>
	Schedule 7	<p>For "controller or processor" in each place it occurs, substitute "person".</p> <p>For "operative provision" in each place it occurs, substitute "e-Privacy requirement".</p>
		<p>In paragraph 1(2) – (a) in item (a), omit "investigate a complaint," and (b) in item (b), omit "investigation or".".</p>

THE DATA PROTECTION (LAW ENFORCEMENT AND RELATED MATTERS) (BAILIWICK OF GUERNSEY) ORDINANCE, 2018

The States are asked to decide:-

Whether they are of the opinion to approve the draft Ordinance entitled "The Data Protection (Law Enforcement and Related Matters) (Bailiwick of Guernsey) Ordinance, 2018", and to direct that the same shall have effect as an Ordinance of the States.

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

EXPLANATORY MEMORANDUM

This Ordinance is made under the Data Protection (Bailiwick of Guernsey) Law, 2017 ("**the Law**"). It seeks to implement provisions equivalent to the EU Law Enforcement Directive (Directive (EU) 2016/680), with adaptations, exceptions and exemptions tailored to the needs of the Bailiwick of Guernsey.

**PART I
PRELIMINARY**

This Part sets out the object of this Ordinance and provides that this Ordinance applies to the processing of personal data in the context of a competent authority for a law enforcement purpose. It also applies certain parts and provisions of the Law to such processing, subject to modifications set out in Schedule 1 to this Ordinance.

Generally, this Ordinance sets out duties and rights pertaining to the processing of personal data for a law enforcement purpose that are different from the duties and rights set out in the Law for other kinds of processing. But this Ordinance applies provisions in the Law relating to enforcement (such as those relating to the Data Protection Authority and its functions and powers) and administration (such as duties of controllers and processors to register with the Authority, pay prescribed levies, keep prescribed records and make prescribed information returns).

**PART II
DUTIES AND PRINCIPLES OF PROCESSING**

This Part requires controllers to comply with the data protection principles pertaining to law enforcement: lawfulness and fairness, purpose limitation, data minimisation, accuracy, storage limitation, and integrity and confidentiality. In order to be lawful, processing of special category (sensitive) data must be based on one or more of the conditions in Schedule 2 to this Ordinance.

PART III DATA SUBJECT RIGHTS

This Part sets out specific rights of data subjects and the corresponding duties of controllers. These data subject rights are:

- (a) the right to be given information when one's personal data is processed;
- (b) the right of access;
- (c) the right to rectification or restriction of processing;
- (d) the right to erasure; and
- (e) the right not to be subjected to decisions based on automated processing.

There are exceptions and exemptions relating to these rights set out in this Part and in Schedule 3 (given effect by clause 48 of this Ordinance). Notably, clause 24 in this Part allows a controller to wholly or partly restrict the publication of information or provision of information to a data subject or the Authority, where necessary and proportionate to –

- (a) avoid obstructing an official or legal inquiry, investigation or procedure within or outside the Bailiwick,
- (b) avoid prejudicing the prevention, detection, investigation or prosecution of a criminal offence within or outside the Bailiwick,
- (c) avoid prejudicing any proceedings relating to a criminal offence within or outside the Bailiwick,
- (d) protect public security or the security of the British Islands, or
- (e) protect the significant interests of any individual.

PART IV DUTIES OF CONTROLLERS AND PROCESSORS

This Part sets out more general duties of controllers and processors, many of which are similar to the duties set out in Part IV of the Law (duties of controllers and processors).

PART V SECURITY OF PERSONAL DATA

This Part imposes duties on controllers and processors relating to security. Many of these, including notification of a personal data breach, are similar to the security duties in Part VI of the Law. Notably, the security duties in the Law Enforcement Ordinance are subject to the power of controllers under clause 24 of this Ordinance to wholly or partly restrict notifications.

PART VI
DATA PROTECTION IMPACT ASSESSMENTS AND PRIOR CONSULTATION

This Part imposes duties on controllers to carry out impact assessments or consultation in relation to high-risk processing or legislation. These duties are similar to duties of controllers under Part VII of the Law.

PART VII
DATA PROTECTION OFFICERS

This Part requires all controllers (competent authorities) processing personal data for law enforcement purposes to designate a data protection officer. It sets out the qualifications required for such a designation, the functions of data protection officers, and duties of designating entities that are similar to those set out in Part VIII of the Law.

PART VIII
TRANSFERS TO OTHER JURISDICTIONS

This Part imposes stricter rules for transfers to authorised jurisdictions than Part X of the Law. Part X of the Law allows such transfers where there are adequate available safeguards (such as an enforceable contract or binding corporate rules), where authorised by the Authority or in a range of other circumstances (such as for the performance of a contract involving the data subject).

In contrast, Part VIII of this Ordinance prohibits such transfers unless four conditions are met. The first condition is that the transfer is necessary for a law enforcement purpose. The second condition is that appropriate safeguards are in place for the protection of the personal data or special circumstances exist for that particular transfer (e.g. it is necessary to protect the vital interests of an individual or to prevent an immediate and serious threat to public security or national security). The third condition is that the transfer is to a competent authority or international organisation engaged in law enforcement functions or otherwise meets special conditions of transfer to other bodies. The fourth and final condition applies where the personal data was originally transferred by a competent authority in another authorised jurisdiction, and requires authorisation by a competent authority in the transferring jurisdiction in the absence of an immediate and serious threat to public security or national security or other essential interests of a country.

PART IX
GENERAL AND MISCELLANEOUS

This Part gives effect to the exceptions and exemptions relating to data subject rights in Schedule 3 to this Ordinance. It also sets out interpretation provisions and provides for this Ordinance to come into force on the 25th May, 2018.

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

ARRANGEMENT OF SECTIONS

PART I PRELIMINARY

1. Object of this Ordinance.
2. Application of this Ordinance.
3. Application of provisions of the Law.

PART II DUTIES AND PRINCIPLES OF PROCESSING

4. Duty to comply with data protection principles.
5. Lawfulness and fairness principle.
6. Purpose limitation principle.
7. Data minimisation principle.
8. Accuracy principle.
9. Storage limitation principle.
10. Integrity and confidentiality principle.
11. Transmission to be subject to any applicable conditions.

PART III DATA SUBJECT RIGHTS

Controller's duties and data subject rights

12. Data subject's right to information.
13. Right of access.
14. Right to rectification or restriction of processing.
15. Right to erasure.
16. Actions required following rectification, restriction, etc.
17. Right not to be subjected to decisions based on automated processing.
18. Controller must facilitate exercise of data subject rights.

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

19. General exemption for judicial decisions, etc.
20. Application and effect of sections 21 to 23.
21. Compliance with request to exercise data subject right.
22. Requirement to verify identity.
23. Exceptions based on nature of request.
24. Restrictions on duty to provide information on grounds of obstruction, prejudice, etc.

PART IV
DUTIES OF CONTROLLERS AND PROCESSORS

Duty of controllers to give information or take action

25. Requirements to give information or take action.

Duty to take steps to ensure compliance

26. Duty to take reasonable steps for compliance.
27. Data protection measures by design and default.
28. Joint controllers.

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

29. Duties of controllers in relation to processors.
30. Duties of processors in relation to controllers.
31. Duties of processors in relation to further processing by another processor.

PART V
SECURITY OF PERSONAL DATA

32. Duty to take reasonable steps to ensure security.
33. Special security measures in respect of automated processing.
34. Notification and records required in case of personal data breach.
35. Data subject to be notified if high risk to significant interests.

PART VI
DATA PROTECTION IMPACT ASSESSMENTS AND PRIOR CONSULTATION

36. Impact assessment required for high-risk processing.
37. Prior consultation required for high-risk processing.

38. Prior consultation required for high-risk legislation.

PART VII
DATA PROTECTION OFFICERS

39. Mandatory designation of data protection officer.
40. Requirements for designation.
41. Functions of data protection officers.
42. Further duties in relation to data protection officers.

