

STATES OF JERSEY



DRAFT DATA PROTECTION (JERSEY) LAW 201-

Lodged au Greffe on 5th December 2017
by the Chief Minister

STATES GREFFE



Jersey

DRAFT DATA PROTECTION (JERSEY) LAW 201-

European Convention on Human Rights

In accordance with the provisions of Article 16 of the Human Rights (Jersey) Law 2000, the Assistant Chief Minister has made the following statement –

In the view of the Assistant Chief Minister, the provisions of the Draft Data Protection (Jersey) Law 201- are compatible with the Convention Rights.

Signed: **Senator P.F. Routier, M.B.E.**

Assistant Chief Minister

Dated: 1st December 2017

REPORT

Introduction

We live and work in a digitally connected society, where the Internet has become a feature of everyday life, and where businesses and consumers rely on the ability to share and access personal data online, with confidence and clarity.

The protection of this personal data is essential for the protection of our human rights, particularly those accorded by Article 8 of the European Convention on Human Rights (i.e. the rights to private and family life, home and correspondence).

Personal data is the lifeblood of the financial services industry in particular, and as the digital economy develops and the use of online technology becomes ubiquitous, it is important that Jersey continues to provide a safe environment for processing data, with clear and robust data protection legislation that is monitored and enforced by an effective regulator.

Background and policy

Summary:

- The Data Protection (Jersey) Law 2005 sets out Jersey's current data protection regime.
- On 25th May 2018, the European Union's General Data Protection Regulation ("GDPR") and Law Enforcement Directive ("LED") will come into effect in EU Member States.
- The GDPR and LED will give people greater control over their data and require data controllers and processors to protect and use it appropriately.
- This new legislation will give people in Jersey equivalent rights in respect of their personal data to people in the EU.
- The GDPR and LED include restrictions on the transfer of personal data to third countries outside the EU, unless they have an adequacy decision.
- Jersey already has an adequacy decision for the purposes of the GDPR and the enactment of new data protection legislation is essential to maintain that status and achieve adequacy for LED purposes.
- Crucially, by maintaining essential equivalence with the EU ('adequacy'), the new legislation will also enable data to continue to flow uninterrupted between Jersey and Europe. This is important for all business sectors in Jersey.

The Current Data Protection Regime in Jersey

Jersey currently has a well-established data protection regime. The Island enacted its first data protection legislation in 1987, and has therefore long considered the need to provide robust assurances for personal data.

The Office of the Information Commissioner implements, and ensures compliance with, the current legislation, the Data Protection (Jersey) Law 2005 (the "2005 Law"). This piece of legislation was aligned with the relevant UK and EU laws, and the EU Commission issued a decision that the Island provides 'adequate' protection for personal data. This means that personal information can be shared freely between the EU and Jersey. This is important for all business sectors in Jersey.

The European context

The outgoing EU data protection regime (based on Directive 95/46/EC – the “Directive”) was introduced at a time when the Internet was in its infancy, and prior to the widespread adoption of e-mail and social media, or the rise of cloud computing or big data analytics. Further, in implementing the Directive, different EU member states have applied differing approaches, resulting in disparity between the various compliance regimes across Europe.

Given this disparity, the extent to which technologies have developed, and the ways in which people and businesses communicate and share information have changed, the EU has enacted 2 new pieces of legislation to modernise, standardise and increase the level of protection for personal data across the EU. The GDPR replaces the Directive for most purposes. In addition, the EU has enacted the LED, which is concerned with the protection of personal information processed for the purposes of policing and public protection.

To retain adequacy with the GDPR and assure adequacy with the LED, Jersey now has to introduce new data protection legislation that will provide ‘essentially equivalent’ protection to the GDPR and LED.

Jersey will also have to provide for an effective independent data protection supervisory body and co-operation mechanisms with European data protection authorities, as well as provide data subjects with effective and enforceable rights and administrative redress for breaches of those rights. This is provided for by the Draft Data Protection Authority (Jersey) Law 201- which has been lodged in parallel with this draft Law (*see* P.117/2017).

Engagement with the European Commission indicates that Jersey’s adequacy decision will be ‘grandfathered’ (i.e. it will continue in effect) until the jurisdiction is re-assessed (probably in 2020). However, putting new legislation in place for May 2018 remains a matter of urgency, as it reduces the risk of challenges to Jersey’s existing status. Failure to secure continued adequacy with the EU would likely have detrimental economic consequences, particularly to the financial services sector, which relies heavily on the unrestricted flow of personal data to and from EU member states (and elsewhere relating to EU citizens). Failure to update our data protection regime would also result in people in Jersey being afforded a lower standard of individual rights in respect of data than their European counterparts.

A summary of the most important changes introduced by the GDPR and LED

A brief summary of the most important requirements introduced by the GDPR is set out below.

In terms of new requirements, businesses and organisations processing personal data will be required to –

- i. provide better and more information about how they process personal data in a clearer and more accessible way;
- ii. evidence that they design and build new services and products from the earliest stage of development in a way that protects ‘privacy by design’ and default;
- iii. notify the local independent ‘supervisory authority’ of any data breach within 72 hours where that is feasible and notify the individuals concerned without undue further delay;
- iv. appoint a Data Protection Officer who will be responsible for ensuring compliance with the requirements of the GDPR where they conduct ‘large

scale' processing operations or 'systemic and regular monitoring' as part of their 'core activities'; and

- v. demonstrate that where individual consent is used as a basis for processing that consent was freely given, specific, informed and indicated by an affirmative action (e.g. the person must actively tick a box rather than untick one that has been pre-ticked).

The GDPR also confers additional rights on individuals including –

- i. an enhanced right of access to their personal data;
- ii. the right to withdraw consent to the processing of their data in a particular way and the right to erasure (or right to be forgotten as it is often referred to in the press) providing there is no legitimate reason for it to be retained by the data controller; and
- iii. a right to require the transfer of their personal data between service providers. This right to “portability”, will promote competition and remove barriers to entry to markets, is consistent with the principles of Jersey’s Digital Policy Framework.

The GDPR provides for the following tougher enforcement mechanisms to protect individuals –

- i. the new European Data Protection Board will be responsible for ensuring consistency in enforcement of the GDPR across the EU;
- ii. individual Member States will be required to continue to have their own Independent Supervisory Authority, and will need to ensure that it has robust enforcement powers; and
- iii. substantial fines; failure to comply with the requirements of the GDPR will leave businesses and organisations liable to much more significant fines. Serious breaches of the GDPR may result in a maximum penalty which is the greater of 20 million Euros or 4% of global annual turnover, or in less serious cases a maximum penalty which is the greater of 10 million Euros or 2% global annual turnover. (There is flexibility to go for lower fine schemes).

Why this legislation is essential

It is clear that new legislation is required if Jersey is to provide essentially equivalent protection for personal data to that set out in the GDPR and LED.

On 20th February 2017, the Assistant Chief Minister made a Ministerial Decision approving instructions to the Law Draftsman to repeal the Data Protection (Jersey) Law 2005 and to prepare new legislation that will replace it and set out the new powers, functions and funding arrangements for the data protection regulator.

This Law places privacy obligations on data controllers and processors and rights on data subjects that are equivalent to those imposed by the GDPR and LED.

Lodged in parallel with this Law is the Data Protection Authority (Jersey) Law 201- (the “Authority Law”) (*see* P.117/2017), which establishes and sets out the powers and functions of the new Data Protection Authority (the “Authority”), which will provide robust, effective and independent regulation of the requirements in this Law. The establishment of the Authority is essential to ensuring equivalent protection for personal data to that provided under EU law. The Authority Law reforms the governance and funding arrangements for the regulator to ensure that the Authority has sufficient guarantees of structural independence. It also provides the Authority with powers to investigate breaches of the law and impose effective and dissuasive sanctions for breaches of this draft Law.

The primary policy objectives of this Law and the Authority Law are to provide effective protection for personal data and maintain Jersey's adequacy under the new European regime. Where there is doubt as to whether a particular approach to the drafting would provide equivalent protection to that provided in the EU, the draft legislation closely reflects the GDPR and the LED. However, where there is scope to be flexible with the approach of our legislation in a way that might benefit Jersey, the legislation seeks to do so.

Research and consultation

Summary:

- The government undertook an extensive programme of research and consultation, commissioning expert advice, engaging closely with the Island's business community and opening dialogue with international stakeholders.
- The local business community is supportive of the government's policy goals. It recognises the criticality of consistency with the EU framework, as this will allow data to flow freely to between Jersey and EU Member States.

To inform policy development on data protection, the Chief Minister's Department and the Law Officers' Department conducted considerable analysis.

There were 2 principal work-streams comprised in the research project: one considered what was required for Jersey's data protection regime to continue to be deemed adequate by the EU Commission; the other assessed what the Island could do above and beyond to gain a competitive advantage. To inform this second work-stream, the Chief Minister's Department commissioned specialist researchers to review what opportunities there might be in how the Island implemented new data protection legislation. The outcomes of this consultancy have informed the policy development and the law drafting instructions for both pieces of legislation.

In developing the policy and drafting the legislation, the government has engaged widely with stakeholders across Jersey and internationally.

International Engagement

With the assistance of the Channel Islands Brussels Office, the government has engaged with officials from the European Commission to begin the process of renewing the adequacy decision. A pan-Island delegation met with representatives from the Directorate-General for Justice in February 2017. This was well-received by the Commission, which was positive about Jersey's data protection regime and approach to the new legislation and was supportive of the Island's commitment to continued adequacy.

The Government of Jersey has also engaged with other third countries that are currently considered adequate by the European Commission and are updating their legislation to ensure continued adequacy. There has been positive dialogue with New Zealand and Canada, where officers have sought to share best practice.

Throughout the process, the Government of Jersey has engaged closely with the UK. Whilst it is still a member of the EU, the UK will be implementing the GDPR as an EU Member State. The UK Government has introduced a draft Data Protection Bill to the House of Lords in September 2017, to address aspects of the GDPR where it has scope to derogate and to implement the LED. The UK has indicated that it intends to maintain parity with EU data protection standards after Brexit, and that it will be looking to ensure that data can continue to flow freely between the EU and UK after Brexit, which may be achieved through seeking an adequacy decision like Jersey's.

Local Stakeholder Engagement

During the process there has been close engagement with stakeholders. Clear policy and drafting guidelines were set out in early conversations and have been adhered to. These guidelines were welcomed by industry.

The business community has been supportive of Jersey's policy goals. It recognises the critical importance for businesses in Jersey of maintaining the 'adequacy' decision from the EU Commission as this enables the free flow of data to and from the Island from residents of EU member states.

A programme of industry engagement has been conducted, including a series of roundtables and workshops, news releases and industry updates. There have been regular updates to key stakeholder groups including the Jersey Financial Services Commission, Jersey Finance, Digital Jersey and Jersey Business.

The draft Law and the Authority Law were reviewed by an expert stakeholder group with representatives from the financial services sector, legal services, the digital economy and public bodies in August and September 2017. There were 18 written and 2 verbal submissions to this expert consultation. The information gained from these responses was complemented by feedback from around 50 participants at 2 stakeholder events in October 2017 and a submission from the Office of the Information Commissioner. The consultation feedback was constructive, often focussing on highly technical elements, and has helped improve the legislation. A key theme of the feedback was to ensure data controllers and processors have clarity as to what is required. Another theme was that government should, where possible, avoid gold-plating the new EU regime by placing any additional burdens on business through our own legislation.

Also of critical importance was the protection of Jersey citizens and their personal and sensitive data. Through this legislation Jersey residents will be as well protected as EU citizens.

Data Protection (Jersey) Law 201-

Summary:

- The Data Protection (Jersey) Law 201- ensures that Jersey legislation offers an equivalent level of data protection to the EU framework. Jersey residents will enjoy equivalent rights over their data as their European counterparts.
- The Data Protection (Jersey) Law 201- introduces new requirements on data controllers and processors to ensure they secure and use personal data appropriately.
- Wherever possible, legal definitions have remained unchanged from the 2005 Law. This allows businesses and public bodies to build upon existing compliance structure and staff training.

The draft Law has been drafted to ensure that Jersey legislation offers an equivalent level of protection to the GDPR and LED. In doing so, it confers new duties on data controllers and processors and bolsters the rights of individuals in relation to their personal data. Some of the key elements of the new legislation are:

Accountability

Going forward, controllers and processors will be required to be more accountable for the ways in which they process personal data, including by preparing records of their processing activities and implementing appropriate technical and organisational measures to comply with the draft Law. Controllers will in particular be required to

consider data protection standards when developing new systems, and to carry out data protection impact assessments, ensuring that they protect data subjects' rights. Data controllers must also ensure that personal data is only processed to the extent necessary for the purposes for which it is processed.

Consent

The rules for obtaining consent to process data have been strengthened. Consent must be specific, auditable and the request must be in a clear and accessible form. Consent must also be as easy to withdraw as it is to give it.

Children

The draft Law introduces the age of 13 as the digital age of consent at which children may give effective consent to the processing of their data by online services, such as social media sites, including Twitter or Facebook. Below that age, valid consent to the processing of a child's data may be given by a parent or guardian on the child's behalf.

There is no universal standard on what age *precisely* constitutes the digital age of consent. The GDPR allows EU Member States to set their own digital age of consent within a window from 13 years of age to 16.

The United Kingdom, Ireland, the United States and many European countries have set their digital age of consent at 13. The age of 13 is viewed as appropriately balancing the right and need to participate online with ensuring appropriate parental protection.

For these reasons, the legislation establishes a digital age of consent of 13 years.

Processors

A difference between the 1995 Directive and the GDPR is that the former placed direct compliance obligations only on data controllers, whereas the latter applies to the processing of personal data by a controller or a processor that falls within the scope of the GDPR. Data processors therefore have to abide by new compliance obligations providing equivalent protection to the GDPR and LED.

Breach notification

In the event of a data breach, the Authority must be informed within 72 hours and any relevant affected individuals informed as soon as possible. Data processors must inform their customers, the data controllers, of any data breach they become aware of without undue delay.

Right of Access

Data subjects can obtain from data controllers confirmation as to whether or not personal data is being processed, where and for what purpose. The controller must provide a copy of the personal data, free of charge, in an electronic format.

Right to be forgotten

A data subject is entitled to have the data controller erase his or her personal data and cease further dissemination.

Data portability

A data subject has the right to receive personal data concerning them and transmit this to another controller.

The effect of each Part of the Data Protection (Jersey) Law 201- is briefly summarised below:

Part 1 – Introductory

Key definitions are found in Part 1. Definitions form the building blocks of the GDPR, the LED and the previous Jersey legislation. Where appropriate, definitions have remained unchanged from the 2005 Law to allow businesses and public bodies to build upon existing compliance structure and staff training. However, for Jersey to retain its adequacy decision it is essential that the Jersey legislation adheres closely to the GDPR and LED including in reflecting changes that have been made to these definitions compared to the 1995 Directive. Given this, where necessary, the definitions in the draft Law have an equivalent effect to the definitions used in the GDPR (and where relevant the LED).

As well as harmonising rules inside the EU, the GDPR also claims extraterritorial effect over the processing of personal data taking place outside of the EU. In terms of application, the draft Law claims a wide territorial jurisdiction similar to that claimed by the GDPR. This is in order to provide equivalent protection to Jersey residents who would not be data subjects in the EU.

Part 2 – Fundamental Duties of Controllers

Part 2 of the draft Law sets out the fundamental obligations for data controllers. They include their obligation to comply with the Data Protection Principles, the obligation to ensure appropriate safeguards for the rights of data subjects are put in place by design and default, record-keeping obligations, the obligation to report a data breach in the manner by the Law, the obligation to appoint a data protection officer, the obligation to pay the appropriate charges to the Authority, the obligation to co-operate with any requests of the Authority under this Law or the Authority Law, and to comply with any order of the Authority under the Law or the Authority Law.

Article 8 in Part 2 sets out the data protection principles, as it is the responsibility of the controller to ensure that the processing of personal data complies with the data protection principles, namely that data are –

- i. processed lawfully, fairly and in a transparent manner in relation to the data (“lawfulness, fairness and transparency”);
- ii. collected for specified, explicit and legitimate purposes and, once collected, not further processed in a manner incompatible with those purposes (“purpose limitation”);
- iii. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (“data minimization”);
- iv. accurate and, where necessary, kept up to date. Reasonable steps are taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay (“accuracy”);
- v. kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the data are processed (“storage limitation”); and
- vi. processed in a manner that ensures appropriate security of the data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures “integrity and confidentiality”).

The position of joint data controllers changes under the draft Law as joint data controllers are all liable to the data subject unless they prove they had no responsibility for damage.