PART VIII
TRANSFERS TO OTHER JURISDICTIONS

43. Prohibition of transfers to other jurisdictions.
44. Transfers on the basis of available safeguards.
45. Transfers on the basis of special circumstances.
46. Transfers of personal data to persons other than relevant authorities.
47. Subsequent transfers.

PART IX
GENERAL AND MISCELLANEOUS

48. General exceptions and exemptions.
49. General provisions as to regulations.
50. Interpretation.
51. Citation.
52. Commencement.

SCHEDULE 1: Modifications to the Law for competent authorities processing for a law enforcement purpose

SCHEDULE 2: Conditions for lawful processing of special category data

SCHEDULE 3: General exceptions and exemptions

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

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

PART I

PRELIMINARY

Object of this Ordinance.

1. The object of this Ordinance is to –
 - (a) protect the rights of individuals in relation to their personal data, and provide for the free movement of personal data, in a manner equivalent to the Law Enforcement Directive,
 - (b) make other provisions considered appropriate in relation to the processing of personal data for a law enforcement purpose.

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

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

Application of this Ordinance.

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

Application of provisions of the Law.

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

- (a) the provisions of Part I, except section 1,
- (b) section 10, except subsection (7) of that section,
- (c) section 11, except subsection (1)(b) of that section,
- (d) section 37,
- (e) the provisions of Part V, and
- (f) the provisions of Parts XI to XVI, except section 96.

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

PART II
DUTIES AND PRINCIPLES OF PROCESSING

Duty to comply with data protection principles.

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

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

Lawfulness and fairness principle.

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

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

(a) in the case of any personal data –

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

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

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

and

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

(3) The condition in this subsection is that –

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

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

(4) The condition in this subsection is that –

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

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

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

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

Purpose limitation principle.

6. (1) Personal data –

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

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

(3) The condition in this subsection is that –

- (a) the consent of the data subject is obtained for the secondary processing (for the secondary law enforcement purpose),
- (b) the secondary processing is for a historical or scientific purpose related to the secondary law enforcement purpose, or

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

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

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

- (a) the consent of the data subject is obtained for the processing for that other purpose,
- (b) the processing for that other purpose is authorised by regulations made by the Committee for this purpose and carried out in accordance with those regulations, or
- (c) the processing for that other purpose is authorised or required by any other enactment and carried out in accordance with the enactment.

Data minimisation principle.

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

Accuracy principle.

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

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

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

- (a) persons suspected of having committed or being about to commit a criminal offence,
- (b) persons convicted of a criminal offence,
- (c) persons who are or may be victims of a criminal offence, and
- (d) witnesses or other persons with information about criminal offences.

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

- (5) For the purposes of subsection (4), so far as practicable—
- (a) the quality of personal data (in relation to its accuracy, completeness and recentness) must be verified before it is transmitted or made available,
 - (b) in all transmissions of personal data, the necessary information enabling the recipient to assess the degree of accuracy, completeness and reliability of the data and the extent to which it is up to date must be included, and
 - (c) if, after personal data has been transmitted, it emerges that the data was incorrect or that the transmission was unlawful, the recipient must be notified without delay.

Storage limitation principle.

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

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

Integrity and confidentiality principle.

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

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

Transmission to be subject to any applicable conditions.

11. (1) This section applies where –
 - (a) a competent authority transmits personal data to another person, and
 - (b) this Ordinance or any other enactment imposes specific conditions in relation to the processing of the personal data by the competent authority.
- (2) The competent authority must –
 - (a) inform the recipient of the personal data of those conditions, and
 - (b) require the recipient to comply with those conditions.

PART III

DATA SUBJECT RIGHTS

Controller's duties and data subject rights

Data subject's right to information.

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

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

- (a) the identity and contact details of the controller and, where applicable, the controller's representative,
- (b) the contact details of the data protection officer, where applicable,
- (c) the purposes of the processing,
- (d) information as to the existence of the data subject rights under sections 13 to 17,
- (e) the complaints and appeals information, and
- (f) the possibility of requesting the Authority to bring civil proceedings before a court under section 85 of the Law.

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

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

- (c) where applicable, information about the categories of recipients of the personal data (including recipients in authorised or unauthorised jurisdictions), and
- (d) any other information necessary to enable the data subject to exercise the data subject rights.

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

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

- (a) within a reasonable period of that personal data being processed in the context of the controller, having regard to the specific circumstances in which the personal data is so processed, and
- (b) in any case, before or at the earlier of the following times –
 - (i) if the personal data is used for communication with the data subject, the time of the first communication with the data subject, and

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

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

- (a) as soon as practicable, and
- (b) in any case, upon request by the data subject.

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

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

- (a) means a decision made by the European Commission that the country, sector or international organisation concerned ensures an adequate level of protection within the meaning of Article 36 of the Law Enforcement Directive, and
- (b) includes a finding of the European Commission under Article 31(2) of the former Directive, in force immediately before the commencement date, that the country, sector or international organisation concerned ensures an adequate level of protection within the

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

Right of access.

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

- (a) confirmation as to whether or not personal data relating to the individual is being processed in the context of a controller, and
- (b) if personal data relating to the individual is being processed in the context of a controller –
 - (i) one copy of the personal data,
 - (ii) the purposes and the legal basis of the processing,
 - (iii) the categories of personal data concerned,
 - (iv) any available information as to the source of the personal data,

- (v) the recipients or categories of recipients to whom the personal data is disclosed, in particular recipients in any unauthorised jurisdiction,
- (vi) the period for which the personal data is expected to be stored, or if that is not possible, the criteria used to determine that period,
- (vii) information as to the existence of the data subject rights under sections 14 to 17,
- (viii) the complaints and appeals information,
- (ix) the possibility of requesting the Authority to bring civil proceedings before a court under section 85 of the Law, and
- (x) information as to the personal data undergoing processing and any available information as to its origin.

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

Right to rectification or restriction of processing.

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

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

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

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

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

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

(a) rectify that personal data, or

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

(4) Subsection (5) applies where –

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

- (b) it is not reasonable to expect the controller to verify the accuracy or completeness of the personal data.
- (5) Where this subsection applies, the controller –
- (a) must add to the personal data a statement to the effect that the data subject disputes the accuracy or (as the case may be) completeness of that personal data, and
 - (b) may, if requested by the data subject, restrict processing of the personal data in a manner and for a time agreed with the data subject, except to the extent that the data subject gives consent to processing of that personal data in any other manner.
- (6) Nothing in this section limits section 15.

Right to erasure.

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

- (a) the processing of any personal data breaches or would breach section 4, including any of these principles –
 - (i) the principle in section 5(1) (lawfulness and fairness),
 - (ii) the principle in section 6(1) (purpose limitation),

- (iii) the principle in section 7 (data minimisation),
 - (iv) the principle in section 8(1), (2), (3) or (4) (accuracy),
 - (v) the principle in section 9(1) or (2) (storage limitation), or
 - (vi) the principle in section 10 (integrity and confidentiality), or
- (b) the controller has a duty imposed by law to erase the personal data, otherwise than under this section.

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

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

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

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

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

- (a) must add to the personal data a statement to the effect that the data subject disputes the accuracy or (as the case may be) completeness of that personal data, and
- (b) may, if requested by the data subject, restrict processing of the personal data in a manner and for a time agreed with the data subject, except to the extent that the data subject gives consent to processing of that personal data in any other manner.

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

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

- (a) the controller must notify any person ("**recipient**") to whom the controller has disclosed that data, and
- (b) where a recipient is the controller of that personal data, the recipient must similarly erase that personal data.

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

Actions required following rectification, restriction, etc.

16. (1) This section applies where a controller –
 - (a) rectifies or completes personal data under section 14(3),
 - (b) adds to or restricts the processing of personal data in accordance with section 14(5) or 15(5), or
 - (c) restricts the processing of personal data under section 15(6).
- (2) The controller must, as soon as practicable, notify –
 - (a) any competent authority or other relevant authority from which the personal data originated, and
 - (b) any person ("**recipient**") to whom the controller has disclosed the personal data.
- (3) If a recipient is the controller of that personal data, the recipient must similarly rectify, complete, add to or (as the case may be) restrict the processing of that data.
- (4) A controller must inform the data subject before lifting any restriction on the processing of personal data.