Part 3 – Other Duties of Controllers

This Part sets out the other duties of controllers. Some of the key changes to the previous legislation are –

- The introduction of the concept of data protection by design and default.
This reflects the requirement under the GDPR that data protection principles and appropriate safeguards should be taken into account in both the planning phase of any processing activities and the implementation phase of any new product or service. For example, the controller must implement appropriate security measures for any data processed and give effect to the rights of data subjects. In reality, this means that controllers should consider the entire life-cycle of the relevant processing activities and plan for foreseeable uses of the new technology, product or service that may affect the data protection rights of data subjects.
- The requirement for Data Protection Impact Assessments for high risk processing.
The GDPR introduces the need for controllers to prepare Data Protection Impact Assessments for high-risk processing. The main objectives of these are to assess the privacy risks to individuals related to a proposed data processing activity and to identify measures to assess these risks and demonstrate compliance with the Law. If a Data Protection Impact Assessment indicates that the processing is too high-risk and that this risk cannot be mitigated, then the controller will be required to consult the Supervising Authority. In practice, Data Protection Impact Assessments provide a tangible tool to which a controller can point in order to demonstrate that it takes the privacy concerns of data subjects seriously and that it has taken steps to appropriately address these concerns. The draft Law gives some more guidance to controllers as to the circumstances that they will be required to undertake a Data Protection Impact Assessment and also requires the Authority to publish Codes of Practice.
- The need for prior consultation for high-risk processing.
The draft Law requires that where a data protection impact assessment indicates that any processing would pose a substantial risk to the significant interests of data subjects (which hasn't been mitigated by the controller), the controller must consult the Authority before commencing the processing. The draft Law sets out the manner in which the controller must do this, and also the process that the Authority must follow (and the timescale it needs to keep to), if it is of the opinion that the proposed processing would be in breach of provisions of the new Law.
- The requirement for prior consultation for high-risk legislation.
The GDPR requires Member States to consult their supervisory authority during the preparation of a proposal for new legislation to be adopted by the national parliament, or on a regulatory measure based on such a legislative measure, which is related to processing. This is very wide, and while fulfilling the need to give equivalent protection to the GDPR, the draft Law adopts a practical approach to this provision. Article 18 provides that consultation is required only where a Law or secondary legislation proposed; or Act that would be extended, taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedom of natural persons. The approach taken is designed to reinforce the

approach to Data Protection Impact Assessments and to ensure that the Authority is not needlessly consulted on a wide range of low-risk processing arrangements.

- Breach reporting.

One of the high-profile obligations introduced by the GDPR is the need for controllers to report a breach to the Authority and, in certain cases, affected data subjects. This assists the Authority in performing its supervising functions, and enables affected data subjects to take measures to mitigate any risks associated with the breach (e.g. cancel credit cards). In practice, they are likely to motivate controllers to implement robust security measures to minimise the risk of data breaches and the associated reputational harm.

These requirements reflect the requirements of the GDPR and are necessary for continued adequacy.

Parts 4 – Joint Security Duty and Duties of Processors

The draft Law, like the GDPR and LED, places obligations on controllers and processors to take proportionate organisational and technical measures to ensure that personal data is kept securely. Such measures may include the adoption of appropriate policies for staff and the deployment of appropriate software to protect against ‘malware’.

Importantly, the draft Law also introduces new obligations on data processors. A data processor is any entity that processes personal data under the controller’s instructions. (For example, many cloud service providers are processors.) This is a key difference from the 2005 Law.

The change stems from the change in the European approach. Unlike the 1995 Directive, which generally placed direct compliance objectives on controllers and asked them to flow these to processors through contractual obligations, the GDPR imposes direct compliance obligations on processors as well as controllers. It also enables enforcement action to be taken against them by the supervisory authorities and for fines, penalties and compensation claims to be imposed or made for failure to satisfy those requirements. The GDPR also explicitly states that a processor will be considered a joint controller in the event that it processes personal data other than in accordance with the instructions of the controller. This has also been reflected in the draft Law.

Parts 5 – Data Protections Officers

To offer equivalent protection to the GDPR, Article 24 of the draft Law sets out the circumstances under which a controller or processor must appoint a Data Protection Officer (a “DPO”). A DPO must be appointed when –

- processing is carried out by a public authority (*except* for the courts acting in their judicial capacity);
- the core activities involve systemic monitoring on a large scale;
- its core activities involve large scale processing of sensitive data; or
- it is required by the relevant law.

To offer greater clarity and to avoid placing an insupportable burden on businesses, the draft Law also sets out the circumstances where a single DPO might be appointed for a group of undertakings or several public authorities. It also makes it clear that the DPO must operate independently and report to the highest management of the business. Articles 25 and 26 give clear detail on the position and duties of the DPO.

Part 6 – Rights of Data Subjects

One of the main effects of the GDPR is to confer greater rights on data subjects. These rights are broad in the GDPR, Article 23 of the GDPR providing Member States with extensive latitude to place restrictions on these rights where that is necessary for a number of purposes. Many of these rights are already provided for in the Data Protection (Jersey) Law 2005, and the draft Law draws on these where possible to give continuity to data subjects and controllers and processors. In effect, the draft Law greatly strengthens the rights of data subjects (to reflect the scale of data currently being used and the potential impact of inappropriate processing) while balancing this with the need for businesses and organisations to be able to process data under appropriate circumstances.

Under the new Law, data subjects are entitled –

- to receive certain minimum information from the controller about the processing of their data and a copy of the data itself (the ‘right of access’);
- to have their personal data erased without undue delay under certain circumstances (known colloquially as ‘the right to be forgotten’);
- the rectification of inaccurate personal data concerning him or her or to have incomplete personal data completed;
- to have their personal data erased under certain circumstances, including where the personal data are no longer necessary, or when they have withdrawn consent and there is no other legal ground for processing (known colloquially as ‘the right to be forgotten’);
- to obtain from the controller restriction of processing where specific circumstances apply;
- to have the ‘right to data portability’, in other words to receive personal data concerning them in a structured, commonly-used and machine readable format (this is to assist with ‘switching’ controller);
- to object to processing; and
- not to be subject to a decision based solely on automated processing when it has a legal effect or other significant effect on the data subject.

Part 7 – Exemptions

Jersey has some flexibility to adopt exceptions in our legislation both from the rights of data subjects and from the obligations of data controllers and processors. The approach taken seeks, where possible, to replicate the existing exemptions in the current domestic legislation, for example in maintaining broadly the same approach to academic, journalistic, literary and artistic material. The *status quo* is also broadly maintained for national security, which continues to be generally exempt from the requirements of the new Law in most cases.

The draft Law includes an exemption from the transparency and subject rights provision to the extent required to avoid an infringement of the privileges of the States Assembly. The United Kingdom has a similar exemption in its draft data protection legislation to avoid infringement on the privileges of the Houses of Parliament.

A certificate signed by the Greffier of the States to that effect is evidence of the fact an exemption is required. The decision of the Royal Court is final in relation to any appeal submitted in relation to the Greffier’s decision. The Jersey exemption mirrors similar provisions in the Freedom of Information (Jersey) Law 2011.

The draft Law also brings forward the existing Trusts exemption which is crucial for Jersey's financial services sector.

Part 8 – Cross-Border Data Transfers

The draft Law puts in place equivalent restrictions to those in the EU with regard to the transfer of personal data to third countries outside the EU.

International co-operation is an important tenet of international data protection regulation. The GDPR obliges the European Commission and Supervisory Authorities to take appropriate steps to develop international co-operation mechanisms to facilitate effective enforcement of legislation for the protection of personal data, including by providing for mutual assistance with enforcement.

Given the uncertainty as to the types of international co-operation mechanisms that might be required in the future, the draft Law and the draft Authority Law provide Regulation-making powers to enable appropriate provision to be made in the future.

Part 9 – Remedies and Enforcement

The draft Law and the draft Authority Law give data subjects, controllers and processors rights to bring complaints and seek judicial remedies. There is a right of appeal against the regulator's decisions in respect of complaints and notices or determinations provided for in the Authority Law. This right to appeal does not extend to the exercise of the regulator's advisory functions.

The offences the draft Law brings forward are –

- the offence of unlawfully obtaining personal data in Article 71 of the draft Law (previously set out in Article 55 of the 2005 Law);
- the offence of requiring a person to produce certain records in Article 72 of the draft Law (previously set out in Article 56 of the 2005 Law);
- the offence of providing false information set out in Article 73 of the draft Law (previously set out in Article 60 of the 2005 Law); and
- the offence of providing obstruction set out in Article 74 of the draft Law (previously set out in paragraph 13 of Schedule 9 to the 2005 Law, but now expanded to capture failure to comply with an information notice).

Under the draft Law most offences are punishable with a fine, except where expressly provided.

Part 10 – Miscellaneous

This includes a number of Regulation-making powers to ensure that the Law remains future-proofed.

Article 83 enables the States to prescribe by Regulations when information can be disclosed to improve public service delivery.

Data is a vital asset for enabling efficient government. The effective and secure use of data can enable the making of better policy and delivery of more responsive public services. For example, frontline staff can use data to ensure that people get the right support to meet their needs.

There are numerous examples where appropriate data sharing could improve outcomes for customers. These include, but are not limited to –

- data analytics for performance monitoring;
- data analytics for policy development;
- data mining to determine eligibility for benefits and services;

- data matching to identify benefit fraudsters and non-compliant tax cases;
- data matching to identify potentially at-risk school-aged children who are in the Island but not attending school;
- personal and business customer ‘Tell Us Once’ services
- sharing data with the Parishes and third parties (e.g. G.P.s); and
- making anonymised publishable data available, enabling third parties to design solutions for Islanders.

Article 84 of the draft Law enables Regulations to constitute an Information Board to oversee, co-ordinate and develop a clear framework for the sharing of data across government.

The Information Board will comprise senior figures from several departments. It will set the agenda for effective data sharing and ensure that the organisation meets legal requirements for privacy and security.

Initiatives that the Information Board could pursue may include the following –

- encouraging public authorities to focus on data sharing and security;
- promoting the ability of customers to see, amend and control data held by public authorities;
- acting as the liaison between public authorities and the Information Commissioner; and
- ensuring that departments, parishes and other public authorities use common/enterprise data assets.

The Information Board will also promote principles for using data across the organisation. These may include –

- applying the citizen-first approach;
- minimising bureaucracy and enabling efficiency across departments;
- balancing operational efficiency with data privacy requirements;
- following the principles of ‘Tell Us Once’;
- protecting data, recognising that it is a vital asset;
- using data proactively (e.g. eligibility for benefits or ability to detect and pursue fraud) rather than waiting for an application;
- ensuring audit functionality and compliance; and
- promoting Information Governance with a view to taking on more responsibility in the future.

Schedule 1

Schedule 1 modifies the application of the Law where the processing of personal data is carried out by a controller that is a competent authority for a law enforcement purpose.

The draft Law defines a competent authority as one which processes personal data for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties.

A list of competent authorities is included in Schedule 1.

Collective responsibility under Standing Order 21(3A)

The Council of Ministers has a single policy position on this proposition, and as such, all Ministers, the Assistant Chief Minister acting as *rapporteur*, and the Assistant Chief Minister for eGov and Digital Jersey, are bound by the principle of collective responsibility to support the proposition, as outlined in the Code of Conduct and Practice for Ministers and Assistant Ministers ([R.11/2015](#) refers).

Financial and manpower implications

Summary:

- There are no financial implications arising from the Data Protection (Jersey) Law 201-.

There are no financial implications arising from the adoption of the Draft Data Protection (Jersey) Law 201-.

Departments and other administrations of the States that fall under the remit of the Draft Data Protection (Jersey) Law 201- will be required to meet the enhanced levels of regulation in the same way that private sector businesses will. It is expected, however, that any additional resource requirements, over and above those needed under the existing Law, will be met from existing budgets.

Timetable for implementation

The government aims to enact the legislation at the same time as the new EU framework comes into force. This will provide certainty and consistency for citizens, businesses and public authorities. Given the relationship between the draft Law and the draft Authority Law – the government needs to enact both pieces of legislation to the same timetable.

Proposed timetable –

- December 2017 – legislation lodged for debate by the States Assembly
- January 2018 – legislation debated by the States Assembly
- February 2018 – legislation sent for Royal Assent
- 25th May 2018 – legislation comes into force.

Human Rights

The notes on the human rights aspects of the draft Law in the **Appendix** have been prepared by the Law Officers' Department and are included for the information of States Members. They are not, and should not be taken as, legal advice.

Human Rights Notes on the Draft Data Protection (Jersey) Law 201-

These Notes have been prepared in respect of the Draft Data Protection (Jersey) Law 201- (the “**draft Data Law**”) by the Law Officers’ Department. They summarise the principal human rights issues arising from the contents of the draft Data Law and explain why, in the Law Officers’ opinion, the draft Data Law is compatible with the European Convention on Human Rights (“**ECHR**”).

These notes are included for the information of States Members. They are not, and should not be taken as, legal advice.

The draft Data Law, together with the Draft Data Protection Authority (Jersey) Law 201- (the “**draft Authority Law**”) will replace the existing Data Protection (Jersey) Law 2005 (the “**2005 Law**”) with a new data protection regulatory regime that implements the General Data Protection Regulation 2016/679 (the “**GDPR**”) and the associated Directive, the Law Enforcement Directive (Directive (EU) 2016/680 (the “**LED**”).

The purpose of the draft Data Law is to make provision setting out the duties on controllers and processors and the rights of individuals in respect of their personal data. The draft Authority Law sets out the constitution, functions and powers of the new Data Protection Authority (the “**Authority**”), which will regulate compliance with the draft Data Law.

The draft Data Law engages 3 rights under the ECHR. The right to a fair trial in Article 6 of the ECHR, the right to private and family life in Article 8 ECHR and the right to freedom of expression in Article 10 of the ECHR.

The issues in respect of each of these rights and the reasons why the draft Data Law is compatible with them are set out below.

Article 6 ECHR – The right to a fair trial

Article 6(1) ECHR provides –

“In the determination of his civil rights and obligations or of any criminal charge against him, everyone is entitled to a fair and public hearing within a reasonable time by an independent and impartial tribunal established by law. Judgment shall be pronounced publicly but the press and public may be excluded from all or part of the trial in the interests of morals, public order or national security in a democratic society, where the interests of juveniles or the protection of the private life of the parties so require, or to the extent strictly necessary in the opinion of the court in special circumstances where publicity would prejudice the interests of justice.”

Article 6(1) ECHR requires that those who face a determination of their ‘civil rights and obligations’ must be entitled to a ‘fair and public hearing ... by an independent and impartial tribunal’. The guarantees afforded by Article 6 of the ECHR will only be relevant to the extent that an act or a decision is determinative of a ‘civil right’ or ‘obligation’.

The human rights memorandum in respect of the draft Authority Law deals with the Article 6(1) implications of regulatory decision-making by the Authority. That

memorandum sets out how such decisions may determine civil rights, but that the ability to bring proceedings or an appeal to the Royal Court in respect of the Authority's decision making ensures that the requirements of Article 6(1) of the ECHR are met.

The provisions of the draft Authority Law work in harmony with the draft Data Law, Articles 68 and 69 of which provide a method for a person to enforce the obligations of data controllers and processors without recourse to the Authority. These Articles provide the right to bring proceedings before the Royal Court for a contravention of the controllers' or processors' obligations in the draft Data Law and for compensation in respect of a contravention. The provision of 2, essentially parallel enforcement mechanisms, an independent regulator and access to a court, is a requirement of the GDPR and the LED.

For the purposes of Article 6 of the ECHR, the determination of any complaint of a breach of the rights or obligations afforded by the draft Data Law or for compensation will amount to the determination of a civil right for the purposes of Article 6 ECHR. The ability to bring proceedings in the Royal Court is sufficient to ensure that these civil rights and obligations are determined in a manner that is compatible with Article 6 of the ECHR.

Article 8 ECHR: Right to respect for private and family life

Article 8 of the ECHR provides –

“Everyone has the right to respect for his private and family life, his home and his correspondence.

There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.”

The European Court of Human Rights (“**ECHR**”) has held that the protection of personal data is of fundamental importance to a person's enjoyment of his or her right to respect for private and family life, as guaranteed by Article 8 of the ECHR. States are obliged to enact domestic law that affords appropriate safeguards to prevent the use of personal data in a way that would be inconsistent with Article 8 ECHR, particularly where that personal data is held for law enforcement purposes. The domestic law should ensure that such data are relevant and not excessive in relation to the purposes for which they are stored; and preserved in a form which permits identification of the data subjects for no longer than is required. Domestic law must also afford adequate guarantees that retained personal data are efficiently protected from misuse and abuse.

The draft Law fulfils these obligations by putting in place controls on the use of personal data generally and, in particular, by putting in place special controls on the use of personal data by a controller who is a competent authority (meaning either a body listed in that Schedule or with law enforcement functions) that is processing data for a law enforcement purpose.

Four areas of the draft Data Law warrant particular attention from an Article 8 ECHR perspective –

- The protection of criminal records data;
- Exemptions;

- Processing conditions for special category data; and
- Cross-border data transfers.

Each of these aspects of the draft Law is considered in more detail below to explain why the draft Data Law is compatible with Article 8 of the ECHR.

The protection of criminal records data

In addition to the particular controls on the use of personal data by competent authorities, the draft Data Law puts in place appropriate offences to prevent personal data and special categories of data from being inappropriately obtained and misused. An example of this is the enactment of the offence in Article 72 of the draft Data Law. That Article will, except in very limited circumstances, make it an offence for an employer or service provider to require a person to supply the outcome of a subject access request for his or her criminal record in connection with the person's employment or as a condition of the provision of a service.

The absence of sufficient safeguards in the system for the retention and disclosure of criminal record data, so as to ensure that data relating to the applicant's private life would be disclosed only where that is proportionate to a legitimate aim, may amount to a breach of Article 8 of the ECHR. Article 72 of the draft Data Law, in combination with the existing controls on the disclosure of such information in the Police Act 1997 as extended to Jersey and the Rehabilitation of Offenders (Jersey) Law 2001 ensures that sufficient safeguards are in place.

Exemptions

Part 7 of the draft Data Law includes a number of exemptions from the rights given to data subjects in the draft Data Law. Exceptions from certain rights of data subjects and obligations of controllers provided for under the draft Data Law could result in an interference with the rights of individuals provided for under Article 8(1) of the ECHR. However, in each case the exemptions can be justified on the basis that the interference is in accordance with the Law and is proportionate in pursuit of one or more of the legitimate aims set out in Article 8(2) of the ECHR.