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

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

- (a) a data subject has a right not to be subjected to an automatic decision, and
- (b) a controller must not cause or permit a data subject to be subjected to an automatic decision.

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

- (a) the data subject has given consent to the automated processing, or
- (b) the automated processing is –
 - (i) authorised by regulations made by the Committee for this purpose and carried out in accordance with those regulations, or
 - (ii) otherwise authorised or required by law.

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

- (a) the data subject has given consent to the automated processing of that special category data, or
- (b) the automated processing of that kind or description of special category data is –

- (i) specifically authorised by regulations made by the Committee for this purpose and carried out in accordance with those regulations, or
- (ii) specifically authorised or specifically required by any other enactment and carried out in accordance with the enactment.

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

- (a) the controller must, as soon as reasonably practicable, inform the data subject that an automatic decision has been taken based solely on automated processing of personal data relating to the data subject, and
- (b) the data subject may, before the end of the period of 21 days beginning with receipt of the notification, request the controller to—
 - (i) reconsider the decision, or
 - (ii) take a new decision that is not based solely on automated processing.

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

- (a) consider the request, including any information provided by the data subject that is relevant to it,
- (b) comply with the request, and
- (c) inform the data subject of—
 - (i) the steps taken to comply with the request, and
 - (ii) the outcome of complying with the request

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

(7) In this section –

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

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

- (a) is based solely on automated processing of personal data relating to the data subject, and
- (b) affects the significant interests of the data subject.

Controller must facilitate exercise of data subject rights.

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

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

General exemption for judicial decisions, etc.

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

(2) In this section –

"crime-related investigation" means –

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

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

Application and effect of sections 21 to 23.

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

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

(b) to take any action.

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

(3) In sections 21 to 23 –

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

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

Compliance with request to exercise data subject right.

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

(a) as soon as practicable, and

(b) in any event within the designated period.

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

- (a) the controller's reasons for not so complying,
- (b) the complaints and appeals information, and
- (c) the possibility of requesting the Authority to bring civil proceedings before a court under section 85 of the Law.

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

- (a) as soon as practicable, and
- (b) in any event within the designated period.

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

- (a) any such extension, and
- (b) the reasons for the extension.

(5) In this section –

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

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

- (a) the day on which the controller receives the request,
- (b) the day on which the controller receives any information reasonably necessary to confirm the identity of the requestor, and
- (c) the day on which any fee or charge payable under this Ordinance in respect of any information or action requested is paid to the controller.

Requirement to verify identity.

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

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

- (a) the requestor is not entitled to exercise any data subject right conferred on the requestor in relation to the controller, and
- (b) the controller is not required to give the information or take the action requested by the individual.

Exceptions based on nature of request.

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

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

- (a) refuse to give the information or take any action requested in that part of the request, or
- (b) in exceptional circumstances, give that information or take that action but charge a reasonable fee for the administrative costs of so doing.

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

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

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

- (a) avoid obstructing an official or legal inquiry, investigation or procedure within or outside the Bailiwick,
- (b) avoid prejudicing the prevention, detection, investigation or prosecution of a criminal offence within or outside the Bailiwick,
- (c) avoid prejudicing any proceedings relating to a criminal offence within or outside the Bailiwick,
- (d) protect public security or the security of the British Islands, or
- (e) protect the significant interests of any individual.

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

- (a) give the data subject the following information –
 - (i) a statement to the effect that the provision of information has been restricted,
 - (ii) the reasons for the restriction,
 - (iii) the complaints and appeals information, and

- (iv) the possibility of requesting the Authority to bring civil proceedings before a court under section 85 of the Law, and
 - (b) record the reasons for the restriction.
- (3) Neither subsection (2)(a) nor (2)(b) applies where complying with those provisions would undermine the purpose of the restriction.
- (4) In this section, "**information duty**" means -
 - (a) a duty imposed on the controller to publish information or give information to the data subject under –
 - (i) section 12(2) or (3),
 - (ii) section 13(2),
 - (iii) section 21(1) or (2), or
 - (iv) section 35(1), or
 - (b) a duty imposed on the controller to give information to the Authority under section 34(2).

PART IV
DUTIES OF CONTROLLERS AND PROCESSORS

Duty of controllers to give information or take action

Requirements to give information or take action.

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

- (a) in writing, unless the information is given in response to a request and the person requests that it be given orally, in which case it may be given orally after verifying the identity of that person,
- (b) if the information is given in response to a request and the request is made by electronic means, by similar or commonly used electronic means unless otherwise requested by the person, in which case it may be given by the other means requested after verifying the identity of that person,
- (c) if the information is given in writing, in a concise, transparent, easily visible, easily accessible, intelligible and clearly legible form, and
- (d) in any case –
 - (i) in clear and plain language, and

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

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

- (a) prescribed by regulations made by the Committee, or
- (b) specified by any other provision of this Ordinance.

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

- (a) the fee or charge payable for the information or action, or
- (b) the basis on which the amount of the fee or charge payable is to be calculated or ascertained.

Duty to take steps to ensure compliance

Duty to take reasonable steps for compliance.

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

- (a) to ensure that processing of personal data is carried out in compliance with this Ordinance, and
 - (b) to be able to demonstrate such compliance upon request by the Authority.
- (2) In discharging the duty in subsection (1), the controller must take into account –
- (a) the nature, scope, context and purpose of the processing,
 - (b) the likelihood and severity of risks posed to the significant interest of data subjects, if processing is not carried out in compliance with this Ordinance,
 - (c) best practices in technical measures, organisational measures and any other steps that may be taken for the purposes of subsection (1), and
 - (d) the costs of implementing appropriate measures.

Data protection measures by design and default.

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

- (a) effectively comply with the data protection principles,

- (b) ensure, by default, that only personal data that is necessary for each specific purpose of processing is processed, and
- (c) integrate any other necessary safeguards into the processing to comply with this Ordinance and safeguard data subject rights.

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

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

- (a) the amount of personal data collected,
- (b) the extent of its processing,
- (c) the period of its storage, and
- (d) its accessibility, in particular ensuring that personal data is not made accessible to an indefinite number of persons without human intervention.

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

Joint controllers.

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

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

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

- (a) specify the respective roles, relationships, responsibilities and duties of each joint controller, in relation to the data subjects, and
- (b) designate the controller which is to be the contact point for data subjects.

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

- (a) a data subject may exercise any data subject right against any joint controller, and
- (b) each joint controller remains jointly and severally liable for the performance of any duty imposed on a controller by this Ordinance.

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

Duties of controllers in relation to processors.

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

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

- (a) to ensure that the processing meets the requirements of this Ordinance, and
- (b) to safeguard data subject rights.

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

- (a) the subject matter of the processing,
- (b) the duration of the processing,
- (c) the nature, scope, context and purpose of the processing,
- (d) the category of personal data to be processed,
- (e) the categories of data subjects,

- (f) the duties and rights of the controller, and
- (g) the duties imposed on the processor by sections 30 and 31.

Duties of processors in relation to controllers.

30. (1) A processor must –
- (a) subject to paragraph (b), process personal data only on written instructions from the controller, including with regard to transfers of personal data to an unauthorised jurisdiction,
 - (b) where a processor is required by law to process personal data contrary to paragraph (a), inform the controller of that requirement (unless prohibited by an enactment) before so processing the personal data,
 - (c) ensure that any person authorised by the processor to process the personal data is legally bound to a duty of confidentiality,
 - (d) at the controller's discretion, after the end of the provision of services relating to processing, and unless required to store the personal data by an enactment –
 - (i) delete all personal data, or
 - (ii) return all personal data to the controller, and

delete existing copies,

- (e) put in place reasonable technical and organisational measures to assist the controller to exercise or perform the controller's duties under Part III, and
- (f) make available to the controller all information necessary to demonstrate compliance with this section and sections 29 and 31.