One important example of this is Article 41 of the draft Data Law, which provides for exemptions from the rights and obligations provided for in the draft Data Law in so far as this is necessary for the purpose of safeguarding national security. The approach in the draft Data Law to the national security exemption will replicate the existing position under Article 28 of the 2005 Law, and therefore the draft Law will not be creating any greater interference with a person's ECHR rights. In any event, the approach in Article 41 of the draft Data Law provides appropriate safeguards on the application of this exemption. In particular, Article 41(4) of the draft Data Law provides the opportunity to challenge a certificate conferring the benefit of this exemption, issued by the Minister for Home Affairs under Article 41(2), in the Royal Court. This right to challenge ensures that the interference with the Article 8 ECHR rights of data subjects can be justified as proportionate to the legitimate aim of protecting national security for the purposes of Article 8(2) of the ECHR.

It should also be noted that the Article 41 exemption is consistent with the Council of Europe's Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data ("**Convention 108**"), Article 9 of which permits derogation from principles of processing and safeguarding provided for under Convention 108, including for the purposes of safeguarding national security.

Special category data

The draft Data Law defines ‘special category data’ under Article 1(1) of the draft Data Law. In view of the impact that the processing of such data may have on the rights of individuals, the processing of special category data is restricted by Article 9(2) of the draft Data Law in order to protect the rights of individuals under Article 8 of the ECHR. In particular, the processing of special category data will only be lawful for the purposes of the draft Data Law where the processing is for a purpose set out in Part 2 of Schedule 2 to the draft Data Law.

The purpose set out in Part 2 of Schedule 2 to the draft Data Law have, in most respects, been brought forward from the 2005 Law and the Regulations made under it, which have been consolidated into the draft Data Law. These purposes reflect Article 8(2) of the ECHR and any potential interference with the right to a private and family life that may arise from the processing of special category data pursuant to these provisions of Schedule 2 may be justified as being in accordance with the law and proportionate to one of the legitimate aims set out in Article 8(2) of the ECHR.

Cross-border data transfer exceptions

Part 8 of the draft Law provides for restrictions on cross-border data transfers. Article 66(2)(c) of, and Schedule 3 to, the draft Data Law provide for derogations from these restrictions. Further, Article 66(3)(b) enables the States Assembly (the “**Assembly**”) to specify by Regulations further derogations from these restrictions.

The cross-border transfer of personal data, particularly to countries that may not afford all of the same protections for personal data has the potential to interfere with the rights afforded by Article 8 of the ECHR.

The derogations in Schedule 3 to the draft Data Law are brought forward from Schedule 3 to the Data Protection (Jersey) Law 2005 (the “**2005 Law**”). These derogations are limited to circumstances where the individual consents to the transfer or there would be a legitimate aim pursued by the transfer. For example, paragraph 4 of Schedule 3 to the draft Data Law enables overseas transfers of personal data by the JFSC for reasons of substantial public interest to help combat financial crime.

In exercising this Regulation-making power, the States could provide further grounds for transfers of personal data to third countries and international organisations, which could result in interferences with the Article 8 ECHR rights of data subjects. Accordingly, the power to make Regulations should be exercised in such a way as to ensure that any derogation from the restrictions on cross-border transfers is limited to circumstances that would be proportionate to a legitimate aim set out in Article 8(2) of the ECHR.

Therefore the provisions in respect of cross-border transfers are compatible with Article 8 of the ECHR.

Article 10: Freedom of expression

Article 10 of the ECHR provides –

- “(1) Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers. This article shall not prevent States from requiring the licensing of broadcasting, television or cinema enterprises.*
- “(2) The exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions,*

restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary.”

Like Article 8(2) of the ECHR mentioned above, Article 10(2) ECHR provides that an interference with the right to freedom of expression is permitted where it is in the interests of, amongst other things, the protection of the rights and freedoms of others. In principle, an interference with a person’s Article 10(1) ECHR rights would be justified so long as the interference is in accordance with law and is no more than what is proportionate to this legitimate aim.

There is the potential for conflict to arise between the rights in Articles 8 and 10 of the ECHR in respect of the protection of personal data. In particular, this may arise where personal data or special category data are processed, including by being published, by journalists. Recital 153 and Article 85 of the GDPR require EU Member States to make provision in their domestic law to reconcile the rights to the protection of personal data with the right to freedom of expression.

Article 44 of the draft Data Law balances these rights by providing for an exemption from the requirements of the draft Data Law where personal data are processed for academic, journalist, literary or artistic purposes with a view to publication, and publication would be in the public interest. For these purposes the public interest must outweigh the rights of any individual in the protection of that individual’s personal data.

The limits imposed on the ability to rely on the exemption in Article 44(1) of the draft Data Law mean that the exemption from the privacy rights is only activated when necessary for publication and that publication is reasonably considered to be in the public interest. The exemption therefore provides an appropriate mechanism to balance the right to privacy and the right to freedom of expression.

Further, Articles 67 and 68 (proceedings against controllers and compensation) continue to apply to the exempt types of processing under Article 44, providing remedies to data subjects and persons who suffer loss, damage or distress due to a contravention of the Law.

The draft Data Law is therefore compatible with Article 10 of the ECHR.

Explanatory Note

This Law repeals and replaces the Data Protection (Jersey) Law 2005 with provisions to protect the rights of individuals in relation to their personal data, and provide for the free movement of personal data, in a manner equivalent to and consistent with the General Data Protection Regulation (Regulation (EU) 2016/679 (“the GDPR”) and an associated Directive, the Law Enforcement Directive (Directive (EU) 2016/680.

Further compliance with the Regulation is provided by a related Law, the Data Protection Authority (Jersey) Law 201- (P.117/2017) (“the Authority Law”). Broadly, this Law is concerned with the duties on controllers and processers and the rights of individuals in respect of their personal data. The Authority Law is concerned with the constitution and functions of the new Data Protection Authority (“the Authority”) and sets out its regulatory powers and the obligations on controllers or processors to register with the Authority.

Part 1 – Introductory

Article 1 of this Law contains most of the interpretative provisions, in particular the meaning of “data”, “controller” and “processor”, the controller being the person who determines the purposes and means of processing. *Article 2* defines “personal data” as meaning any data relating to a data subject and “data subject” is defined, in summary, as an identified natural, living person. The word “pseudonymization”, the means of processing personal data in a manner so that further information kept separately is needed to identify the particular data subject, is fully defined in *Article 3*.

Article 4 is the application provision. It excludes from this Law the processing of personal data by a natural person in the course of a purely personal or household activity. The Law applies to the processing of personal data where the controller or processor is established in Jersey, or if not so established, uses equipment in Jersey (in which case a representative established in Jersey must be appointed) or processes personal data relating to Jersey-based data subjects or for the purposes of offering them goods or services. The Article explains what is meant by “established in Jersey”, relying on EU terminology.

Article 4 also introduces *Schedule 1* which modifies the Law where processing of personal data is carried out by a controller who is a competent authority (meaning either a body listed in that Schedule or otherwise exercising a law enforcement purpose in Jersey other than the security services) for a law enforcement purpose. The Schedule therefore gives effect to the Law Enforcement Directive referred to above which is in effect a variation of the GDPR for law enforcement purposes. These purposes are defined in *Article 1* and relate broadly to functions concerned with criminal justice or threats to public security.

Article 5 states that if the purposes for which a controller processes personal data do not require the identification of a data subject, the controller does not have to maintain, acquire or process additional information to identify the data subject. Where and while the controller can no longer identify the data subject, *Articles 28 to 34* do not apply.

Part 2 – Fundamental duties of controllers

Article 6 lists, by reference to provisions elsewhere in the Law and in the Authority Law, the main duties and accountability of controllers.

Article 7 sets out the particular arrangements that apply where 2 or more controllers jointly determine the purposes and means of the processing of personal data.

Article 8 sets out the GDPR's 6 data protection principles, namely –

- (a) lawfulness, fairness and transparency;
- (b) purpose limitation;
- (c) data minimization;
- (d) accuracy;
- (e) storage limitation;
- (f) integrity and confidentiality.

Lawful processing is further explained in *Article 9*, which requires personal data to meet one of the conditions set out in *Schedule 2*. In the case of special category data, one of the conditions in *Part 2 of Schedule 2* must be satisfied. Special category data is defined in *Article 1* as data concerning matters such as race, political or religious beliefs, trade union membership, genetic, biometric or health-related data and sexual and criminal matters.

Article 10 makes further provision in relation to determining the fairness of processing personal data and the obligations of the processor in relation to fair and transparent processing.

Article 11 sets out the requirements for establishing consent to processing. In particular, a child under the age of 13 cannot give valid consent to processing for the purposes of an information society service (a remote electronic service provided on request and for remuneration for the processing and storage of data), though a person with parental responsibility for the child may give the requisite consent.

Article 12 sets out the information that must be provided to a data subject by the controller and when it must be provided.

Article 13 covers the obligation where personal data is processed for a purpose other than that for which it was collected.

Part 3 – Other duties of controllers

Article 14 requires controllers to implement proportionate technical and organizational measures to ensure processing is performed in accordance with the Law and to maintain written records of processing activities. *Article 15* requires controllers to implement such measures to give effect to the data protection principles and integrate necessary safeguards to meet the requirements of the Law and protect the rights of data subjects. The measures must ensure that by default only personal data necessary for each purpose are processed and the data are not made accessible to individuals at large without the data subject's consent or other lawful authority.

Article 16 requires controllers to carry out data protection impact assessments where a type of processing is likely to result in a high risk to the rights and freedoms of natural persons. Where that assessment indicates that any processing would pose such a risk, *Article 17* sets out the steps that a controller must take in the absence of measures taken to mitigate that risk, which involve consulting the Authority who may take certain action as a consequence.

Article 18 contains a requirement to consult the Authority when proposed legislation is likely to result in a high risk to the rights and freedoms of natural persons.

Article 19 sets out the controller's duties regarding the appointment of a processor, being a person or body that processes personal data on behalf of a controller.

Article 20 sets out a controller's obligation to notify the Authority, and in serious cases the data subject, where there has been a breach of security regarding personal data.

Part 4 – Joint security duty and duties of processors

Article 21 sets out the requirements that apply to both controllers and processor to implement technical and organizational measures against unauthorized or unlawful processing of personal data and accidental loss, destruction of or damage to it that are proportionate to the risk to data subjects' rights.

Article 22 places a series of general obligation on processors with reference to the Law and the Authority Law. Processing obligations of processors are set out in *Article 23*.

Part 5 – Data protection officer

Article 24 requires controllers and processors to appoint a data protection officer in certain circumstances. *Article 25* places obligations on them with respect to data protection. *Article 26* sets out the duties of data protection officers.

Part 6 – Rights of data subjects

Article 27 is about the handling of requests from data subjects under this Part by controllers, and in particular the time limits for dealing with such requests.

Article 28 is concerned with the individual's right to be informed of processing of his or her personal data and to be given information about it. *Article 29* contains specific provisions on the handling of right of access requests that relate to health records, which, under *Article 60*, are exempt from *Article 28* in certain circumstances. *Article 30* is concerned with how right of access requests under *Article 28* should be treated.

Article 31 sets out the data subject's rights to rectification in the case of inaccurate or incomplete data. *Article 32* covers the right to erasure of data in certain circumstances.

Article 33 gives the data subject a right to obtain restriction of processing and *Article 34* gives the data subject right to have data transmitted elsewhere.

Articles 35 to 37 cover the right to object to processing for the purposes of public functions or legitimate interest, for direct marketing purposes and for the purposes of archiving or for statistical, scientific or historical research.

Article 38 gives the data subject a right not to be subject to a decision based solely on automated processing that has a significant effect on him or her.

Article 39 makes certain contractual terms void in so far as they contain a requirement for an individual to supply or produce to any other person any records concerning a person's health.

Part 7 – Exemptions

This Part creates exemptions from certain provisions of the Law.

Article 40 provides that except as provided under this Part, rights to transparency of processing, the provision of information and the data subject's rights under *Part 6* (known as the transparency and subject rights provisions) have effect despite any enactment or rule of law restricting disclosure or authorizing the withholding of information.

Article 41 exempts the processing of personal data necessary for safeguarding national security from the data protection principles, the transparency and subject rights provisions, the offence of unlawfully obtaining personal data under *Article 71* and Parts 3 and 4 of the Authority Law.

Article 42 overrides the Law in respect of criminal record certifications and under *Article 43* manual data held by public authorities is exempt from all of the Law apart from *Articles 28 to 31, Part 7 and Articles 68 and 71*.

Article 44 exempts personal data processed for academic, journalistic, artistic or literary purposes from all of the Law apart from *Articles 68 and 69* if the conditions set out are satisfied.

Articles 45 to 59 make the following exemptions from the transparency and subject rights provisions that are detailed in those Articles –

- crime and taxation (*Article 45*);
- corporate finance (*Article 46*);
- trusts (*Article 47*);
- functions relating to the protection from financial loss, charities, health and safety, maladministration and practices contrary to fair trading (*Article 48*);
- management forecasting and planning (*Article 49*);
- negotiations with the data subject (*Article 50*);
- information available to the public by or under an enactment (*Article 51*);
- where disclosure would be contrary to certain enactments (*Article 52*);
- confidential references given by the controller (*Article 53*);
- examination scripts (*Article 54*);
- Crown or judicial appointments and honours (*Article 55*);
- the armed forces (*Article 56*);
- legal professional privilege (*Article 57*);
- self-incrimination (*Article 58*);
- privilege of the States Assembly (*Article 59*).

Article 60 modifies the application of *Article 27* in the case of marking data relating to examinations.

Article 61 exempts data processed by a court relating to health, education or social work matters from *Article 28*.

Article 62 restricts the application of *Article 28* where the controller is a credit reference agency.

Article 63 exempts certain public authorities from *Article 28(1)* in relation to unstructured personal data (data other than auto-generated data or data recorded as part of or to be part of a filing system) unless the request under that provision contains a description of the data or the costs of complying would be exceed a prescribed limit.

Article 64 provides for any provision of the Law to be overridden and for processing (including disclosure) of personal data permitted for a purpose other than that for which it was collected and without the consent of the data subject to take place, if the processing meets one of the conditions set out in *Schedule 2*. This applies where processing is for the purposes of *Article 45* or for legal proceedings. Processing is also

permitted where the controller is obliged by statute to make the information available to the public.

Article 65 enables further exemptions to be made in certain circumstances by Regulations.

Part 8 – Cross-border data transfers

Article 66 states that a controller or processor must not transfer data for processing to a third country or international organization unless the level of protection for the rights and freedoms of data subjects is adequate. The level of protection is adequate if the Commission has decided by means of an implementing act under *Article 45* of the GDPR, there are safeguards in place that meet *Article 67* or the transfer falls within the exceptions set out in *Schedule 3*.

Article 67 sets out those safeguards, which include binding corporate rules that comply with *Schedule 4*.

Part 9 – Remedies and enforcement

Article 68 empowers a data subject who considers that the transparency and subject rights provisions have been contravened to bring proceedings in the Royal Court.

Article 69 gives a right to compensation to any person who suffers loss, damage or distress by reason of a contravention of the Law by a controller or processor.

Article 70 enables a person with standing to make a complaint or bring proceedings under this Law or the Authority Law to authorize a data protection organization (a non-profit association that has objectives in the public interest and is active in the data protection field) to represent the person.

Articles 71 to 74 contain the offences of unlawful obtaining of personal data, requiring a person to produce certain records, giving false information or obstruction, giving of false information and obstruction. They attract penalties of 2 years' imprisonment and/or a fine.

Article 75 is a general provision relating to offences and makes offences where no penalty is otherwise provided liable to a fine as well as including standard provisions as to criminal liability of certain bodies and partnerships and secondary parties to offences. *Article 76* contains further provision concerning unincorporated bodies.

Article 76 is a standard provision about making Rules of Court.

Part 10 – Miscellaneous

Article 78 provides for the Authority to approve codes of conduct to encourage or facilitate compliance with the Law or to enable controllers or processor who are not otherwise subject to it to demonstrate adequate safeguards for transfers of personal data to third countries or international organizations. The provisions that a code may contain are set out in the Article as are the conditions for code approval.

Article 79 enables the Authority to accredit any person to monitor compliance with a code if it considers that the person meets criteria laid down in the Article. The accredited person is given powers to take certain action in a case of infringement of a code.

Article 80 enables Regulations to provide for the establishment of mechanisms, seals or marks to certify or signify that particular processing operations comply with the Law or certain safeguards exist in the case of data transfers to third countries or international organizations.

Article 81 provides for the application of the Law to the public sector.

Article 82 is a standard provision about the service of notices, etc.

Article 83 empowers Regulations to prescribe certain matters to improve public service delivery and *Article 84* enables Regulations to provide for the constitution of an Information Board to co-ordinate the disclosure of data to improve the delivery of public services and ensure the legal requirements are met.

Article 54 contains general provisions about Regulations and Orders, including powers to amend primary legislation (including this Law) and for offences set out in Regulations to attract a fine of up to £10,000.

Article 86 introduces *Schedule 5* which contains various savings and transitional arrangements. The Article also empowers Regulations to make further such arrangements.

Article 87 repeals the Data Protection (Jersey) Law 2005 and introduces *Schedule 6*. This Schedule contains various consequential amendments to other enactments and a new provision inserted into the Electronic Communications (Jersey) Law 2000 for the States to make Regulations amending or extending the interpretation of any expression to take account of a change or advancement in technology. There is also power for Regulations to amend other enactments or schemes, licences etc. made under enactments to facilitate electronic communications or storage.

Article 88 names the Law and provides for most of it to come into force on 25th May 2018 (the day that the GDPR comes into force). There are later dates specified to bring in particular provisions.