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

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

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

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

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

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

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

- (a) notify the controller of the proposed engagement, and
- (b) give the controller an opportunity to object to the engagement.

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

- (a) is an employee of the primary processor, or
- (b) processes the personal data under the direction and control of the primary processor.

PART V
SECURITY OF PERSONAL DATA

Duty to take reasonable steps to ensure security.

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

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

- (a) pseudonymising and encrypting personal data,
- (b) ensuring that the controller or processor has and retains the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services,
- (c) ensuring that the controller or processor has and retains the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident, and
- (d) establishing and implementing a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

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

- (a) the nature, scope, context and purpose of the processing,
- (b) the likelihood and severity of risks posed to the significant interest of data subjects, if the personal data is not secure,
- (c) best practices in technical measures, organisational measures and any other steps that may be taken for the purposes of subsection (1), and
- (d) the costs of implementing appropriate measures.

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

- (a) accidental or unlawful destruction, loss or alteration of personal data, or
- (b) unauthorised disclosure of, or access to, personal data.

Special security measures in respect of automated processing.

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

- (a) deny unauthorised persons access to processing equipment (referred to as "equipment access control" in the Law Enforcement Directive),
- (b) prevent the unauthorised reading, copying, modification or removal of data media (referred to as "data media control" in the Law Enforcement Directive),
- (c) prevent the unauthorised input of personal data and the unauthorised inspection, modification or deletion of stored personal data (referred to as "storage control" in the Law Enforcement Directive),
- (d) prevent the use of automated processing systems by unauthorised persons using data communication equipment (referred to as "user control" in the Law Enforcement Directive),
- (e) ensure that persons authorised to use an automated processing system have access only to the personal data covered by their access authorisation (referred to as "data access control" in the Law Enforcement Directive),
- (f) ensure that it is possible to verify and establish the persons to which personal data have been or may be transmitted or made available using data communication equipment (referred to as

"communication control" in the Law Enforcement Directive),

- (g) ensure that it is subsequently possible to verify and establish which personal data have been input into automated processing systems and when and by whom the personal data were input (referred to as "input control" in the Law Enforcement Directive),
- (h) prevent the unauthorised reading, copying, modification or deletion of personal data during transfers of personal data or during transportation of data media (referred to as "transport control" in the Law Enforcement Directive),
- (i) ensure that installed systems may, in the case of interruption, be restored (referred to as "recovery" in the Law Enforcement Directive), and
- (j) ensure that the functions of the system perform, that the appearance of faults in the functions is reported (referred to as "reliability" in the Law Enforcement Directive) and that stored personal data cannot be corrupted by means of a malfunctioning of the system (referred to as "integrity" in the Law Enforcement Directive).

Notification and records required in case of personal data breach.

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

- (a) give the controller notice of it as soon as practicable, and
- (b) where oral notice is given under paragraph (a), follow up the oral notice with a written notice to the controller at the first available opportunity.

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

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

(3) Subject to subsection (4), a notice under subsection (2) must include –

- (a) a description of the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned,

- (b) the name and contact details of the data protection officer or other contact point where more information can be obtained,
- (c) a description of the likely consequences of the personal data breach,
- (d) a description of the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects, and
- (e) if the notice is given more than 72 hours after the controller becomes aware of the personal data breach, an explanation of the reasons for the delay.

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

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

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

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

- (a) the facts relating to the breach,
- (b) the effects of the breach,
- (c) the remedial action taken, and
- (d) any steps taken by the controller to comply with this section, including whether the controller gave a notice to the Authority under subsection (2), and if so, a copy of the notice.

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

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

(2) The notice must include –

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

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

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

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

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

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

(c) performing that duty would involve disproportionate effort.

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

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

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

PART VI

DATA PROTECTION IMPACT ASSESSMENTS AND PRIOR CONSULTATION

Impact assessment required for high-risk processing.

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

- (2) The assessment must include –
- (a) a general description of the proposed processing operations (including the means of processing),
 - (b) an assessment of the risks posed to the significant interests of data subjects by the processing, and
 - (c) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and demonstrate

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

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

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

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

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

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

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

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

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

Prior consultation required for high-risk processing.

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

- (a) where a data protection impact assessment indicates that the processing is likely to be high-risk processing in the absence of measures taken by the controller to mitigate risks to the significant interests of data subjects,
- (b) where the type of processing involved is likely to be high-risk processing, or
- (c) in other prescribed circumstances.

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

(3) A request must include the following information–

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

- (b) a copy of the data protection impact assessment (if any),
- (c) the contact details of any data protection officer, and
- (d) any other information required by the Authority.

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

- (a) must give written notice of its opinion to the controller and, where applicable to the processor, and
- (b) may exercise any power conferred on the Authority by the Law or this Ordinance in relation to a breach or potential breach of an operative provision.

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

- (a) as soon as practicable, and
- (b) in any event within six weeks of the designated date.

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

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

- (7) In this section, "**designated date**" means the later of –
 - (a) the date on which the Authority receives the request made by the controller, or
 - (b) if the Authority has requested information from the controller or processor within the six-week period following the date specified in paragraph (a), the date on which the Authority receives the information requested.

Prior consultation required for high-risk legislation.

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

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

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

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

PART VII
DATA PROTECTION OFFICERS

Mandatory designation of data protection officer.

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

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

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

(b) in any case –

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

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

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

judicial capacity.

Requirements for designation.

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

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

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

(b) the individual satisfies any prescribed requirements.

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

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

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

Functions of data protection officers.

41. (1) A data protection officer must –
- (a) inform and advise the officer's designating entity and its employees who carry out processing operations ("**relevant employees**") of their duties under this Ordinance and any other enactments relating to data protection,
 - (b) monitor the designating entity's compliance with –
 - (i) this Ordinance,
 - (ii) any other enactments relating to data protection,
 - (iii) the policies of the designating entity in relation to data protection, including in relation to the assignment of responsibilities, awareness-raising and training of relevant employees, and
 - (iv) any data protection audits required by or under the Law or this Ordinance,
 - (c) where requested, provide advice to the designating entity and relevant employees relating to data protection impact assessments and monitor the carrying out of such assessments,

- (d) act as the contact point for the Authority on issues relating to processing, including any prior consultation required by section 37 and any other consultation with the Authority with regard to any other matter, and
- (e) cooperate with the Authority in the exercise or performance of any of the Authority's functions under the Law or this Ordinance.

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

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

Further duties in relation to data protection officers.

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

- (a) give written notice to the Authority of the name and contact details of the officer, and
- (b) publish a notice stating –
 - (i) the fact that a data protection officer has been designated, and

(ii) the contact details of the officer.

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

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

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

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

(c) the officer is provided the resources necessary -

(i) to perform those functions,

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

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

- (d) the officer is not dismissed or penalised for performing those functions, other than for failing to perform those functions in a professional and competent manner and to the best of the officer's abilities,
- (e) data subjects are allowed to contact the officer directly with regard to any issues related to the processing of their personal data or the exercise of their rights under this Ordinance, and
- (f) any other tasks and duties assigned to the officer do not result in a conflict of interest in relation to the performance of the officer's functions.

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

- (a) to avoid obstructing an official or legal inquiry, investigation or procedure within or outside the Bailiwick,
- (b) to avoid prejudicing the prevention, detection, investigation or prosecution of a criminal offence within or outside the Bailiwick,
- (c) to avoid prejudicing any proceedings relating to a criminal offence within or outside the Bailiwick, or

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

PART VIII

TRANSFERS TO OTHER JURISDICTIONS

Prohibition of transfers to other jurisdictions.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Transfers on the basis of available safeguards.

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

- (a) in a legally binding instrument, or
- (b) otherwise in all the circumstances surrounding the transfer.

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

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

- (a) the date and time of the transfer,
- (b) the name of and any other pertinent information about the recipient,
- (c) the justification for the transfer, and
- (d) a description of the personal data transferred.

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

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

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

Transfers on the basis of special circumstances.

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

- (a) to protect the vital interests of the data subject or any other individual,
- (b) to safeguard the legitimate interests of the data subject,
- (c) to prevent an immediate and serious threat to the public security or national security of any country,
- (d) in individual cases for any law enforcement purpose, or
- (e) in individual cases –
 - (i) for the purpose of, or in connection with, any legal proceedings (including prospective legal proceedings) relating to a law enforcement purpose,
 - (ii) for the purpose of obtaining legal advice in relation to a law enforcement purpose, or

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

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

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

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

(a) the date and time of the transfer,

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

(c) the justification for the transfer, and

(d) a description of the personal data transferred.

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

Transfers of personal data to persons other than relevant authorities.

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

- (a) the transfer is strictly necessary in a specific case for the performance of a function conferred or imposed by law on the controller for a law enforcement purpose,
- (b) the controller has determined that no significant interests of the data subject override the public interest necessitating the transfer,
- (c) the transferring controller considers that the transfer of the personal data to a relevant authority or to a relevant international organisation would be ineffective or inappropriate, and
- (d) the controller informs the recipient of the specific purpose for which the personal data may, so far as is necessary, be processed.

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

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

- (a) inform a relevant authority of the unauthorised jurisdiction of the transfer as soon as practicable, unless this would be ineffective or inappropriate, and
 - (b) record the transfer in writing and keep the record for a prescribed period.
- (4) A record required to be kept by subsection (3)(b) must include–
- (a) the date and time of the transfer,
 - (b) the name of and any other pertinent information about the recipient,
 - (c) the justification for the transfer, and
 - (d) a description of the personal data transferred.
- (5) The controller must notify the Authority of the categories of data transferred in reliance on meeting the requirements of subsection (1).
- (6) This section does not limit or affect the operation of any international agreement in force between the Bailiwick and any other country in the field of judicial co-operation in criminal matters and police co-operation.

Subsequent transfers

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

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

- (a) the transferring controller, or
- (b) another competent authority of the Bailiwick or an authorised jurisdiction.

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

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

- (a) the seriousness of the circumstances leading to the request for authorisation,
- (b) the purpose for which the personal data was originally transferred,
- (c) the standards for the protection of personal data that apply in the unauthorised jurisdiction to which the personal data would be further transferred, and
- (d) any other relevant matters.

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

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

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

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

(b) the transfer –

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

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

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

(7) In this section –

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

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

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

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

PART IX
GENERAL AND MISCELLANEOUS

General exceptions and exemptions.

48. Schedule 3 has effect.

General provisions as to regulations.

49. (1) Regulations under this Ordinance -

- (a) may be amended or repealed by subsequent regulations hereunder,
- (b) may contain such consequential, incidental, supplemental and transitional provision as may appear to the Committee to be necessary or expedient, and
- (c) must be laid before a meeting of the States of Deliberation as soon as possible and, if at that or the next meeting the States of Deliberation resolve to annul them, cease to have effect, but without prejudice to anything done under them or to the making of new regulations.

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

may be exercised -

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

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

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

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

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

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

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

- (b) may empower the Authority, any public committee, any other body or authority (including, without limitation, any court of the Bailiwick), or any other person to issue codes or guidance in relation to any matter for which regulations may be made under this Ordinance, and
 - (c) may repeal, replace, amend, extend, adapt, modify or disapply any rule of custom or law.
- (4) Regulations under this Ordinance may not –
 - (a) provide for offences to be triable only on indictment, or
 - (b) authorise the imposition –
 - (i) on summary conviction, of imprisonment for a term exceeding 12 months, or a fine exceeding level 5 on the uniform scale, or
 - (ii) on conviction on indictment, of imprisonment for a term exceeding two years.
- (5) Before making any regulations under this Ordinance, the Committee must consult –
 - (a) the Authority,

- (b) in the case of regulations having effect in Alderney, the Policy and Finance Committee of the States of Alderney, and
- (c) in the case of regulations having effect in Sark, the Policy and Performance Committee of the Chief Pleas of Sark,

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

Interpretation.

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

"authorised jurisdiction" means –

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

"competent authority" means –

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

(i) the States,

(ii) a public committee,

(iii) a holder of a public office,

(iv) a statutory body,

(v) a court or tribunal of the Bailiwick,

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

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

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

- (ix) any person exercising or performing functions or holding any office similar or comparable to any of the persons described in subparagraphs (i) to (viii) in respect of any country other than the Bailiwick, or
- (b) any other person that exercises or performs any function that is of a public nature in respect of the Bailiwick or any other country, when exercising or performing a function that is of a public nature in respect of the Bailiwick or any other country for a law enforcement purpose, or
- (c) any other prescribed person,

"the complaints and appeals information" means –

- (a) information as to the existence of –
 - (i) the right to complain to the Authority under section 67 of the Law, and
 - (ii) a complainant's rights of appeal under sections 82 and 83 of the Law, and
- (b) the contact details of the Authority,

"criminal proceeds enactment" means –

- (a) any of the following enactments, including any Ordinance or subordinate legislation made under any of them –
 - (i) the Criminal Justice (Proceeds of Crime) (Bailiwick of Guernsey) Law, 1999^c,
 - (ii) the Drug Trafficking (Bailiwick of Guernsey) Law, 2000^d,
 - (iii) the Terrorism and Crime (Bailiwick of Guernsey) Law, 2002^e,

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

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

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

- (iv) the Criminal Justice (Fraud Investigation) (Bailiwick of Guernsey) Law, 1991^f,
- (v) the Criminal Justice (International Cooperation) (Bailiwick of Guernsey) Law, 2001^g,
- (vi) the Forfeiture of Money etc. in Civil Proceedings (Bailiwick of Guernsey) Law, 2007^h,
- (vii) the Disclosure (Bailiwick of Guernsey) Law, 2007ⁱ,
- (viii) the Beneficial Ownership of Legal Persons (Guernsey) Law, 2017^j, or
- (ix) the Beneficial Ownership of Legal Persons (Alderney) Law, 2017^k, or

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

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

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

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

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

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

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

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

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

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

"enactment" includes –

- (a) an Act of Parliament that extends to the Bailiwick, and
- (b) a Law, an Ordinance and any subordinate legislation and includes any provision or portion of a Law, an Ordinance or any subordinate legislation,

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

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

"**the former Commissioner**" means the Data Protection Commissioner under the Data Protection (Bailiwick of Guernsey) Law, 2001¹,

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

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

- (a) prevention, investigation, detection or prosecution of a criminal offence within or outside the Bailiwick,
- (b) the execution of criminal penalties within or outside the Bailiwick,
- (c) safeguarding against or preventing threats to public security or the security of the British Islands, or
- (d) exercising or performing any power or duty conferred or imposed on a public authority by a criminal proceeds enactment,

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

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

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

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

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

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

- (a) any proceedings for the purpose of executing a criminal penalty,
- (b) any proceedings under or for the purposes of a criminal proceeds enactment, and
- (c) the exercise or performance of any power or duty conferred or imposed on a public authority by a criminal proceeds enactment,

"**public security**" includes –

- (a) the health or safety of the population,
- (b) the security of any infrastructure facility, information systems or communications network, which if prejudiced may endanger human life, and
- (c) the economic or environmental security,

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

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

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

"relevant authority" –

- (a) means any person in a jurisdiction that has, in respect of that jurisdiction, functions comparable to those of a competent authority, and
- (b) includes an authority competent for the purposes referred to in Article 1(1) of the Law Enforcement Directive,

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

- (a) means the marking of stored personal data with the aim of limiting its processing in the future, and
- (b) includes restricting or otherwise limiting the processing of that personal data in a manner and for a period of time under section 14(5) or 15(5) or (6), and

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

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

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

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

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

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

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

(b) the context requires otherwise.