Jersey

DRAFT DATA PROTECTION (JERSEY) LAW 201-

Arrangement

Article

PART 1	35
INTRODUCTORY	35
1 Interpretation	35
2 Personal data and data subject	40
3 Pseudonymization	41
4 Application	41
5 Processing that does not require identification	42
PART 2	43
FUNDAMENTAL DUTIES OF CONTROLLERS	43
6 General duties and accountability	43
7 Joint controllers	44
8 Data protection principles	44
9 Lawful processing	45
10 Fair and transparent processing	45
11 Consent to processing	46
12 Information to be provided to data subject	47
13 Purposes of processing	49
PART 3	49
OTHER DUTIES OF CONTROLLERS	49
14 Duty to comply with Law and keep records	49
15 Data protection by design and by default	50
16 Data protection impact assessments required for high risk processing	51
17 Prior consultation required for high risk processing	52
18 Prior consultation required for high risk legislation	53
19 Appointment of processor	54
20 Notification of breach	55
PART 4	57
JOINT SECURITY DUTY AND DUTIES OF PROCESSORS	57
21 Security of personal data	57

22	General obligations on processors	58
23	Processing obligations	59
PART 5		59
DATA PROTECTION OFFICER		59
24	Appointment of data protection officer.....	59
25	Position of data protection officer.....	60
26	Duties of data protection officer	61
PART 6		62
RIGHTS OF DATA SUBJECTS		62
27	Handling of requests by data subjects.....	62
28	Right of access requests: general	63
29	Right of access requests: information contained in health records	64
30	Treatment of right of access requests.....	66
31	Right to rectification	66
32	Right to erasure.....	67
33	Right to restriction of processing.....	68
34	Right to data portability	68
35	Right to object to processing for purpose of public functions or legitimate interests	69
36	Right to object to processing for direct marketing purposes.....	69
37	Right to object to processing for historical or scientific purposes	70
38	Right regarding automated individual decision-making	70
39	Certain contractual terms relating to health records void	71
PART 7		71
EXEMPTIONS		71
DIVISION 1 – GENERAL AND WIDER EXEMPTIONS		71
40	Effect of this Part	71
41	National security	71
42	Criminal record certifications	72
43	Manual data held by public authorities	72
44	Academic, journalistic, literary or artistic material.....	72
DIVISION 2 – EXEMPTIONS FROM TRANSPARENCY AND SUBJECT RIGHTS PROVISIONS		73
45	Crime and taxation.....	73
46	Corporate finance.....	74
47	Trusts	75
48	Financial loss, charities, health and safety, maladministration and practices contrary to fair trading	76
49	Management forecasts etc.....	77
50	Negotiations	78
51	Information available to public by or under enactment	78
52	Disclosure contrary to certain enactments	78
53	Confidential references given by the controller.....	78
54	Examination scripts etc.	78
55	Crown or judicial appointments and honours	78

56	Armed forces	79
57	Legal professional privilege	79
58	Self-incrimination.....	79
59	States Assembly privilege	79
DIVISION 3 – EXCEPTIONS TO ARTICLE 27 OR 28		80
60	Examination marks.....	80
61	Health, education and social work	80
62	Credit reference agency as controller	83
63	Unstructured personal data held by scheduled public authorities	83
DIVISION 4 – PERMISSIONS AND EXEMPTIONS BY REGULATIONS		84
64	Permitted processing for law enforcement, legal proceedings and public records purposes.....	84
65	Exemptions by Regulations.....	84
PART 8		85
CROSS-BORDER DATA TRANSFERS		85
66	General principles for cross-border data transfers	85
67	Transfer subject to appropriate safeguards.....	85
PART 9		87
REMEDIES AND ENFORCEMENT		87
68	Proceedings against controllers	87
69	Compensation.....	87
70	Representation of data subjects	88
71	Unlawful obtaining etc. of personal data.....	88
72	Requirement to produce certain records illegal.....	89
73	False information.....	90
74	Obstruction.....	91
75	General provisions relating to offences.....	91
76	Proceedings concerning unincorporated bodies	92
77	Rules of Court	92
PART 10		93
MISCELLANEOUS		93
78	Codes of conduct.....	93
79	Accreditation and duties of accredited person	94
80	Regulations establishing certification mechanism	95
81	Application to public sector	95
82	Service of notices etc.....	95
83	Regulations – disclosure of information to improve public service delivery.....	97
84	Regulations - constitution of Information Board	98
85	Regulations and Orders - general	98
86	Savings and transitional arrangements	99
87	Repeals and consequential and miscellaneous amendments	99
88	Citation and commencement	100

SCHEDULE 1 **101**

**MODIFICATIONS OF LAW IN CASES OF PROCESSING BY
COMPETENT AUTHORITIES** **101**

- 1 List of competent authorities 101
- 2 Application and power to prescribe time limits 101
- 3 Article 8 modified 102
- 4 Article 9 substituted 102
- 5 Article 10 modified 103
- 6 Article 12 substituted 103
- 7 Article 13 substituted 104
- 8 Article 15 modified 105
- 9 Article 17 modified 105
- 10 Article 20 modified 105
- 11 Article 21 modified 105
- 12 Article 27 modified 107
- 13 Article 28 modified 107
- 14 Article 31 modified 107
- 15 Article 32 modified 108
- 16 Article 33 modified 109
- 17 Articles 34 to 37 omitted 109
- 18 Article 38 modified 109
- 19 Part 8 substituted 110

SCHEDULE 2 **114**

CONDITIONS FOR PROCESSING **114**

PART 1 – CONDITIONS FOR PROCESSING PERSONAL DATA **114**

- 1 Consent 114
- 2 Contract 114
- 3 Vital interests 114
- 4 Public functions 114
- 5 Legitimate interests 114

**PART 2 – CONDITIONS FOR PROCESSING PERSONAL DATA AND
SPECIAL CATEGORY DATA** **115**

- 6 Consent 115
- 7 Other legal obligations 115
- 8 Employment and social fields 115
- 9 Vital interests 115
- 10 Non-profit associations 115
- 11 Information made public 116
- 12 Legal proceedings, etc. 116
- 13 Public functions 116
- 14 Public interest 116
- 15 Medical purposes 116
- 16 Public health 116
- 17 Archiving and research 117
- 18 Avoidance of discrimination 117
- 19 Prevention of unlawful acts 117

20	Protection against malpractice and mismanagement.....	118
21	Publication about malpractice and mismanagement	118
22	Counselling	118
23	Insurance and pensions: general determinations	119
24	Insurance and pensions: current processing	119
25	Functions of a police officer.....	120
26	Regulations.....	120

SCHEDULE 3 **121**

EXCEPTIONS TO ADEQUACY REQUIREMENTS		121
1	Order of court, public authorities etc.....	121
2	Consent.....	121
3	Contract between data subject and controller.....	121
4	Third-party contract in interest of data subject	121
5	Transfer by or on behalf of JFSC	121
6	Legal proceedings etc.....	122
7	Vital interests	122
8	Public register.....	122
9	Other exceptions.....	123
10	Public authorities.....	123
11	Recording of assessment	123

SCHEDULE 4 **124**

BINDING CORPORATE RULES		124
--------------------------------	--	------------

SCHEDULE 5 **126**

SAVINGS AND TRANSITIONAL ARRANGEMENTS		126
1	Interpretation	126
2	Processing underway at time of commencement of this Law	126
3	Request for information and copy of personal data.....	126
4	Right to compensation for inaccuracy, loss or unauthorized disclosure	126
5	Application for rectification, blocking, erasure or destruction.....	126
6	Self-incrimination, etc.....	127
7	General: references to Data Protection Commissioner	127
8	General saving (except for Regulations, Rules or Orders).....	127

SCHEDULE 6 **128**

CONSEQUENTIAL AND MISCELLANEOUS AMENDMENTS		128
1	Consequential amendments to various enactments	128
2	Public Records (Jersey) Law 2002.....	129
3	Freedom of Information (Jersey) Law 2011.....	129
4	Medical Practitioners (Registration) (Jersey) Law 1960.....	129
5	Firearms (General Provisions) (Jersey) Order 2011.....	129
6	Goods and Services Tax (Jersey) Law 2007	130
7	Health Insurance (Jersey) Law 1967	130
8	Miscellaneous amendment: Electronic Communications (Jersey) Law 2000.....	130



Jersey

DRAFT DATA PROTECTION (JERSEY) LAW 201-

A LAW to make new and consolidated provision relating to the protection of natural persons with regard to the processing and free movement of personal data and for connected purposes.

Adopted by the States [date to be inserted]

Sanctioned by Order of Her Majesty in Council [date to be inserted]

Registered by the Royal Court [date to be inserted]

THE STATES, subject to the sanction of Her Most Excellent Majesty in Council, have adopted the following Law –

PART 1

INTRODUCTORY

1 Interpretation

(1) In this Law –

“Authority” means the Data Protection Authority established by Article 2 of the Authority Law;

“Authority Law” means the Data Protection Authority (Jersey) Law 201⁻¹;

“appropriate safeguards”, in relation to the protection of personal data or the rights and freedoms of natural persons includes –

(a) technical or organizational measures to ensure that the personal data are processed fairly;

(b) encryption or pseudonymization of the personal data concerned; and

(c) duties imposed by law, such as duties of confidentiality or secrecy;

“automated processing” includes profiling;

“biometric data” means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, that allow or confirm the unique

identification of that natural person, such as facial images or fingerprint data;

“binding corporate rules” means personal data protection policies that are adhered to by a controller or processor established in the territory of a Member State for transfers or a set of transfers of personal data to a controller or processor in one or more third countries within a group of undertakings, or group of enterprises, engaged in a joint economic activity;

“business” includes any activity, trade or profession, whether or not carried on for profit and for clarity includes any such activity, trade or profession carried on for a charity or other not-for-profit body;

“code” means a code of conduct approved by the Authority under Article 78 and includes any amendment or extension of such a code;

“competent supervisory authority” means any supervisory authority with jurisdiction to regulate the controller or processor in question;

“controller” means the natural or legal person, public authority, agency or other body that, whether alone or jointly with others, determines the purposes and means of the processing of personal data, and where those purposes and means are determined by the relevant law, the controller or the specific criteria for its nomination may be provided for by such law;

“data” means information that –

- (a) is being processed by means of equipment operating automatically in response to instructions given for that purpose;
- (b) is recorded with the intention that it should be processed by means of such equipment;
- (c) is recorded as part of a filing system or with the intention that it should form part of a filing system; or
- (d) is recorded information held by a scheduled public authority and does not fall within any of sub-paragraphs (a) to (c);

“data concerning health” means personal data related to the physical or mental health of a natural person, including the provision of health care services, that reveal information about his or her health status;

“data protection impact assessment” has the meaning assigned by Article 16(1);

“data protection officer” means the person appointed as such under Article 24;

“data protection principles” means the requirements set out in Article 8(1);

“data subject” has the meaning assigned by Article 2;

“enterprise” means a natural or legal person engaged in an economic activity, irrespective of its legal form, including partnerships or associations regularly engaged in an economic activity;

“evidence of certification” means evidence of certification granted in accordance with a mechanism established by Regulations made under Article 80;

“filing system” means any set of personal data that, although the data is not processed by means of equipment operating automatically in response to instructions given for that purpose, is structured, either by reference to natural persons or to criteria relating to natural persons, in such a way that specific information relating to a particular natural person is readily accessible and whether the criteria is centralised, decentralised or dispersed on a functional or geographical basis;

“establishment”, in the context of establishment in a territory or jurisdiction, means the effective and real exercise of activity through arrangements that are stable but that need not take any particular legal form and whether or not via a branch or subsidiary with a legal personality;

“GDPR” means Regulation (EU) 2016/79 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (OJ L 119/1 4.5.2016);

“genetic data” means personal data relating to the inherited or acquired genetic characteristics of a natural person that give unique information about the physiology or the health of that natural person and that result, in particular, from an analysis of a biological sample from the natural person in question such as DNA or RNA analysis;

“group of undertakings” means a controlling undertaking and its controlled undertakings;

“health professional” means –

- (a) a person lawfully practising as a medical practitioner, dentist, optometrist, dispensing optician, pharmacist, nurse, midwife or health visitor, osteopath, chiropractor, clinical psychologist, child psychotherapist or speech therapist;
- (b) a music therapist employed by a body lawfully providing health services;
- (c) a scientist employed by such a body as head of a department; or
- (d) any person who may be prescribed;

“health record” means a record that –

- (a) consists of data concerning health; and
- (b) has been made by or on behalf of a health professional in connection with the care of that individual;

“information society service” means, subject to paragraph (3), a service normally provided for remuneration –

- (a) without the parties being present at the same time;
- (b) that is sent initially and received at its destination by means of electronic equipment for the processing (including digital compression) and storage of data, and entirely transmitted, conveyed and received by wire, by radio, by optical means or by other electromagnetic means; and
- (c) through the transmission of data on individual request;

“international organization” means an organization and its subordinate bodies governed by public international law, or any other body that is set up by, or on the basis of, an agreement between 2 or more countries;

“joint controller” has the meaning assigned by Article 7(1);

“large scale” means large scale having regard to the number of data subjects, volume or range of data being processed, duration or permanence of the activity and geographical extent;

“Law Enforcement Directive” means Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (OJ L 119/89 4.5.16);

“law enforcement purpose” means any of the following purposes, namely the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against, and the prevention of, threats to public security;

“Member State” means a Member State of the European Union;

“Minister” unless otherwise indicated, means the Chief Minister;

“parental responsibility” has the same meaning as in the Children (Jersey) Law 2002²;

“personal data” has the meaning assigned by Article 2(1);

“personal data breach” means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed;

“prescribed” means prescribed by Regulations;

“processing” means any operation or set of operations that is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

“processor” means a natural or legal person, public authority, agency or other body that processes personal data on behalf of the controller, but does not include an employee of the controller;

“profiling” means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person’s performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;

“pseudonymization” has the meaning assigned by Article 3;

“public authority” means –

- (a) the States Assembly including the States Greffe;
- (b) a Minister;
- (c) a committee or other body established by a resolution of the States or by, or in accordance with, standing orders of the States Assembly;
- (d) an administration of the States;
- (e) a Department referred to in Article 1 of the Departments of the Judiciary and the Legislature (Jersey) Law 1965³;
- (f) any court or tribunal;
- (g) the States of Jersey Police Force;
- (h) a parish;
- (i) the holder of a public office;
- (j) in relation to any country other than Jersey, any person exercising or performing functions or holding any office similar or comparable to any of the persons described in sub-paragraphs (a) to (i); and
- (k) any other person or body (whether incorporated or unincorporated) that exercises functions of a public nature;

“recipient”, in relation to any personal data, means any person to whom the data are disclosed, whether a third party or not, but does not include a public authority to whom disclosure is or may be made in the framework of a particular inquiry in accordance with the relevant law;

“Regulations” means Regulations made by the States;

“relevant law” means the law of Jersey, another jurisdiction in the British Islands, a Member State or the European Union;

“representative” means a representative nominated by the controller under Article 4(3);

“restriction of processing” means the marking of stored personal data with the aim of limiting their processing in the future;

“scheduled public authority” has the same meaning as in the Freedom of Information (Jersey) Law 2011⁴;

“States’ employee” has the same meaning as in Article 2 of the Employment of States of Jersey Employees (Jersey) Law 2005⁵;

“special category data” means –

- (a) data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership;
- (b) genetic or biometric data that is processed for the purpose of uniquely identifying a natural person;
- (c) data concerning health;
- (d) data concerning a natural person’s sex life or sexual orientation; or
- (e) data relating to a natural person’s criminal record or alleged criminal activity;

“special purposes” means –

- (a) academic purposes;
- (b) the purpose of journalism;
- (c) artistic purposes; or
- (d) literary purposes;

“supervisory authority” means an independent public authority established under the relevant law for the purposes of the GDPR or equivalent legislation;

“third country” means a country or territory outside the European Economic Area other than Jersey;

“third party” means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who are authorized to process personal data under the direct authority of the controller or processor;

“transparency and subject rights provisions” means –

- (a) the first data protection principle set out in Article 8(1)(a), to the extent that it requires data to be processed transparently;
 - (b) the provisions as to information to be provided to a data subject under Article 12; and
 - (c) the rights of data subjects set out in Part 6.
- (2) If personal data are processed for purposes for which they are required to be processed by or under an enactment, the person on whom the obligation to process the data is imposed is, in relation to the data, the controller for the purposes of this Law.
- (3) The Minister may, by Order, specify the services that do or do not fall within the definition “information society service”, by reference either to individual services or by class or description.
- (4) Regulations may amend any of the definitions in paragraph (1).

2 Personal data and data subject

- (1) Personal data means any data relating to a data subject.
- (2) A data subject is an identified or identifiable, natural, living person who can be identified, directly or indirectly, by reference to (but not limited to) an identifier such as –
- (a) a name, an identification number or location data;
 - (b) an online identifier; or
 - (c) one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the person.
- (3) The following matters must be taken into account in deciding whether the person is identified or identifiable –
- (a) the means reasonably likely to be used by the controller or another person to identify the person, taking into account factors such as

the cost and amount of time required for identification in the light of the available technology at the time of processing and technological factors;

- (b) whether the personal data, despite pseudonymization, is capable of being attributed to that person by the use of information other than that kept separately for the purposes of pseudonymization.
- (4) In this Article “identifier” means a number or code (including any unique number or code issued to the individual by a public authority) assigned to an individual by a controller or processor for the purposes of its operations that uniquely identifies the individual and includes location data.

3 Pseudonymization

- (1) In this Law “pseudonymization” means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, and where that additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.
- (2) Pseudonymization may be achieved even though the additional information that would enable the attribution of the data to a specific data subject is retained within the controller’s organization provided that the controller maintains records indicating who has access to that additional information.