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

^m Ordres en Conseil Vol. XIII, p. 355.

interpretation of this Ordinance throughout the Bailiwick of Guernsey.

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

Citation.

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

Commencement.

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

SCHEDULE 1

Section 3(1)

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

Provision of the Law	Modifications
Section 11(2)	For "Part III of this Law", substitute "Part III of the Law Enforcement Ordinance".
Section 73(2)	<p>At the end of paragraph (e)(iii), immediately after the comma, insert "and".</p> <p>At the end of paragraph (f), for ", and", substitute a full stop.</p> <p>Omit paragraph (g).</p>
Section 73(7) and (7A)	<p>For these subsections, substitute the following subsection –</p> <p style="padding-left: 40px;">"(7) In determining what, if any, order to make under subsection (2) in any case where a controller or processor has breached an operative provision, the Authority must have regard to –</p> <ul style="list-style-type: none"> (a) the nature, gravity and duration of the breach concerned, taking into account – <ul style="list-style-type: none"> (i) the nature, scope and purpose of the processing concerned, (ii) the categories of personal data affected by the breach, (iii) the number of data subjects affected, and (iv) the level of any damage suffered by these data subjects, (b) the manner in which the breach became known to the Authority, in particular whether, and if so to what extent, the person concerned notified the breach to the Authority, (c) whether the breach was intentional or negligent, (d) the degree of responsibility of the person concerned, taking into account technical and organisational measures implemented by that person for the purposes of any provision of this Law, (e) any relevant previous breaches by the person concerned,

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

SCHEDULE 2

Section 5(4)(b)

CONDITIONS FOR LAWFUL PROCESSING OF SPECIAL CATEGORY DATA

1. The information contained in the personal data has been made public as a result of steps deliberately taken by the data subject.
2. The processing is necessary for the controller to exercise any right or power, or perform or comply with any duty, conferred or imposed on the controller by an enactment or otherwise by law.
3. The processing is necessary in order to comply with an order or a judgment of a court or tribunal having the force of law in the Bailiwick.
4. The processing is necessary –
 - (a) for the purpose of, or in connection with –
 - (i) any legal proceedings (including prospective legal proceedings), or
 - (ii) the discharge of any functions of a court or tribunal acting in its judicial capacity,
 - (b) for the purpose of obtaining legal advice, or
 - (c) otherwise for the purposes of establishing, exercising or defending legal rights.

5. The processing is necessary for –
 - (a) the administration of justice, or
 - (b) the exercise of any function of the Crown, a Law Officer of the Crown, the States or a public committee.
6. The processing is necessary for a historical or scientific purpose.
7. The processing is –
 - (a) authorised by regulations made by the Committee for this purpose and carried out in accordance with those regulations, or
 - (b) authorised or required by any other enactment and carried out in accordance with the enactment.
8. The data subject has given consent to the processing of the personal data for the purpose for which it is processed.
9. The processing is necessary to protect the vital interests of the data subject or any other individual, and –
 - (a) the data subject is physically or legally incapable of giving consent, or
 - (b) the controller cannot reasonably be expected to obtain the consent of the data subject.

10. (1) The processing—
- (a) is necessary for the purposes of preventing fraud or a particular kind of fraud, and
 - (b) consists of —
 - (i) the disclosure of personal data by a competent authority as a member of an anti-fraud organisation,
 - (ii) the disclosure of personal data by a competent authority in accordance with arrangements made by an anti-fraud organisation, or
 - (iii) the processing of personal data disclosed as described in sub-item (i) or (ii).
- (2) In this paragraph, "**anti-fraud organisation**" means any unincorporated association, body corporate or other person which —
- (a) enables or facilitates any sharing of information to prevent fraud or a particular kind of fraud, or
 - (b) has, as its purpose or one of its purposes, the sharing of information to prevent fraud or a particular kind of fraud.

GENERAL EXCEPTIONS AND EXEMPTIONS

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

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

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

2. **Disclosure required by law, etc.**

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

- (a) to comply with a duty imposed –
 - (i) by or under any enactment,
 - (ii) by any rule of law, or
 - (iii) by the order of a court or tribunal, or

- (b) for the purpose of, or in connection with, any legal proceedings (including prospective legal proceedings),
- (c) for the purpose of obtaining legal advice, or
- (d) otherwise for the purposes of establishing, exercising or defending legal rights.

3. **Privileged items.**

Privileged items are exempt from a provision of Part III.

4. **Armed forces.**

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

5. **Negotiations.**

- (1) A negotiation record is exempt from a designated provision to the extent that the application of the provision to the record would be likely to prejudice those negotiations.
- (2) In subparagraph (1), "**negotiation record**" means a record of the intentions of the controller in relation to any negotiations with the data subject.

6. **Self-incrimination.**

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

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

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

(a) an offence under the Law,

(b) perjury, or

(c) perverting the course of justice.

7. **Judicial independence and judicial proceedings.**

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

8. **Public information.**

(1) Public information is exempt from –

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

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

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

- (a) information which the controller is required to publish by law,
and
- (b) information held on a public register.

9. Historical or scientific information.

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

10. Tax and crime information.

- (1) The exemption in each of subparagraphs (2) and (3) apply to personal data processed for –
 - (a) a law enforcement purpose, or
 - (b) the assessment or collection within or outside the Bailiwick of any tax, duty, or other imposition of a similar nature, including any interest or penalty required to be paid as a result of late payment or non-payment of such a tax, duty or other imposition.
- (2) Personal data is exempt from a designated provision (other than the lawfulness principle) to the extent that the application of the provision to the personal data would be likely to prejudice a purpose specified in subparagraph (1)(a) or (b).

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

11. Prejudice to international obligations, etc.

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

- (a) breach an international obligation of the Bailiwick, or
- (b) otherwise prejudice the ability of the Bailiwick to meet its international obligations.

12. Protective functions.

- (1) This paragraph applies to personal data processed in the discharge of a protective function that –
 - (a) is conferred or imposed by an enactment on any person,
 - (b) is a function of the Crown, a Law Officer of the Crown, the States or a public committee, or
 - (c) is of a public nature and is exercised in the public interest.

- (2) Personal data is exempt from a designated provision to the extent that the application of the provision to the personal data would be likely to prejudice the proper discharge of the protective function.
- (3) In this paragraph, "**protective function**" means –
- (a) the protection of members of the public against –
- (i) financial loss due to dishonesty, malpractice or other seriously improper conduct by, or the unfitness or incompetence of, persons concerned in the provision of banking, insurance, investment, fiduciary, trustee services or other financial services or in the establishment or management of any body corporate, limited partnership with legal personality or foundation,
 - (ii) financial loss due to the conduct of a person that is bankrupt or otherwise insolvent,
 - (iii) dishonesty, malpractice or other seriously improper conduct by, or the unfitness or incompetence of, persons authorised to carry on any profession or other activity,
 - (iv) maladministration by any public authority,
 - (v) failure in the services provided by any public authority, or

- (vi) a failure of a public authority to provide a service which it is a function of the public authority to provide,
 - (b) the protection of non-profit organisations or charities against misconduct or mismanagement (whether by trustees, directors or other persons) in their administration,
 - (c) the protection of the property of non-profit organisations or charities from loss or misapplication,
 - (d) the recovery of the property of non-profit organisations or charities,
 - (e) the securing of the health, safety and welfare of persons at work,
 - (f) the protection of persons other than those at work against risk to health or safety arising out of or in connection with the action of persons at work, or
 - (g) the protection of the reputation and standing of the Bailiwick.
- (4) Any power or duty conferred or imposed on a person by a criminal proceeds enactment is deemed to be a protective function within the meaning of subparagraph (1).

13. **Regulatory purposes.**

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

(2) In this paragraph –

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

"regulatory purpose" means –

- (a) prevention, investigation, detection, determination or punishment of an administrative offence,
- (b) carrying out the measures imposed as punishment of an administrative offence, or
- (c) determination by a public authority of an application for a registration, licence, approval or any other kind of authorisation or consent, in accordance with an enactment.