4 Application

- (1) This Law does not apply to the processing of personal data by a natural person in the course of a purely personal or household activity (but applies to controllers or processors that provide the means for processing personal data for such an activity).
- (2) This Law applies to the processing of personal data –
 - (a) in the context of a controller or processor established in Jersey;
 - (b) by a controller or processor not established in Jersey but who uses equipment in Jersey for processing the data otherwise than for the purposes of transit through Jersey; or
 - (c) by a controller or processor not established in Jersey where the processing –
 - (i) relates to data subjects who are in Jersey, and
 - (ii) is for the purpose of offering goods or services to persons in Jersey or monitoring the behaviour of such persons.
- (3) A controller referred to in paragraph (2)(b) must nominate, in writing and for the purposes of this Law, a representative established in Jersey.
- (4) For the purposes of paragraphs (2) and (3), each of the following is to be treated as established in Jersey –

-
- (a) a natural person who is ordinarily resident in Jersey;
 - (b) a body incorporated under the law of Jersey;
 - (c) a partnership or other unincorporated association formed under the law of Jersey;
 - (d) any person who does not fall within sub-paragraph (a), (b) or (c) but maintains in Jersey –
 - (i) an office, branch or agency through which the person carries on any processing of personal data, or
 - (ii) a regular practice that carries on any processing of personal data; or
 - (e) any person engaging in effective and real processing activities through stable arrangements in Jersey.
- (5) Schedule 1 has effect to modify the application of this Law where the processing of personal data is carried out –
- (a) by a controller that is a competent authority; and
 - (b) for a law enforcement purpose,
- and Regulations may amend Schedule 1 in order to make further provision for such purposes.
- (6) Regulations may also amend Schedule 1 so as to –
- (a) add or remove any person or body to the list of competent authorities;
 - (b) ensure that the Law provides equivalent protection for personal data to that provided under the Law Enforcement Directive or by another jurisdiction in the British Islands; or
 - (c) make provision as to personal data contained in a judicial decision or record or case file processed in the course of a criminal investigation or proceedings.
- (7) In this Article “competent authority” means –
- (a) any person, body or other entity listed in paragraph 1 of Schedule 1; and
 - (b) any other person, body or other entity who exercises a function for a law enforcement purpose in Jersey,
- but does not include the security and intelligence services of the Government of the United Kingdom.

5 Processing that does not require identification

- (1) If the purposes for which a controller processes personal data do not, or no longer, require the identification of a data subject by the controller, the controller is not obliged to maintain, acquire or process additional information in order to identify the data subject for the sole purpose of complying with this Law.
- (2) Where paragraph (1) applies and the controller is able to demonstrate that it is no longer able to identify the data subject, Articles 28 to 34 do not apply except where the data subject, for the purposes of exercising his or

her rights under those Articles, provides additional information enabling his or her identification.

PART 2

FUNDAMENTAL DUTIES OF CONTROLLERS

6 General duties and accountability

- (1) A controller –
 - (a) is responsible for, and must be able to demonstrate compliance with, the data protection principles in the manner provided for in this Law;
 - (b) if established in Jersey, may process personal data or cause it to be processed only if the controller is registered under Article 17 of the Authority Law;
 - (c) must pay such charges to the Authority as Regulations under Article 18 of the Authority Law may prescribe;
 - (d) in planning and implementing the processing of personal data, must ensure that appropriate safeguards for the rights of data subjects are put in place by design and by default in accordance with Article 15;
 - (e) must comply with the record-keeping requirements and disclose the records covered by those requirements on request to the Authority;
 - (f) where a processor is appointed, must appoint a processor only in accordance with Article 19;
 - (g) must report any personal data breach in the manner and to the extent required by Article 20 unless Part 7 applies;
 - (h) must appoint a data protection officer where so required by Article 24;
 - (i) must co-operate with any requests of the Authority under this Law or the Authority Law; and
 - (j) must comply with any order of the Authority under Article 25 of, and notice of the Authority under paragraph 1 of Schedule 1 to, the Authority Law.
- (2) Adherence to a code or evidence of certification may provide evidence that an individual controller has complied with a particular obligation under this Law.
- (3) The record keeping requirements do not apply in the case of organizations with fewer than 250 employees unless the processing –
 - (a) is likely to result in a risk to the rights and freedoms of data subjects;
 - (b) is not occasional; or
 - (c) includes special category data or relates to criminal convictions or related security measures.

- (4) The Authority must take into account the specific needs of different sizes of enterprise in the application of this Law.
- (5) Regulations may make further provision to modify or limit the application of paragraph (1) in the case of organizations mentioned in paragraph (3) and may amend the description of those organizations.
- (6) In this Article “record keeping requirements” means the requirements with respect to record keeping set out in Articles 3(2) and 14(3).

7 Joint controllers

- (1) Where 2 or more controllers jointly determine the purposes and means of the processing of personal data they are joint controllers.
- (2) Joint controllers must make arrangements between themselves in a transparent manner so as to apportion their responsibilities in advance of the processing of personal data.
- (3) Joint controllers must make a summary of the arrangements available to data subjects and may designate a contact point to facilitate communication between data subjects and joint controllers.
- (4) Regardless of the terms and conditions of any arrangement under paragraph (2) or any other agreement –
 - (a) a data subject may exercise any right that he or she has under this Law against any joint controller; and
 - (b) each joint controller is jointly and severally liable for any damage caused by processing if it is in contravention of this Law.
- (5) Where a joint controller proves that it had no responsibility for the damage, it may be exempted from liability.
- (6) Paragraphs (1) to (3) do not apply where the respective responsibilities of joint controllers are clearly determined by law (otherwise than under this Article).
- (7) Any joint controller may bring proceedings against any other joint controller to recover that part of the compensation corresponding to the other joint controller’s part of responsibility for the damage.
- (8) Regulations may make further provision about the respective roles of joint controllers, including the circumstances in which a joint controller is treated as being a sole controller.

8 Data protection principles

- (1) A controller must ensure that the processing of personal data in relation to which the controller is the controller complies with the data protection principles, namely that data are –
 - (a) processed lawfully, fairly and in a transparent manner in relation to the data (“lawfulness, fairness and transparency”);
 - (b) collected for specified, explicit and legitimate purposes and once collected, not further processed in a manner incompatible with those purposes (“purpose limitation”);

- (c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (“data minimization”);
 - (d) accurate and, where necessary, kept up to date, with reasonable steps being taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay (“accuracy”);
 - (e) kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the data are processed (“storage limitation”); and
 - (f) processed in a manner that ensures appropriate security of the data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures (“integrity and confidentiality”).
- (2) In relation to –
- (a) paragraph (1)(b), further processing for the purposes specified in paragraph 17 of Schedule 2 (archiving and research) is not to be taken as incompatible with the initial purposes for which the data was collected;
 - (b) paragraph (1)(e), personal data may be stored to the extent necessary for the purposes specified in paragraphs 7 (other legal obligations) and 17 of Schedule 2 subject to implementation of the appropriate technical and organization measures required by this Law in order to safeguard the rights and freedoms of the data subject.

9 Lawful processing

- (1) The processing of personal data that would otherwise be lawful is lawful for the purposes of this Law only if it meets at least one of the conditions specified in Schedule 2.
- (2) However, in the case of any processing of data that includes special category data, it must meet at least one of the conditions mentioned in Part 2 of Schedule 2.

10 Fair and transparent processing

- (1) To determine the fairness of processing personal data regard must be had to whether the method by which the data are obtained, including in particular whether any person from whom they are obtained is deceived or misled as to the purpose or purposes for which they are to be processed.
- (2) Personal data are regarded as obtained fairly if they consist of information obtained from a person who –
 - (a) is authorized by or under any enactment to supply it; or

-
- (b) is required to supply it by or under any enactment or any international agreement imposing an international obligation on Jersey.
 - (3) In order that personal data may be processed fairly and transparently, a controller must –
 - (a) facilitate the exercise of the rights of data subjects under Part 6;
 - (b) act on a data subject's request unless the controller is unable to do so because the data subject cannot be identified or the processing is exempted from such a requirement under this Law.

11 Consent to processing

- (1) In this Law, “consent”, in relation to the processing of a data subject's personal data, means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, whether orally or in writing, signifies agreement to the processing of that data.
- (2) Consent –
 - (a) is not informed unless the data subject is aware of the identity of the controller who will process the data and the purposes of the processing for which the personal data are intended;
 - (b) is not freely given if it does not allow separate consent to be given to different personal data processing operations where it is appropriate in the individual case.
- (3) To establish the presence of such consent, the controller must be able to demonstrate that –
 - (a) the request for consent was in a concise, intelligible and easily accessible form;
 - (b) where that request was in writing together with other matters, that it was clearly distinguishable from those other matters;
 - (c) where the request for consent was by electronic means, that it was sought in a way that was not unnecessarily disruptive to the use of the service for which the request was provided;
 - (d) where consent was sought for the purposes of the performance of a contract that includes the provision of a service –
 - (i) consent was necessary for the performance of the contract, or
 - (ii) if it was not necessary, the controller has advised the data subject that he or she may refuse separate consent for the provision of the service without prejudice to the performance of the contract;
 - (e) the data subject was informed of the right to withdraw consent at any time and that it was as easy to withdraw consent as it was to give it; and
 - (f) the controller has made reasonable efforts to verify that the person giving the consent is who the person claims to be, particularly

where that person claims to be the person authorized to consent for a child under the age of 13.

- (4) A child under the age of 13 may not give valid consent to the processing of his or her personal data by a controller for the purposes of an information society service but valid consent on behalf of that child may be given by a person with parental responsibility for him or her.
- (5) Consent is taken to cover all processing activities carried out for the same purpose for which it is given and separate consent is required for each separate purpose.
- (6) The States may make Regulations –
 - (a) amending the age of consent in paragraphs (3)(f) or (4), providing exceptions to the inability of the child to consent and making further provision as to the steps that the controller must take to verify –
 - (i) the age and identity of the child and any person purporting to given consent on his or her behalf, and
 - (ii) that the person has actually given consent;
 - (b) governing the effect of consent where personal data is to be used for the purposes of scientific research.

12 Information to be provided to data subject

- (1) A controller must ensure as far as practicable that where personal data have been obtained by the controller from the data subject, the data subject is provided with, or has made readily available to him or her, the specified information at the same time as the data are obtained.
- (2) Where personal data were not obtained from the data subject, the controller must ensure that the specified information is provided or made readily available to the data subject before the relevant time except where –
 - (a) the data were already in his or her possession;
 - (b) paragraph (6) applies; or
 - (c) Regulations so specify.
- (3) For the purposes of this Article, the relevant time is –
 - (a) a reasonable period after obtaining the personal data, but at the latest within 4 weeks, having regard to the specific circumstances in which the personal data are processed;
 - (b) if the personal data are to be used for communication with the data subject, at the latest at the time of the first communication to that data subject; or
 - (c) if a disclosure to another recipient is envisaged, at the latest when the personal data are first disclosed.
- (4) For the purposes of this Article, the specified information is all of the following –

-
- (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 (if any);
 - (c) the purposes for which the data are intended to be processed and the legal basis for the processing;
 - (d) an explanation of the legitimate interests pursued by the controller or by a third party, if the processing is based on those interests;
 - (e) the recipients or categories of recipients of the personal data (if any);
 - (f) where applicable, the fact that the controller intends to transfer personal data to a third country or international organization and whether or not there is an adequate level of protection for the rights and freedoms of data subjects within the meaning of Article 66;
 - (g) the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;
 - (h) information concerning the rights of data subjects under Part 6, to the extent that these apply;
 - (i) where the processing is based on consent, the existence of the right to withdraw consent under Article 11(3)(e);
 - (j) the existence of any automated decision-making, as referred to in Article 38, and any meaningful information about the logic involved in such decision-making as well as the significance and the envisaged consequences of such processing for the data subject;
 - (k) a statement of the right to complain to the Authority;
 - (l) whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and the possible consequences of failing to provide such data;
 - (m) where the personal data are not obtained directly from the data subject, information identifying the source of the data;
 - (n) any further information that is necessary, having regard to the specific circumstances in which the data are or are to be processed, to enable processing in respect of the data subject to be fair.
- (5) The specified information –
- (a) must be provided in an intelligible form using clear language;
 - (b) may be supplemented by standardized machine-readable icons, and if so, the use of such icons is subject to such requirements that the Minister may, by Order, prescribe.
- (6) Paragraph (2) does not apply if the controller believes that –
- (a) providing the specified information is impossible, would involve a disproportionate effort on the part of the controller, or is likely to prejudice the objectives of the processing and the controller records the reasons for its belief and retains this record while it retains the data; or

- (b) the recording of the information to be contained in the data, or the disclosure of the data by the controller, is necessary for compliance with any legal obligation to which the controller is subject, other than an obligation imposed by contract; or
 - (c) the data are held subject to an obligation of professional secrecy regulated by law (whether in Jersey or elsewhere).
- (7) Where the controller does not provide the information the controller must take appropriate measures to protect the data subject's rights and interests, which may include making the specified information publicly available.

13 Purposes of processing

- (1) Paragraph (2) applies where personal data are processed for a purpose other than that for which they were collected without the consent of the data subject and such processing is not authorized by the relevant law.
- (2) Where this paragraph applies, the controller must assess whether that processing is compatible with the purposes for which the personal data were collected by taking into account factors that include –
 - (a) any link between the purposes for which the data have been collected and the purposes of the intended further processing;
 - (b) the context in which the data have been collected, in particular regarding the relationship between data subjects and the controller;
 - (c) the nature of the data, in particular whether it is special category data;
 - (d) the possible consequences of the intended further processing for data subjects; and
 - (e) the existence of appropriate safeguards.
- (3) Where the controller intends to process personal data further, for a purpose other than that for which the data were collected, the controller must provide the data subject with information on that other purpose, together with the specified information referred to in Article 12(4) before that further processing takes place.

PART 3

OTHER DUTIES OF CONTROLLERS

14 Duty to comply with Law and keep records

- (1) A controller is responsible for –
 - (a) implementing proportionate technical and organizational measures to ensure processing is performed in accordance with this Law; and
 - (b) demonstrating that those measures are in place so that processing is indeed performed in accordance with this Law.

-
- (2) The measures referred to in paragraph (1) may include the adoption of appropriate data protection policies by the controller.
 - (3) The controller and any representative of the controller must maintain a written record of the processing activities for which the controller or representative is responsible containing –
 - (a) the name and contact details of the controller and any joint controller, representative of the controller or data protection officer;
 - (b) the purposes of the processing;
 - (c) a description of the categories of data subjects and personal data processed;
 - (d) a description of the recipients (if any) to whom the controller intends to, or may wish to, disclose the data;
 - (e) where it is envisaged that data will be transferred to a third country or an international organization, the name of that country or organization, and in the case of transfers referred to in paragraph 9 of Schedule 3, the appropriate safeguards that are put in place;
 - (f) where possible, the envisaged data retention periods for different categories of data; and
 - (g) where possible, a general description of the technical and organizational measures implemented in respect of the processed data.
 - (4) Adherence to a code or evidence of certification may provide evidence that an individual controller has complied with this Article.
 - (5) In this Article “proportionate” means proportionate having regard to –
 - (a) the nature, scope, context and purposes of processing;
 - (b) the risk and likelihood of prejudice to the rights of data subjects;
 - (c) best practices in technical and organizational measures;
 - (d) the state of technological development; and
 - (e) the costs of implementation.

15 Data protection by design and by default

- (1) A controller must, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organizational measures that are designed to –
 - (a) implement the data protection principles in an effective manner; and
 - (b) integrate the necessary safeguards into the processing to meet the requirements of this Law and protect the rights of data subjects.
- (2) In determining whether or not a measure is appropriate for the purposes of this Article, regard must be had to the state of technological development, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and

severity for rights and freedoms of natural persons posed by the processing.

- (3) The technical and organizational measures must ensure as far as practicable that, by default –
 - (a) only personal data that are necessary for each specific purpose of the processing are processed; and
 - (b) personal data are not made accessible to an indefinite number of natural persons without the data subject's consent or other lawful authority.
- (4) Paragraph (3) applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility.
- (5) Adherence to a code or evidence of certification may provide evidence that an individual controller has or has not contravened paragraph (1).

16 Data protection impact assessments required for high risk processing

- (1) Where a type of processing is likely to result in a high risk to the rights and freedoms of natural persons, a controller must carry out an assessment of the impact of the envisaged processing operations on the protection of personal data before the processing, to be known as a data protection impact assessment.
- (2) In assessing the risk to the rights and freedoms of natural persons, regard must be had in particular to the use of new technologies, and the nature, scope, context and purposes of the processing.
- (3) Where more than one processing operation is similar as to the degree of risk involved, the risks may be assessed using a single assessment.
- (4) When carrying out a data protection impact assessment, the controller must seek the advice of the data protection officer, where one is appointed.
- (5) A data protection impact assessment is, in particular, required in the case of –
 - (a) a systematic and extensive evaluation of personal aspects relating to natural persons that is based on automated processing, and on which decisions are based that produce legal effects concerning, or similarly significantly affecting, those persons;
 - (b) the processing of special category data on a large scale; or
 - (c) a systematic monitoring of a publicly accessible area on a large scale.
- (6) A data protection impact assessment must contain the following minimum requirements –
 - (a) a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller;
 - (b) an assessment of the necessity and proportionality of the processing operations in relation to the purposes;

-
- (c) an assessment of the risks to the rights and freedoms of natural persons referred to in paragraph (1); and
 - (d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Law, taking into account the rights and legitimate interests of any person.
- (7) The Authority may publish a list of the types of processing operation that are subject to the requirement for a data protection impact assessment and those types of processing operation for which no data protection impact assessment is required.
- (8) Where appropriate, the controller must seek the views of data subjects or their representatives on the intended processing, without limiting the protection of commercial or public interests or the security of processing operations.
- (9) Paragraphs (1) to (6) do not apply where –
- (a) processing in accordance with paragraphs 4 (public functions) and 7 (other legal obligations) of Schedule 2 has a legal basis and is regulated by the relevant law; and
 - (b) a data protection impact assessment has already been carried out as part of a general impact assessment in the context of the adoption of that legal basis.
- (10) The controller must review, and where appropriate, revise the data protection impact assessment where –
- (a) there is a change in the risks posed to the rights and freedoms of data subjects by the processing operations; or
 - (b) the controller otherwise considers it necessary.
- (11) A review under paragraph (10) must include a review of –
- (a) whether the processing operations being carried out accord with those described in the data protection impact assessment; and
 - (b) whether the measures established and carried out to address the risks of processing accord with those envisaged in the data protection impact assessment.

17 Prior consultation required for high risk processing

- (1) This Article applies where a data protection impact assessment indicates that any processing would pose a high risk to the rights and freedoms of natural persons in the absence of measures taken by the controller to mitigate the risk.
- (2) Before starting the processing, the controller must consult the Authority giving the following information in writing –
 - (a) where applicable, the respective responsibilities of the controller, joint controllers and processors involved in the proposed processing, in particular for processing within a group of undertakings;
 - (b) a copy of the data protection impact assessment;

- (c) the contact details of any data protection officer; and
 - (d) any other information required by the Authority.
- (3) Where the Authority considers that the proposed processing would be in contravention of this Law, in particular where the controller has insufficiently identified or mitigated the risk, the Authority –
- (a) must give written notice of its opinion to the controller and, where applicable to the processor; and
 - (b) may exercise any power conferred on the Authority by this Law or the Authority Law in relation to a contravention or potential contravention of a requirement of this Law.
- (4) The Authority must give the notice required by paragraph (3)(a) –
- (a) without undue delay; and
 - (b) in any event within 8 weeks of receiving the information from the controller under paragraph (2).
- (5) The Authority may extend the period in paragraph (4)(b) by a further 6 weeks taking into account the complexity of the intended 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 4 weeks of receiving the information from the controller under paragraph (2).
- (6) If the Authority has requested information from the controller or the processor for the purposes of the consultation, any period of time spent awaiting the provision of that information must be discounted from each period specified in paragraph (4)(b) or (5).

18 Prior consultation required for high risk legislation

- (1) This Article applies where any draft Law or Regulations, or any proposal under Article 31 of the States of Jersey Law 2005⁶, is or are to be lodged *au Greffe* in accordance with standing orders⁷ made under Article 48 of that Law, or any draft Jersey legislation that a Minister is responsible for making is to be made –
- (a) that would require, authorize or otherwise relate to the processing of personal data; and
 - (b) taking into account the nature, scope and purposes of the processing, is likely to result in a high risk to the rights and freedom of natural persons.
- (2) The Minister or other person responsible for the lodging or making, as the case may be, must consult the Authority by means of a written notice, to be known as a “consultation notice”.
- (3) The consultation notice must include any data protection impact assessment carried out in connection with the proposed processing of personal data mentioned in paragraph (1)(a) and, unless included within such an assessment –

-
- (a) a systematic description of the proposed processing (including the means of processing), its purposes and the objectives of the provisions of the legislation effecting it;
 - (b) an assessment of the necessity (including proportionality) of the proposed processing in relation to those objectives;
 - (c) an assessment of the risks to the rights and freedoms of data subjects posed by the processing; and
 - (d) the measures envisaged to address those risks, including appropriate safeguards, security measures and mechanisms to ensure the protection of personal data and demonstrate compliance with this Law, taking into account the rights and freedoms of data subjects.

19 Appointment of processor

- (1) Where processing is to be carried out on behalf of a controller, the controller must use only processors that provide sufficient guarantees to implement appropriate technical and organizational measures in such a manner that processing will meet the requirements of this Law and ensure the protection of the rights of the data subject.
- (2) The processor must not engage another processor without prior specific or general written authorization of the controller, and where the authorization is general, the processor must inform the controller of any intended changes concerning the addition or replacement of other processors, so that the controller may object to the changes.
- (3) Processing by a processor must be governed by a contract or other legal act under the relevant law, that –
 - (a) is binding on the processor with regard to the controller; and
 - (b) sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller.
- (4) The contract or other legal act must, in particular, stipulate that the processor –
 - (a) processes the personal data only on documented instructions from the controller, including with regard to transfers of personal data to a third country or an international organization, unless required to do so by the relevant law to which the processor is subject, in which case the processor must inform the controller of that legal requirement before processing, unless that law prohibits such information being given;
 - (b) ensures that persons authorized to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;
 - (c) takes all measures required by Article 21;
 - (d) respects the conditions referred to in paragraphs (2), (6) and (7) for engaging another processor;

- (e) taking into account the nature of the processing, assists the controller by appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights set out in Part 6;
 - (f) assists the controller in ensuring compliance with the obligations under Articles 16, 20 and 21, taking into account the nature of processing and the information available to the processor;
 - (g) at the choice of the controller, deletes or returns all the personal data to the controller after the end of the provision of services relating to processing, and deletes existing copies unless the relevant law requires storage of the personal data;
 - (h) makes available to the controller all information necessary to demonstrate compliance with the obligations laid down in this Article and allows for and contributes to audits, including inspections, conducted by the controller or another auditor mandated by the controller.
- (5) With respect to paragraph (4)(h), the processor must immediately inform the controller if, in its opinion, an instruction infringes this Law or other data protection provisions of the relevant law.
 - (6) Where the processor engages another processor the obligations set out in paragraph (4) must, in particular, provide sufficient guarantees to implement appropriate technical and organizational measures in such a manner that the processing will meet the requirements of this Law and where that other processor fails to fulfil those obligations, the initial processor remains fully liable to the controller for the performance of that other processor's obligations.
 - (7) Adherence to a code or evidence of certification may provide evidence that an individual processor has complied with paragraphs (1) and (6).
 - (8) Without limiting the provisions of an individual contract between the controller and the processor, the contract or the other legal act referred to in paragraph (4) may be based, in whole or in part, on standard contractual clauses as referred to in paragraph (9).
 - (9) The Authority may publish standard contractual clauses for the matters referred to in paragraphs (4) to (6).
 - (10) The contract or the other legal act referred to in this Article must be in writing.

20 Notification of breach

- (1) In the case of a personal data breach, the controller must, without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach in writing to the Authority in the manner required by the Authority, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons.
- (2) If the notification to the Authority is not made within 72 hours, it must be accompanied by reasons for the delay.

-
- (3) The notification referred to in paragraph (1) must –
 - (a) describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
 - (b) communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;
 - (c) describe the likely consequences of the personal data breach; and
 - (d) describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.
 - (4) Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.
 - (5) The controller must document any personal data breaches, including the facts relating to the personal data breach, its effects and the remedial action taken, in such detail as will enable the Authority to verify compliance with this Article.
 - (6) If the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller must communicate the breach to the data subject –
 - (a) without undue delay; and
 - (b) in clear and plain language describing the nature of the personal data breach; and
 - (c) giving the information referred to in paragraph (3)(b) to (d).
 - (7) Despite paragraph (6) communication is not required if –
 - (a) the controller has implemented proportionate technical and organizational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular measures that render the personal data unintelligible to any person who is not authorized to access it, such as encryption;
 - (b) the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects referred to in paragraph (6) is no longer likely to materialize; or
 - (c) it would involve disproportionate effort, in which case there must instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.
 - (8) If the controller has not already communicated the personal data breach to the data subject, the Authority, having considered the likelihood of the personal data breach resulting in a high risk to the rights and freedoms of natural persons, may require it to do so or may decide that any of the conditions referred to in paragraph (7) are met.

PART 4**JOINT SECURITY DUTY AND DUTIES OF PROCESSORS****21 Security of personal data**

- (1) Controllers and processors must implement technical and organizational measures against unauthorized or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data that are proportionate to the risk of harm posed to the rights of data subjects by such events.
- (2) The technical measures that the controller may take to ensure a level of security appropriate to the risk include –
 - (a) the pseudonymization and encryption of personal data;
 - (b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
 - (c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
 - (d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.
- (3) Adherence to a code or evidence of certification may provide evidence that an individual controller has complied with paragraph (1).
- (4) Controllers and processors must take reasonable steps to ensure the proper performance of duties by any person under the controller's or the processor's authority.
- (5) If processing of personal data is carried out by a processor on behalf of a controller, the controller must –
 - (a) choose a processor providing sufficient guarantees in respect of the technical and organizational security measures governing the processing to be carried out; and
 - (b) take reasonable steps to ensure compliance with those measures.
- (6) If processing of personal data is carried out by a processor on behalf of a controller, the processing must be carried out under a contract –
 - (a) that is made or evidenced in writing;
 - (b) under which the processor is to act only on instructions from the controller; and
 - (c) that requires the processor to comply with obligations equivalent to those imposed on a controller under this Article.
- (7) The Minister may, by Order, amend the technical measures in paragraph (2).
- (8) In this Article “proportionate” means proportionate having regard to –
 - (a) the nature, scope, context and purposes of processing;
 - (b) the risk and likelihood of prejudice to the rights of data subjects;

- (c) best practices in technical and organizational measures;
- (d) the state of technological development; and
- (e) the costs of implementation.

22 General obligations on processors

- (1) A processor must –
 - (a) if established in Jersey, cause or permit personal data to be processed only if the processor meets the requirement to be registered under Article 17 of the Authority Law;
 - (b) pay such charges to the Authority as Regulations under Article 18 of the Authority Law may prescribe;
 - (c) comply with the requirements on processors set out in Articles 19 and 23;
 - (d) implement appropriate technical and organizational security measures to protect personal data against accidental or unlawful destruction or loss, alteration, unauthorized disclosure or access;
 - (e) keep records of the processor's data processing activities in accordance with this Law and disclose them on request to the Authority;
 - (f) ensure that any personal data that it processes are kept confidential;
 - (g) notify the controller without undue delay after becoming aware of a personal data breach;
 - (h) appoint a data protection officer if required to do so by Article 24;
 - (i) comply with Article 65 regarding cross-border data transfers;
 - (j) co-operate with any requests of the Authority under this Law or the Authority Law; and
 - (k) comply with any order of the Authority under Article 25 of, and an information notice of the Authority under paragraph 1 of Schedule 1 to, the Authority Law.
- (2) Paragraph (1)(e) does not apply in the case of organizations with fewer than 250 employees unless the processing –
 - (a) is likely to result in a risk to the rights and freedoms of data subjects;
 - (b) is not occasional; or
 - (c) includes special category data or relates to criminal convictions or related security measures.
- (3) A processor is liable to a data subject for any damage suffered as a result of processing that contravenes this Law.
- (4) However, the processor is liable for the damage only where –
 - (a) it has not complied with the obligations placed on processors by this Law; or
 - (b) it acted outside of or contrary to the lawful instructions of the controller.

- (5) Adherence to a code or evidence of certification may provide evidence that an individual processor has complied with a particular obligation of this Article.
- (6) Regulations may prescribe mandatory terms that must be implied into processing contracts.

23 Processing obligations

- (1) The processor and any person acting under the authority of the controller or of the processor who has access to personal data, must not process those data unless –
 - (a) instructed to do so by the controller; or
 - (b) required to do so by the relevant law.
- (2) Unless required to do so by the relevant law, a processor is taken to be a controller if the processor processes personal data other than in accordance with the instructions of the controller.
- (3) A processor must maintain a record of all categories of processing activities carried out on behalf of a controller, containing –
 - (a) the name and contact details of the processor or processors and of each controller on behalf of which the processor is acting, and, where applicable, of the controller's or the processor's representative, and the data protection officer;
 - (b) the categories of processing carried out on behalf of each controller;
 - (c) where applicable, transfers of personal data to a third country or an international organization, including the identification of that third country or international organization and, in the case of transfers referred to in paragraph 9 of Schedule 3, the documentation of suitable safeguards; and
 - (d) where possible, a general description of the technical and organizational security measures referred to in Article 21.

PART 5

DATA PROTECTION OFFICER

24 Appointment of data protection officer

- (1) The controller and the processor must appoint a data protection officer in any case where –
 - (a) the processing is carried out by a public authority, except for courts acting in their judicial capacity;
 - (b) the core activities of the controller or the processor consist of processing operations that, by virtue of their nature, scope or purposes, require regular and systematic monitoring of data subjects on a large scale;

-
- (c) the core activities of the controller or the processor consist of processing special category data on a large scale; or
 - (d) it is required by the relevant law.
- (2) A group of undertakings may appoint a single data protection officer provided that the data protection officer is easily accessible from each establishment.
 - (3) Where the controller or the processor is a public authority, a single data protection officer may be appointed for several such authorities or bodies, taking account of their organizational structure and size.
 - (4) However, a single data protection officer is permissible in the circumstances set out in paragraph (2) or (3) only if the officer is easily accessible to –
 - (a) all data subjects;
 - (b) the Authority; and
 - (c) the controller or processor who appointed the officer along with such of the controller or processor’s employees as carry out data processing.
 - (5) In cases other than those referred to in paragraph (1), the controller or processor or associations and other bodies representing categories of controllers or processors may or, where required by the relevant law, must, appoint a data protection officer and the data protection officer may act for such associations and other bodies representing controllers or processors.
 - (6) The data protection officer must be appointed on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfil the duties set out in Article 26.
 - (7) The data protection officer may be a staff member of the controller or processor, or fulfil the duties on the basis of a service contract.
 - (8) The controller or the processor must publish the contact details of the data protection officer and communicate them to the Authority.
 - (9) Regulations may amend paragraph (1) so as to vary the circumstances in which a data protection officer must be appointed.
 - (10) In this Article “core activities” means the primary activities of the controller and does not mean the activity of processing of personal data where this is an ancillary activity.

25 Position of data protection officer

- (1) The controller and the processor –
 - (a) must ensure that the data protection officer is involved, properly and in a timely manner, in all issues that relate to the protection of personal data;
 - (b) must support the data protection officer in performing the duties set out in Article 26 by providing –
 - (i) the resources, and

- (ii) access to personal data and processing operations, necessary to carry out those duties and to maintain his or her expert knowledge;
 - (c) must ensure that the data protection officer operates independently and does not receive any instructions regarding the performance of those duties other than to perform them to the best of the officer's ability and in a professional and competent manner;
 - (d) must not dismiss or penalize the data protection officer for performing his or her duties other than for failing to perform them as required by sub-paragraph (c).
- (2) The data protection officer must directly report to the highest management level of the controller or the processor.
 - (3) Data subjects may contact the data protection officer with regard to any issue related to processing of their personal data and to the exercise of their rights under this Law.
 - (4) The data protection officer must treat information relating to the performance of his or her duties as confidential, except to the extent that this would be incompatible with his or her duties under this Law or the Authority Law.
 - (5) The data protection officer may carry out other functions but the controller or processor must ensure that any such functions do not result in any conflict of interest as regards the data protection officer's duties under this Law.

26 Duties of data protection officer

- (1) The data protection officer's duties include –
 - (a) informing and advising the controller or the processor and the employees who carry out processing of their obligations under the relevant law;
 - (b) monitoring compliance with this Law and any other enactment relating to data protection and with the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits;
 - (c) providing advice where requested as regards a data protection impact assessment and monitoring the process covered by it;
 - (d) co-operating with the Authority on request;
 - (e) acting as the contact point for the Authority on data processing matters;
 - (f) acting as a contact point for data subjects with regard to all issues relating to the processing of their personal data and exercise of their rights under this Law;
 - (g) with respect to data protection impact assessments, advising on –
 - (i) whether or not to carry out the assessment,
 - (ii) the methodology that should be followed in carrying it out,

- (iii) whether to carry it out in-house or to outsource it,
 - (iv) what safeguards (including technical and organizational measures) to apply to mitigate any risks to the rights and interests of data subjects,
 - (v) whether or not the assessment has been carried out correctly and whether its conclusions (whether or not to go ahead with the processing and what safeguards are to apply) are in compliance with this Law, and
 - (vi) any consultation with the Authority under Article 17 or 18.
- (2) The data protection officer, in the performance of his or her duties, must have due regard to the risk associated with processing operations, taking into account the nature, scope, context and purposes of processing.
- (3) Regulations may amend this Article so as to vary the duties of a data protection officer.

PART 6

RIGHTS OF DATA SUBJECTS

27 Handling of requests by data subjects

- (1) Where so requested by the data subject under the following provisions of this Part, a controller must take such action as the controller considers appropriate, and provide information on the action taken to that data subject, without undue delay and in any event within 4 weeks of receipt of the request.
- (2) The period of 4 weeks may be extended by a further 8 weeks where necessary, taking into account the complexity and number of the requests, and the controller must inform the data subject of any such extension within 4 weeks of receipt of the request, together with the reasons for the delay.
- (3) Where the data subject makes the request by electronic means, the information must be provided by electronic means where possible, unless otherwise requested by the data subject.
- (4) If the controller does not take any action under paragraph (1), the controller must inform the data subject without delay and at the latest within 4 weeks of receipt of the request of the reasons for not taking action and on the possibility of lodging a complaint with the Authority and seeking a judicial remedy.
- (5) Specified information provided under Article 12 and any communication or other action taken under Article 20 or any provision of this Part must be provided free of charge.
- (6) Where requests from a data subject are manifestly vexatious, unfounded or excessive, in particular because of their repetitive character, the burden of proving which is on the controller, the controller may either –

- (a) charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the other action requested; or
 - (b) refuse to act on the request.
- (7) Without limiting Article 5, where the controller has reasonable doubts concerning the identity of the individual making any request under this Part, the controller may request the provision of additional information necessary to confirm the identity of the data subject and is not obliged to enable the individual's rights to be exercised unless supplied with that information.
- (8) The controller must communicate any rectification or erasure of personal data or restriction of processing carried out in accordance with Articles 31 to 33 to each recipient to whom the personal data have been disclosed, unless this is impossible or involves disproportionate effort, and must inform the data subject about those recipients if the data subject requests it.
- (9) Regulations may amend this Article so as to vary any of the requirements specified, or any provision as to the manner in which requests to exercise those requirements must or may be made.