14. Disclosures prohibited or restricted by enactments.

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

- (2) Without limiting the generality of subparagraph (1), examples of such enactments include –
- (a) in relation to Guernsey, sections 17, 20A and 20B of the Adoption (Guernsey) Law, 1960ⁿ, and
 - (b) in relation to Alderney, sections 17, 20A and 20B of the Adoption (Guernsey) Law, 1960, as extended to Alderney by the Alderney (Application of Legislation) (Adoption) Ordinance, 1974^o.

15. Court-directed exemptions.

- (1) Personal data withheld by a court or tribunal is exempt from a designated provision.
- (2) Personal data is withheld by a court or tribunal if –
- (a) it is processed by a court or tribunal,
 - (b) it is supplied in a report or other evidence given to the court or tribunal in the course of any legal proceedings by or on behalf of –

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

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

- (i) a probation officer,
 - (ii) a health professional,
 - (iii) an educational establishment,
 - (iv) a public committee, or
 - (v) any other person or body, and
- (c) the court or tribunal directs that the personal data should be withheld from the data subject on the ground that it appears to be –
- (i) impracticable to disclose the report or other evidence to the data subject having regard to the age and understanding of the data subject, or
 - (ii) undesirable to do so having regard to potential serious harm which might be suffered by the data subject as a result of such disclosure.

16. Serious harm to data subjects or other individuals.

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

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

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

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

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

(4) In subparagraphs (2) and (3) –

"appropriate health professional" means –

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

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

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

(c) where –

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

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

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

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

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

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

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

- (1) This paragraph applies where a person falling within subparagraph (2) –
 - (a) is authorised by or under any enactment or rule of law to make a request under a provision of Part III on behalf of a data subject, and
 - (b) has made such a request.
- (2) A person falls within this subparagraph if –
 - (a) the data subject is a child, and that person has parental responsibility for that data subject, or
 - (b) the data subject is incapable of managing the data subject's own affairs, and that person has been appointed by a court to manage those affairs (for example, as a curateur).
- (3) Personal data relating to whether the data subject is or has been the subject of or may be at risk of child abuse is exempt from a

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

- (4) Health data or social assistance data relating to the data subject is exempt from a designated provision to the extent that the application of the provision to the health data would disclose information –
 - (a) provided by the data subject in the expectation that it would not be disclosed to the person making the request,
 - (b) obtained as a result of any examination or investigation to which the data subject consented in the expectation that the information would not be so disclosed, or
 - (c) which the data subject has expressly indicated should not be so disclosed.
- (5) Neither subparagraph (4)(a) nor (4)(b) applies where the data subject has expressly indicated that the data subject no longer has the expectation mentioned in those subparagraphs.
- (6) In subparagraph (3), "**child abuse**" includes –
 - (a) physical injury (other than accidental injury) to a child,
 - (b) physical or emotional neglect of a child,

- (c) ill-treatment of a child, or
- (d) sexual abuse of a child.

18. Public security, etc.

- (1) Personal data is exempt from any provision of Parts II to VIII of this Ordinance to the extent that the application of the provision ("**exemptable provision**") to the data would be likely to prejudice public security or the security of the British Islands.
- (2) Subject to subparagraph (4), a certificate signed by Her Majesty's Procureur certifying that exemption from one or more exemptable provisions specified in the certificate is or at any time was required for the purposes of subparagraph (1) in respect of any personal data is conclusive evidence of that fact.
- (3) A certificate under subparagraph (2) –
 - (a) may identify the personal data to which it applies by means of a general description, and
 - (b) may be expressed to have prospective effect.
- (4) Any person directly affected by the issuing of a certificate under subparagraph (2) may appeal to the Royal Court against the certificate.
- (5) If on an appeal under subparagraph (4), the Royal Court finds that, applying the principles applied by the court on an application for

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

- (a) allow the appeal, and
 - (b) quash the certificate.
- (6) Where in any proceedings under the Law it is claimed by a controller that a certificate under subparagraph (2) which identifies the personal data to which it applies by means of a general description applies to any personal data, any other party to the proceedings may appeal to the Royal Court on the ground that the certificate does not apply to the personal data in question.
- (7) But, subject to any determination under subparagraph (8), the certificate is to be conclusively presumed so to apply.
- (8) On an appeal under subparagraph (6), the Royal Court may determine that the certificate does not so apply.
- (9) A document purporting to be a certificate under subparagraph (2) must be –
- (a) received in evidence, and
 - (b) deemed to be such a certificate unless the contrary is proved.
- (10) A document which purports to be certified by or on behalf of Her Majesty's Procureur as a true copy of a certificate issued by Her

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

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

19. Committee may make further exceptions and exemptions.

- (1) The Committee may by regulations –
- (a) provide for modifications to, and further exceptions to or exemptions from, any designated provision, and
 - (b) amend this Schedule for the purpose specified in item (a).
- (2) The modifications, exceptions and exemptions provided for by regulations under subparagraph (1) may be in addition to, or in substitution of, any modifications, exceptions or exemptions specified in this Schedule before those regulations are made.

Interpretation of this Schedule

20. Interpretation.

In this Schedule –

"a provision of Part III" means –

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

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

"designated provision" means –

- (a) any provision of Part III of this Ordinance,
- (b) any provision of sections 4 to 10 this Ordinance corresponding to a right or duty in Part III of this Ordinance, or
- (c) section 35 of this Ordinance,

"educational data" means any personal data which –

- (a) is processed by or on behalf of the proprietor of, or a teacher at, a school,
- (b) relates to any person who is or has been a pupil at the school, and
- (c) originates from or is supplied by or on behalf of –
 - (i) a teacher or other employee at the school,

- (ii) an individual engaged by the proprietor of the school or working at a school under a contract for the provision of educational services,
- (iii) the pupil to whom the data relates, or
- (iv) a parent of that pupil,

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

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

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

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

- (a) means serious harm to the physical or mental health or condition of the individual, and
- (b) includes psychological or bodily injury, and

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

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

- (a) processed by the States of Guernsey Committee for Employment & Social Security or any other person in connection with the allocation of housing or other residential accommodation,
- (b) processed by the States of Guernsey Committee for Employment & Social Security in connection with the payment of supplementary benefit under the Supplementary Benefit (Guernsey) Law, 1971^s, or
- (c) processed by the States of Guernsey Committee for Health & Social Care in connection with the carrying out of its functions under the States Children Board and Public Assistance (Amendment) (Guernsey) Law, 1970^t.

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

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

THE STATES OF DELIBERATION
of the
ISLAND OF GUERNSEY

REQUÊTE

ASSISTED DYING

The States are asked to decide:-

Whether, after consideration of the Requête titled “Assisted Dying” they are of the opinion:-

To direct that:

1. The States agree in principle to the development of a suitable legal regime to permit assisted dying in Guernsey subject to and conditional upon:
 - a. the development of appropriate and effective capacity legislation and any other legislation which may be required; and
 - b. proposition 2.

2. The Policy & Resources Committee establish a working party with such membership as it sees fit and having consulted appropriately (for example, with members of the public, the Committees *for* Health & Social Care and Home Affairs, the Guernsey Disability Alliance, relevant UK bodies such as the British Medical Association) to report back to the States of Deliberation within 18 months with recommendations for a suitable legal regime, including consideration of *inter alia*:
 - a. the legal and professional obstacles required to be overcome in order to permit assisted dying in Guernsey;
 - b. whether it shall be a requirement that the individual is terminally ill and, if so, the means by which that shall be defined and determined;
 - c. whether it shall be a requirement that the individual shall physically administer the final act to themselves or whether it shall be permitted for others to assist;
 - d. whether there should be a requirement for individuals to be locally resident;
 - e. what measures are required to protect the vulnerable and prevent abuse of the legislation;
 - f. the numbers and roles of doctors under any proposed assisted dying legislation and whether they would be permitted to have any conscientious objection to an individual’s request; and

- g. the age at which an individual shall have capacity for purposes of consenting under the assisted dying legislation.
3. The Policy & Resources Committee liaise with the States of Alderney to consider whether and how the States of Alderney and the States of Guernsey could work together to minimise the duplication of effort necessary to consider the issues in order to develop a suitable policy and legal regime to permit assisted dying in both islands.