28 Right of access requests: general

- (1) An individual is entitled to be informed by a controller whether personal data of which that individual is the data subject are being processed by or on behalf of that controller, and, if that is the case, to be given information as to –
- (a) the purposes for which they are being or are to be processed by or on behalf of that controller;
 - (b) the categories of personal data concerned;
 - (c) the recipients or classes of recipients to whom they are or may be disclosed by or on behalf of that controller, in particular recipients in third countries or international organizations;
 - (d) where possible, the envisaged period for which the personal data will be stored or, if not possible, the criteria used to determine that period;
 - (e) the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject under Articles 31 to 33 or to object to such processing;
 - (f) the right to lodge a complaint with the Authority;
 - (g) where the personal data are not collected from the data subject, any available information as to their source; and
 - (h) the existence of automated decision-making referred to in Article 38(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

-
- (2) Where personal data are transferred to a third country or to an international organization, the data subject has the right to be informed of the appropriate safeguards under Article 67 relating to the transfer.
 - (3) Without limiting the rights and freedoms of other persons, a data subject is entitled to obtain from the relevant controller the following in intelligible form –
 - (a) the information constituting any personal data of which the individual is the data subject and a copy of that data; and
 - (b) further copies of those data on payment of a fee of such amount as will enable the controller to cover its administrative costs.
 - (4) If the supplying of information under this Article would require the disclosing of information relating to another individual who can be identified from that information, the controller is not obliged to enable such information to be supplied unless –
 - (a) the other individual has consented to the disclosure of the information to the person making the request; or
 - (b) it is reasonable in all the circumstances to do so without the consent of the other individual.
 - (5) In paragraph (4), the reference to information relating to another individual includes a reference to information identifying that individual as the source of the information sought in the request.
 - (6) Paragraph (4) is not to be construed as excusing a controller from communicating so much of the information sought in the request as can be communicated without disclosing the identity of the other individual concerned, whether by the omission of names or other identifying particulars or otherwise.
 - (7) For the purposes of paragraph (4)(b), regard must be had, in particular, to –
 - (a) any duty of confidentiality owed to the other individual;
 - (b) any steps taken by the controller to seek the consent of the other individual;
 - (c) whether the other individual is capable of giving consent; and
 - (d) any express refusal of consent by the other individual.

29 Right of access requests: information contained in health records

- (1) A controller who is not a health professional must not, on the ground of the exemption in Article 61(2), refuse a request under Article 28 for information contained in a health record unless –
 - (a) after receiving the request, the controller consulted the appropriate health professional on the question whether the exemption applies and obtained his or her a written opinion that it does so apply; or
 - (b) the following conditions are satisfied –
 - (i) the controller consulted a health professional before receiving the request,

-
- (ii) the health professional was the health professional who would, if the controller had carried out the consultation under sub-paragraph (a), have been the appropriate health professional, and
 - (iii) the controller obtained a written opinion from the health professional that the exemption applied to the information.
 - (2) The conditions referred to in paragraph (1)(b) are taken not to be satisfied if the opinion was obtained –
 - (a) before the start of the period of 26 weeks that ends at the beginning of the 4-week period referred to in Article 27(1) in respect of the request; or
 - (b) within that period of 26 weeks but it is reasonable in all the circumstances to consult the appropriate health professional again.
 - (3) A controller who is not a health professional must not supply information contained in a health record in response to a request under Article 28 unless the controller has first consulted the appropriate health professional on the question whether the exemption set out in Article 61(2) applies with respect to the information.
 - (4) Paragraph (3) does not operate in relation to a request to the extent that the request relates to information that the controller is satisfied has previously been supplied to the data subject or is already within the knowledge of the data subject.
 - (5) Paragraph (3) does not operate in relation to a request if the following conditions are satisfied –
 - (a) the controller consulted a health professional before receiving the request;
 - (b) the health professional was the health professional who would, if the controller had carried out the consultation under paragraph (3), have been the appropriate health professional;
 - (c) the controller obtained a written opinion from the health professional that the exemption set out in Article 61(2) did not apply with respect to the information that is the subject of the request.
 - (6) In this Article, “appropriate health professional” means –
 - (a) if the controller is the Minister for Social Security and the personal data are processed in connection with the exercise of the functions conferred on him or her in respect of health insurance or social security, a health professional who appears to the controller to have the necessary experience and qualifications to advise on the matters to which the information relates;
 - (b) in other cases, the health professional who appears to the controller to be currently or to have been most recently responsible for the clinical care of the data subject in connection with the matters to which the information relates.
 - (7) If, in the application of paragraph (6), more than one health professional would be chosen, the appropriate health professional is the one who

appears to the controller to be the most suitable to advise on the matters to which the information relates.

- (8) If, in the application of paragraph (6), no health professional would be chosen, the appropriate health professional is a health professional who appears to the controller to have the necessary experience and qualifications to advise on the matters to which the information relates.

30 Treatment of right of access requests

- (1) Regulations may provide that, in such cases as may be prescribed, a request under Article 28 for information referred to in any provision of Article 28 is to be treated as a request for information referred to in any other provision of Article 28.
- (2) Article 28(1)(h) is not to be regarded as requiring the provision of information as to the logic involved in any decision-taking to the extent that the information constitutes a trade secret.
- (3) Information supplied under Article 28 must be supplied by reference to the data in question at the time when the request for the data is received, except that account may be taken of any amendment or deletion made between that time and the time when the information is supplied, being an amendment or deletion that would have been made regardless of the receipt of the request.
- (4) For the purposes of Article 28(5) and (7), another individual can be identified from the information being disclosed if the individual can be identified from that information, or from that and any other information that, in the reasonable belief of the controller, is likely to be in, or to come into, the possession of the data subject making the request.

31 Right to rectification

- (1) A data subject who disputes the accuracy or completeness of personal data may make a written request to the controller to rectify or change the personal data, stating the inaccuracy or explaining why the personal data is incomplete.
- (2) Before complying with a request under paragraph (1) the controller may require from the data subject such further information as may be appropriate regarding the purposes of processing the data in order to verify that the requested rectification or completion is accurate.
- (3) On consideration of a request under paragraph (1), the controller must –
 - (a) where the controller is able, by taking reasonable steps, to confirm that the personal data are inaccurate or incomplete, rectify or complete the data;
 - (b) where the controller is satisfied as to the accuracy and completeness of the personal data, take no action regarding the data; or
 - (c) where it is not reasonable to expect the controller to confirm or verify the accuracy or completeness of the personal data, 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.

- (4) Without limiting paragraph (2), before taking any action under paragraph (3)(c) the controller may request that the data subject provide a written statement that includes information as to the additional data needed to rectify or complete it.

32 Right to erasure

- (1) Where so required by the data subject the controller must erase personal data without undue delay where one of the following grounds applies –
 - (a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
 - (b) the data subject withdraws consent given under paragraph 1 or 6 of Schedule 2 and there is no other legal ground for the processing;
 - (c) the data subject objects to the processing –
 - (i) under Article 35, where there are no overriding legitimate grounds or reasons of public interest for the processing, or
 - (ii) under Article 36;
 - (d) the personal data have been unlawfully processed;
 - (e) the personal data have to be erased for compliance with a legal obligation under the relevant law to which the controller is subject;
 - (f) the personal data have been collected in relation to the offer of information society services directly to a child who is unable to give valid consent under Article 11(4).
- (2) Where the controller has made the personal data public and is obliged under paragraph (1) to erase it, the controller, taking account of available technology and the cost of implementation, must take reasonable steps, including technical measures, to inform other controllers that are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data.
- (3) Paragraphs (1) and (2) do not apply to the extent that processing is necessary –
 - (a) for exercising the rights of freedom of expression and information;
 - (b) for compliance with a legal obligation which requires processing by the relevant law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
 - (c) for reasons of public interest in the area of public health in accordance with paragraph 16 of Schedule 2;
 - (d) for any purposes described in paragraph 17 of Schedule 2 (archiving and research) in so far as the right referred to in paragraph (1) is likely to render impossible or seriously impair the achievement of the objectives of that processing; or
 - (e) for the establishment, exercise or defence of legal claims.

-
- (4) Regulations may prescribe further circumstances in which the right to erasure of personal data may or may not be exercised including the establishment of time limits for that erasure.

33 Right to restriction of processing

- (1) The data subject has the right to obtain from the controller restriction of processing where one of the following circumstances applies –
- (a) the accuracy of the personal data is contested by the data subject, for such a period as will enable the controller to verify the accuracy of the personal data;
 - (b) the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead;
 - (c) the controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims;
 - (d) the data subject has objected to processing under Articles 35 pending the verification whether the legitimate grounds or reasons of public interest of the controller override those of the data subject.
- (2) Where processing has been restricted under paragraph (1), the personal data affected, with the exception of storage, may be processed only –
- (a) with the data subject's consent;
 - (b) for the purposes set out in paragraph 12 of Schedule 2 (legal proceedings etc.);
 - (c) for the purposes set out in paragraph 3 or 9 of Schedule 2 (vital interests); or
 - (d) for the purposes set out in paragraph 14 of Schedule 2 (public interest).
- (3) The controller must inform a data subject who has obtained restriction of processing under paragraph (1) before lifting the restriction of processing.

34 Right to data portability

- (1) Where paragraph (2) applies the data subject has the right –
- (a) to receive the personal data concerning him or her that he or she has provided to a controller in a structured, commonly used and machine-readable format; and
 - (b) to transmit those data to another controller where technically feasible without hindrance from the controller to which the personal data have been provided.
- (2) This paragraph applies where –
- (a) the processing is based on consent under paragraph 1 or 6 of Schedule 2 or on a contract under paragraph 2 of that Schedule; and
 - (b) the processing is carried out by automated means.

- (3) In exercising his or her right to data portability under paragraph (1), the data subject has the right to have the personal data transmitted directly from one controller to another, where technically feasible.
- (4) The exercise of the right referred to in paragraph (1) does not affect the right to erasure under Article 32 save that the right to erasure does not apply to processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.
- (5) The right referred to in paragraph (1) does not apply to the extent that to comply with it would adversely affect the rights and freedoms of others.

35 Right to object to processing for purpose of public functions or legitimate interests

- (1) Where the processing of any personal data is based exclusively on the conditions in paragraph 4 (public functions) or 5 (legitimate interests) of Schedule 2, or any combination of those conditions –
 - (a) the data subject has the right to object to the processing; and
 - (b) the controller must notify the data subject of the processing and the data subject's right to object to it.
- (2) The notification required by paragraph (1)(b) must be given to the data subject –
 - (a) at or before the time of the controller's first communication with the data subject;
 - (b) explicitly; and
 - (c) separately from any other matters notified to the data subject.
- (3) Subject to paragraph (4), the controller must cease the processing if the data subject objects to the processing in accordance with paragraph (1)(a) by written notice to the controller, including, where the processing is in the context of information society services, by notice given by automated means and, if appropriate, using technical specifications to do so.
- (4) Paragraph (3) does not apply where the controller demonstrates that there are compelling legitimate or public interests in continuing to process the data that –
 - (a) outweigh the interests, rights and freedoms of the data subject; or
 - (b) are necessary for the establishment, exercise or defence of legal claims.

36 Right to object to processing for direct marketing purposes

- (1) Where the processing of any personal data is for direct marketing purposes –
 - (a) the data subject has the right to object to the processing to the extent that it is related to that direct marketing; and
 - (b) the controller must notify the data subject of the processing and the right to object.

-
- (2) The notification required by paragraph (1)(b) must be given to the data subject –
 - (a) at or before the time of the controller’s first communication with the data subject;
 - (b) explicitly; and
 - (c) separately from any other matters notified to the data subject.
 - (3) The controller must cease the processing if the data subject objects to the processing in accordance with paragraph (1)(a) by written notice to the controller, including, where the processing is in the context of information society services, notice given by automated means and, if appropriate, using technical specifications to do so.

37 Right to object to processing for historical or scientific purposes

- (1) A data subject has the right to object to any processing of personal data where the lawfulness of the processing is based solely on the processing being necessary for any of the purposes set out in paragraph 17 of Schedule 2 (archiving and research).
- (2) Where a data subject has objected in accordance with paragraph (1) to any processing, the controller must cease the processing unless –
 - (a) the purpose for which the personal data is processed relates to an objective that is in the public interest; and
 - (b) the public interest in the objective outweighs the data subject’s interests.

38 Right regarding automated individual decision-making

- (1) The data subject has the right not to be subject to a decision based solely on automated processing that produces legal effects or similarly significantly affects him or her.
- (2) Paragraph (1) does not apply if the decision –
 - (a) is necessary for entering into, or performance of, a contract between the data subject and a controller;
 - (b) is authorized by the relevant law to which the controller is subject and which also lays down suitable measures to safeguard the data subject’s rights and freedoms and legitimate interests; or
 - (c) is based on the data subject’s explicit consent.
- (3) In the cases referred to in paragraph (2)(a) and (c), the controller must implement suitable measures to safeguard the data subject’s rights and freedoms and legitimate interests, including the right to obtain human intervention on the part of the controller, so that the data subject can express his or her point of view and contest the decision.
- (4) Decisions referred to in paragraph (2) must not be based on special category data unless paragraph 6 (consent) or 14 (public interest) of Schedule 2 applies and appropriate safeguards of the data subject’s rights and freedoms and legitimate interests are in place.

39 Certain contractual terms relating to health records void

- (1) A term or condition of a contract is void in so far as it purports to require an individual to supply, or produce, to any other person a record to which this Article applies, or with a copy of such a record or a part of such a record.
- (2) This Article applies to any record that may be obtained by a data subject in the exercise of the right conferred by Article 28 and consists of the information contained in any health record.

PART 7**EXEMPTIONS****DIVISION 1 – GENERAL AND WIDER EXEMPTIONS****40 Effect of this Part**

Except as provided by or under this Part, the transparency and subject rights provisions have effect despite any enactment or rule of law (whether an enactment or rule of law of Jersey or of another jurisdiction) prohibiting or restricting the disclosure, or authorizing the withholding, of information.

41 National security

- (1) The processing of personal data necessary for the purpose of safeguarding national security is exempt from –
 - (a) the data protection principles;
 - (b) the transparency and subject rights provisions;
 - (c) the offence in Article 71; and
 - (d) Parts 3 and 4 of the Authority Law.
- (2) A certificate signed by the Minister for Home Affairs certifying that exemption from all or any of those provisions is or at any time was required for the purpose there mentioned in respect of any personal data is sufficient evidence of that fact.
- (3) The certificate may identify the personal data to which it applies by means of a general description and may, but need not, be expressed to have prospective effect.
- (4) A person directly affected by the issue of the certificate may apply to the Royal Court for review of the decision to issue the certificate.
- (5) If, on such an application, the Court finds that the Minister for Home Affairs did not have reasonable grounds for the decision to issue the certificate, the Court may quash the decision and void the certificate.
- (6) The certificate is conclusively presumed to apply unless a court determines otherwise.

- (7) In proceedings under paragraph (4) a party may claim that a certificate identifying the personal data to which it applies by means of a general description does not apply to the personal data in question.
- (8) A document purporting to be a certificate under this Article must be received in evidence and taken to be such a certificate unless the contrary is proved.
- (9) A document that purports to be certified by or on behalf of the Minister for Home Affairs as a true copy of a certificate is evidence of the certificate in any legal proceedings.
- (10) No power conferred by any provision of Part 9 of this Law or Part 4 of the Authority Law may be exercised in relation to personal data that are exempt from that provision under this Article.

42 Criminal record certifications

Despite anything to the contrary in this Law a person may require another person to provide any criminal record certificate that may lawfully be obtained by, or in relation to, the data subject under any provision of the Police Act 1997 of the United Kingdom as it extends to Jersey.

43 Manual data held by public authorities

Personal data falling within paragraph (d) of the definition “data” in Article 1(1) are exempt from the provisions of this Law except for Articles 28 to 31, this Part and Articles 68 and 71.

44 Academic, journalistic, literary or artistic material

- (1) Personal data that are processed only for special purposes are exempt from the provisions of this Law except for Articles 68 and 69 if –
 - (a) the processing is undertaken with a view to the publication by any person of any academic, journalistic, literary or artistic material;
 - (b) having regard in particular to the importance of freedom of expression, the publication of the data would be in the public interest; and
 - (c) that public interest outweighs the interests of the data subject and the application of those provisions.
- (2) In considering whether publication would be in the public interest, regard may be had to the controller’s compliance with any code of practice that is relevant to the publication in question and the extent to which publication is regulated by any other body, whether in Jersey or not.
- (3) Regulations may make such further provision as may be necessary or expedient as to the balancing of the rights of data subjects and the public interest in freedom of expression in relation to the processing of data for special purposes.
- (4) In this Article “freedom of expression” means the right protected under Article 10 of the European Convention of Human Rights and

Fundamental Freedoms as incorporated in the Human Rights (Jersey) Law 2000⁸.