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

Requete

Assisted Dying

THE HUMBLE PETITION of the undersigned members of the States of Deliberation SHEWETH THAT:

1. At the September 2002 States' meeting, a Requete entitled 'Death with Dignity,' placed by the then Deputy Patricia Mellor and signed by thirteen other Members of the States of Deliberation, received majority support. Consequent to the States' resolution, the then Advisory and Finance Committee was instructed to:

"..carry out appropriate investigations and consultations with whomever it deems fit, and thereafter, but at the earliest opportunity, to bring a report to the States of Deliberation, on the implications of allowing Doctor Assisted Death or some other similar Death With Dignity Legislation to be implemented within Guernsey, and containing the Committee's recommendations in connection with this matter."

2. The Advisory and Finance Committee established the Death with Dignity Working Party under independent chairmanship to consider the social, legal, medical, ethical and spiritual issues. The Working Party investigated the position in a number of jurisdictions around the world, including those that permitted assisted dying at the time, such as the state of Oregon in the United States of America, the Netherlands, Belgium and Switzerland. The Working Party's report was passed to the Policy Council, as the successor to the Advisory and Finance Committee following the changes to the system of government in 2004.

3. The Policy Council presented a States Report¹ which stated:

"However, after careful consideration of the Working Party's report, the Policy Council, by a majority supports and recommends the majority view i.e. that there should be no change to the present legal position in order to support euthanasia in any form.

"The Policy Council further recommends that the Health and Social Services Department be directed to progress the Working Party's recommendations in the three associated issues detailed above, i.e.

- *the provision of palliative care;*
- *clarification of the position on advance directives, and*
- *clarification of the position on the proper use of double effect medication."*

4. A minority report of the Working Party produced by Deputy Peter Roffey and also endorsed by Deputies Hunter Adam and Francis Quin recommended that Guernsey should legislate to facilitate assisted dying, utilising a system similar to that in force at that time in the state of Oregon in the United States of America. The minority report recognised that if the States resolved to support assisted dying, in whatever form, there would be constitutional and legal issues that would require resolution before legislation could be drafted.

¹ 2004 Billet XVI, p 1401

5. Following debate in October 2004, including on an amendment laid by Deputy Peter Roffey that gave the States of Deliberation an opportunity to support the minority report, the States resolved to accept the Policy Council's recommendations.
6. In the intervening 14 years since that debate, the number of jurisdictions that permit assisted dying has increased, including the State of California, the State of Washington (2008), Canada (2016) and the State of Victoria (2017.) There have been several high profile legal cases heard in the UK, including that of Debbie Purdy, Diane Pretty and Tony Nicklinson that have tested the boundaries of the common law in England & Wales and the meaning of a right to private life, protected under Article 8 of the European Convention on Human Rights; and there have been several attempts by parliamentarians in Westminster to introduce permissive legislation, including Lord Joffe's 'Patient (Assisted Dying) Bill' (2003,) Lord Faulkner's Assisted Dying Bill (2014) and Rob Marris's private members' Assisted Dying Bill (2015). In the same period, society has continued to evolve in other matters of social policy and personal conscience. For example, the adoption and acceptance of equal marriage legislation would have been inconceivable in 2004. In the same period, Guernsey's international identity has continued to evolve, including the signing with Her Majesty's Government in the United Kingdom of the international identity framework agreement in 2009. Consequently, there is now a greater expectation that as a mature, independent jurisdiction, Guernsey is capable of fundamentally different policy and legal approaches to these highly sensitive issues, compared to the UK.
7. The Policy Council's proposals for capacity legislation were agreed by the States of Deliberation in November 2013, following consideration of its report on the Disability and Inclusion Strategy. At that time, the States agreed to direct the Health and Social Services Department to research and develop options for capacity legislation and report back to the States of Deliberation on this matter. Resource constraints and other higher priorities have meant that the requisite legislation has not yet been enacted although it is a priority of the Committee for Health & Social Care. It is recognised by your Petitioners that appropriate and effective capacity legislation is an essential pre-requisite to any legislation permitting assisted dying in order that it can be clearly determined who has the requisite capacity.
8. Your Petitioners take note that in December 2017, the States of Alderney debated without resolution the matter of assisted dying.
9. Your petitioners are of the view that individuals are entitled to a safe and peaceful death and accordingly mentally competent adults should have the right to seek assistance to ensure this outcome.
10. Subject to and conditional upon the adoption of appropriate and effective capacity legislation and any other legal or policy changes that may be necessary, it is the opinion of your Petitioners that, having regard to developments since 2004, it is now appropriate for Guernsey to adapt and adopt an assisted dying regime appropriate to the needs of the community.

THESE PREMISES CONSIDERED, YOUR PETITIONERS humbly pray that the States may be pleased to direct that:

1. The States agree in principle to the development of a suitable legal regime to permit assisted dying in Guernsey subject to and conditional upon:
 - a. the development of appropriate and effective capacity legislation and any other legislation which may be required; and
 - b. proposition 2.

2. The Policy & Resources Committee establish a working party with such membership as it sees fit and having consulted appropriately (for example, with members of the public, the Committees for Health & Social Care and Home Affairs, the Guernsey Disability Alliance, relevant UK bodies such as the British Medical Association) to report back to the States of Deliberation within 18 months with recommendations for a suitable legal regime, including consideration of *inter alia*:
 - a. the legal and professional obstacles required to be overcome in order to permit assisted dying in Guernsey;
 - b. whether it shall be a requirement that the individual is terminally ill and, if so, the means by which that shall be defined and determined;
 - c. whether it shall be a requirement that the individual shall physically administer the final act to themselves or whether it shall be permitted for others to assist;
 - d. whether there should be a requirement for individuals to be locally resident;
 - e. what measures are required to protect the vulnerable and prevent abuse of the legislation;
 - f. the numbers and roles of doctors under any proposed assisted dying legislation and whether they would be permitted to have any conscientious objection to an individual's request; and
 - g. the age at which an individual shall have capacity for purposes of consenting under the assisted dying legislation.

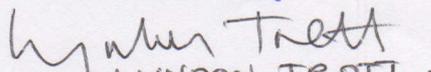
3. The Policy & Resources Committee liaise with the States of Alderney to consider whether and how the States of Alderney and the States of Guernsey could work together to minimise the duplication of effort necessary to consider the issues in order to develop a suitable policy and legal regime to permit assisted dying in both islands.

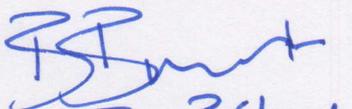
AND YOUR PETITIONERS WILL EVER PRAY

GUERNSEY

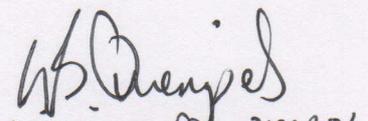
This 7th day of February 2018

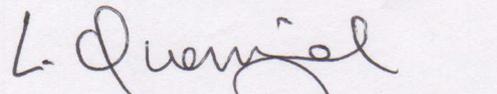

GAVIN S. PIER

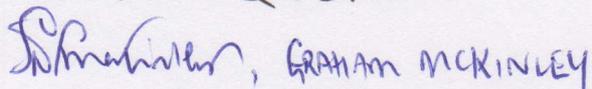

LYNDON TROTT

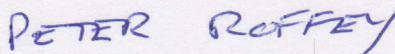

B. L. BREHAUT




LAURIE QUERIPPEL


LESTER QUERIPPEL


GRAHAM MCKINLEY


PETER ROFFEY