DIVISION 2 – EXEMPTIONS FROM TRANSPARENCY AND SUBJECT RIGHTS PROVISIONS

45 Crime and taxation

- (1) The processing of personal data is exempt from the transparency and subject rights provisions where it is carried out for any of the following purposes –
 - (a) the prevention, detection, or investigation, anywhere of crime;
 - (b) the apprehension, or prosecution, anywhere of persons who have committed or are alleged to have committed, an offence anywhere;
 - (c) the assessment, or collection, anywhere of any tax or duty, or of any imposition of a similar nature, wherever due;
 - (d) the disclosure to a police officer under Article 32 or 34A, or any Order made under Article 37, of the Proceeds of Crime (Jersey) Law 1999⁹; or
 - (e) the reporting of suspicious activities under any Tax Information Exchange Agreement,

if the application of those provisions would be likely to prejudice any of those purposes.
- (2) Personal data that –
 - (a) are processed for the purpose of discharging functions under any Law; and
 - (b) consist of information obtained for such a purpose from a person who had it in the person's possession for any of the purposes referred to in paragraph (1)(a) to (e),

are exempt from the transparency and subject rights provisions to the same extent as personal data processed for any of the purposes referred to in paragraph (1)(a) to (e) if the application of those provisions would be likely to prejudice any of those purposes.
- (3) Personal data processed by a public authority are exempt from the transparency and subject rights provisions to the extent to which –
 - (a) they consist of a classification applied to the data subject as part of a system of risk assessment operated by that authority for any of the purposes set out in paragraph (4); and
 - (b) the exemption is required in the interests of the operation of the system.
- (4) The purposes are –
 - (a) the assessment or collection of any tax or duty or any imposition of a similar nature;
 - (b) the prevention or detection of crime; or

- (c) the apprehension or prosecution of persons who commit an offence, if the offence concerned involves any unlawful claim for any payment out of, or any unlawful application of, public funds.

46 Corporate finance

- (1) If personal data are processed for the purposes of, or in connection with, a corporate finance service provided by a relevant person –
 - (a) the data are exempt from the transparency and subject rights provisions in any case to the extent to which either –
 - (i) the application of those provisions to the data could affect the price of any instrument already in existence or that is to be or may be created, or
 - (ii) the controller reasonably believes that the application of those provisions to the data could affect the price of any such instrument; and
 - (b) to the extent that the data are not exempt from the transparency and subject rights provisions by virtue of sub-paragraph (a), they are exempt from those provisions if the exemption is required for the purpose of safeguarding an important economic or financial interest of Jersey.
- (2) For the purposes of paragraph (1)(b) a matter may adversely affect an important economic or financial interest of Jersey if it has an inevitable prejudicial effect on –
 - (a) the orderly functioning of financial markets whether in Jersey or elsewhere; or
 - (b) the efficient allocation of capital within an economy whether in Jersey or elsewhere,that would result from the application (whether on an occasional or on a regular basis) of the transparency and subject rights provisions to data to which paragraph (3) applies.
- (3) The data to which this paragraph applies are any personal data to which the application of the transparency and subject rights provisions could, in the reasonable belief of the relevant person affect –
 - (a) a decision, in Jersey or elsewhere, of a person whether or not to deal in, subscribe for, or issue, an instrument that is already in existence or is to be or may be created; or
 - (b) a decision, in Jersey or elsewhere, of a person to act or not to act in a way that is likely to have an effect on a business activity including an effect on –
 - (i) the industrial strategy of a person (whether the strategy is, or is to be, pursued independently or in association with others),
 - (ii) the capital structure of a business, or
 - (iii) the legal or beneficial ownership of a business or asset.
- (4) In this Article –

“corporate finance service” means a service consisting in –

- (a) underwriting in respect of issues of, or the placing of issues of, any instrument;
- (b) advice to businesses on capital structure, industrial strategy and related matters and advice and service relating to mergers and the purchase of businesses; or
- (c) services relating to such underwriting as is mentioned in paragraph (a);

“instrument” means an instrument listed in section B of the Annex to the European Council Directive on investment services in the securities field (93/22/EEC) or an investment within the meaning of the Financial Services (Jersey) Law 1998¹⁰;

“price” includes value;

“relevant person” means –

- (a) a registered person within the meaning of the Financial Services (Jersey) Law 1998 (being a person registered under that Law in respect of investment business within the meaning of that Law) or a person who is exempted by that Law from the obligation to be registered under that Law in respect of such investment business;
- (b) a person who is an authorized person under the Financial Services and Markets Act 2000 of the United Kingdom, or is an exempt person under that Act, in respect of such investment business;
- (c) a person who may be prescribed by Regulations for the purposes of this Article;
- (d) a person who, in the course of the person’s employment, provides to the person’s employer a service falling within paragraph (b) or (c) of the definition of “corporate finance service”; or
- (e) a partner who provides to other partners in the partnership a service falling within either of those paragraphs.

47 Trusts

Personal data in respect of a trust are exempt from the transparency and subject rights provisions to the extent that –

- (a) in the case of a trust the proper law of which is the law of Jersey, the personal data consist of information the withholding of which by the relevant controller is permitted by Article 29 of the Trusts (Jersey) Law 1984¹¹ or the disclosure, erasure or rectification of which by the relevant controller would be contrary to a prohibition or restriction under any rule of law of Jersey; or
- (b) in the case of a trust the proper law of which is the law of a jurisdiction other than Jersey, the personal data consist of information the withholding of which by the relevant controller is permitted by or under the law of that jurisdiction or the disclosure, erasure or rectification of which by the relevant controller would be contrary to a prohibition or restriction under the law of that jurisdiction.

48 Financial loss, charities, health and safety, maladministration and practices contrary to fair trading

- (1) Personal data processed for the purposes of discharging any of the functions to which this Article applies are exempt from the transparency and subject rights provisions in any case to the extent to which the application of those provisions to the data would be likely to prejudice the proper discharge of the function.
- (2) This Article applies to any function listed in paragraph (3) that is –
 - (a) conferred on any person by or under any enactment;
 - (b) conferred on the Crown or a public authority; or
 - (c) of a public nature and exercised in the public interest.
- (3) The functions are –
 - (a) a function designed for protecting members of the public against –
 - (i) financial loss due to dishonesty, malpractice or other seriously improper conduct by, or the unfitness or incompetence of, persons concerned in the provision of banking, insurance, investment or other financial services or in the management of bodies corporate,
 - (ii) financial loss due to the conduct of discharged or undischarged bankrupts, or
 - (iii) dishonesty, malpractice or other seriously improper conduct by, or the unfitness or incompetence of, persons authorized to carry on any profession or other activity;
 - (b) a function designed for protecting charities against misconduct or mismanagement (whether by trustees or other persons) in their administration;
 - (c) a function designed for protecting the property of charities from loss or misapplication;
 - (d) a function designed for the recovery of the property of charities;
 - (e) a function designed for securing the health, safety or welfare of persons at work;
 - (f) a function designed for protecting persons other than persons at work against risk to health or safety arising out of or in connection with the actions of persons at work.
- (4) This Article applies to a function that is conferred by or under any enactment on a prescribed person, or body that is designed –
 - (a) to protect members of the public against –
 - (i) maladministration by public bodies,
 - (ii) failures in services provided by public bodies, or
 - (iii) a failure by a public body to provide a service which it was a function of the body to provide;
 - (b) to protect members of the public against conduct that may adversely affect their interests by persons carrying on a business;

- (c) to regulate agreements, or conduct, that have as their object or effect the prevention, restriction or distortion of competition in connection with any commercial activity; or
 - (d) to regulate conduct on the part of one or more businesses that amounts to the abuse of a dominant position in a market.
- (5) This Article also applies to the following functions –
- (a) any function relating to an investigation by the Jersey Financial Services Commission under –
 - (i) Article 22 of the Collective Investment Funds (Jersey) Law 1988¹²,
 - (ii) Article 28 of the Banking Business (Jersey) Law 1991¹³,
 - (iii) Part 19 of the Companies (Jersey) Law 1991¹⁴,
 - (iv) Article 11 of the Insurance Business (Jersey) Law 1996¹⁵,
 - (v) Article 33 of the Financial Services (Jersey) Law 1998¹⁶,
 - (vi) Regulation 31 of the Alternative Investment Funds (Jersey) Regulations 2012¹⁷,including the functions of any inspector or competent person appointed under any of those provisions;
 - (b) any function conferred on the Jersey Resolution Authority under Article 7 of the Bank (Recovery and Resolution) (Jersey) Law 2017¹⁸;
 - (c) any function under the Proceeds of Crime (Supervisory Bodies) (Jersey) Law 2008¹⁹ of a supervisory body designated under Article 6 of that Law (including the functions of any competent person appointed under Article 31 of that Law);
 - (d) any function conferred on the Office of the Financial Services Ombudsman or on an Ombudsman, under the Financial Services Ombudsman (Jersey) Law 2014²⁰;
 - (e) any function conferred on the Jersey Financial Services Commission by the Financial Services Commission (Jersey) Law 1998²¹;
 - (f) any function conferred on the registrar of companies appointed under Article 196 of the Companies (Jersey) Law 1991²², arising under that Law or any other enactment;
 - (g) any function (whether or not under any of the Laws referred to in this paragraph) that may be prescribed by Regulations.

49 Management forecasts etc.

Personal data processed for the purposes of management forecasting or managing planning to assist the controller in the conduct of any business or other activity are exempt from the transparency and subject rights provisions to the extent to which the application of those provisions would be likely to prejudice the conduct of that business or other activity.

50 Negotiations

Personal data that consist of records of the intentions of the controller in relation to any negotiations with the data subject are exempt from the transparency and subject rights provisions to the extent to which the application of those provisions would be likely to prejudice those negotiations.

51 Information available to public by or under enactment

Personal data are exempt from the transparency and subject rights provisions if the data consist of information that the controller is obliged by or under any enactment to make available to the public, whether by making it available for inspection or publishing it in another manner, and whether gratuitously or on payment of a fee.

52 Disclosure contrary to certain enactments

Personal data that consist of information the disclosure of which by the relevant controller would be contrary to a prohibition or restriction under any of the following enactments are exempt from the transparency and subject rights provisions –

- (a) Articles 24(5), 27(12) and 30(4)(b) of the Adoption (Jersey) Law 1961²³;
- (b) Article 19B of the Misuse of Drugs (Jersey) Law 1978²⁴;
- (c) Article 35 of the Proceeds of Crime (Jersey) Law 1999²⁵;
- (d) Article 35 of the Terrorism (Jersey) Law 2002²⁶.

53 Confidential references given by the controller

Personal data are exempt from the transparency and subject rights provisions if they consist of a reference given or to be given in confidence by the controller for the purposes of –

- (a) the education, training or employment, or prospective education, training or employment, of the data subject;
- (b) the appointment, or prospective appointment, of the data subject to any office; or
- (c) the provision, or prospective provision, by the data subject of any service.

54 Examination scripts etc.

Personal data consisting of information recorded by candidates during an academic, professional or other examination are exempt from the transparency and subject rights provisions.

55 Crown or judicial appointments and honours

Personal data are exempt from the transparency and subject rights provisions if processed for the purposes of assessing a person's suitability for –

- (a) employment by or under the Crown or any office to which appointments are made by Her Majesty;
- (b) any judicial office or the office of Queen's Counsel; or
- (c) the conferring by the Crown of any honour or dignity.

56 Armed forces

Personal data are exempt from the transparency and subject rights provisions to the extent to which the application of those provisions would be likely to prejudice the effectiveness in combat of any of the armed forces of the Crown.

57 Legal professional privilege

Personal data are exempt from the transparency and subject rights provisions if the data consist of information in respect of which a claim to legal professional privilege could be maintained in legal proceedings.

58 Self-incrimination

- (1) Personal data are exempt from the transparency and subject rights provisions to the extent that compliance would, by revealing evidence of the commission of an offence (other than an offence under this Law or the Authority Law), expose the person to proceedings for that offence.
- (2) Information provided in response to a request under the transparency and subject rights provisions or any order enforcing them is not admissible against the person in proceedings for an offence under this Law or the Authority Law.

59 States Assembly privilege

- (1) Personal data are exempt from the transparency and subject rights provisions to the extent required to avoid an infringement of the privileges of the States Assembly.
- (2) Except as provided by paragraph (3), a certificate signed by the Greffier of the States certifying that such an exemption is required to avoid an infringement of the privileges of the States Assembly is conclusive evidence of that fact.
- (3) A person aggrieved by the decision of the Greffier of the States to issue a certificate under paragraph (2) may appeal to the Royal Court on the grounds that the Greffier did not have reasonable grounds for issuing the certificate.
- (4) The decision of the Royal Court on the appeal is final.

DIVISION 3 – EXCEPTIONS TO ARTICLE 27 OR 28**60 Examination marks**

- (1) Where a request under Article 28 is made for or in relation to marking data, the application of Article 27 to the request is modified so that if the day when the controller receives the request under that Article falls before the publication day, for the period expressed as “within 4 weeks of receipt of the request” in Article 27(1) there is substituted the period set out in paragraph (2).
- (2) The period is –
 - (a) within 20 weeks of the receipt of the request; or
 - (b) within 4 weeks of the publication day,whichever ends first.
- (3) If by virtue of paragraph (2) a period longer than the period mentioned in Article 27(1) elapses before the request is complied with, the required information must be supplied both by reference to the data in question at the time when the request is received and (if different) by reference to the data as from time to time held in the period beginning when the request is received and ending when it is complied with.
- (4) In this Article –

“marking data” means marks or other information processed by the controller –

 - (a) for the purpose of determining the results of an academic, professional or other examination of a candidate;
 - (b) for the purpose of enabling such a determination; or
 - (c) in consequence of such a determination;

“publication day”, in relation to any examination and examination candidate, means the day on which the results of the examination are first published or (if not published) when they are first made available or communicated to the candidate concerned.

61 Health, education and social work

- (1) Personal data are exempt from Article 28 if the data are processed by a court and consist of health, education or social work information that –
 - (a) is supplied in a report or other evidence given to the court in the course of proceedings relating to families or children; and
 - (b) the court directs should be withheld from the data subject on the ground that it appears to be –
 - (i) impracticable to disclose the report or other evidence having regard to the data subject’s age and understanding, or
 - (ii) undesirable to disclose the report or other evidence having regard to the serious harm that might thereby be suffered by the data subject.

-
- (2) Personal data consisting of health, education or social work information are exempt from Article 28 in any case to the extent to which the application of that Article would be likely to cause serious harm to the physical or mental health of the data subject or any other person.
 - (3) Where a defined person is enabled by or under any enactment or rule of law to make a request under Article 28 on behalf of a data subject and has made such a request, personal data consisting of information specified in paragraph (4) are exempt from that Article to the extent mentioned in paragraph (4).
 - (4) The extent of the exemption is –
 - (a) in the case of information contained in a health record or social work information, the extent to which the application of Article 28 would result in the disclosure of information –
 - (i) provided by the data subject in the expectation that it would not be disclosed to the person making the request,
 - (ii) 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
 - (iii) that the data subject has expressly indicated should not be so disclosed;
 - (b) in the case of information constituting an educational record and being information whether the data subject, when a child, is or has been the subject of or may be at risk of abuse, the extent to which the application of that Article would not be in the interests of the data subject.
 - (5) Paragraph (4)(a)(i) or (ii) does not apply to the extent that the data subject has expressly indicated that he or she no longer has the expectation there referred to.
 - (6) In relation to personal data consisting of information contained in a health record, Article 28(4) has effect as if the following word and sub-paragraph were added at the end of that paragraph –
 - “; or
 - (c) the information is contained in a health record and the other individual is a health professional who has compiled or contributed to the health record or has been involved in the care of the data subject in the health professional’s capacity as a health professional.”.
 - (7) In relation to personal data consisting of information constituting either an educational record or social work information –
 - (a) Article 28(4) has effect as if the following word and sub-paragraph were added at the end of that paragraph –
 - “; or
 - (c) the other individual is a relevant person.”;
 - (b) Article 28 has effect as if the following paragraph were added after paragraph (7) –

“(8) A person is a relevant person for the purposes of paragraph (4)(c) if he or she –

- (a) in the case of information constituting an educational record, is a teacher or other employee at a school, engaged by the proprietor of a school or working at a school under a contract for the provision of educational services; or
- (b) in the case of social work information, is or has been employed in an administration of the States in connection with functions that are or have been exercised in relation to data consisting of an educational record or social work information that relates to him or her or that he or she supplied in his or her official capacity.”.

(8) In this Article –

“abuse” in respect of a person when that person is a child –

- (a) includes physical injury to, and physical neglect, emotional neglect, ill-treatment, and sexual abuse, of the person;
- (b) does not include accidental injury;

“care” includes examination, investigation, diagnosis and treatment;

“defined person” means a person who –

- (a) has parental responsibility for a child who is the data subject; or
- (b) has been appointed by a court to manage the affairs of the data subject on account of the data subject being incapable of managing his or her own affairs;

“educational record” means a record of information that –

- (a) is processed by or on behalf of the proprietor of, or a teacher at, a school;
- (b) relates to a person who is or has been a pupil at the school; and
- (c) originated from or was supplied by or on behalf of any of the following –
 - (i) a teacher or other employee at the school,
 - (ii) a person engaged by the proprietor of the school under a contract for the provision of educational services,
 - (iii) the pupil to whom the record relates,
 - (iv) a parent of that pupil;

“health, education or social work information” means –

- (a) a health record;
- (b) information constituting an educational record; or
- (c) social work information;

“parent” in relation to a pupil of a school, includes a guardian and every person who has actual custody of the pupil;

“proceedings relating to families or children” includes proceedings relating to adoption, matrimonial matters or guardianship;

“social work information” means personal data processed by the States (including an administration of the States) in relation to any of the following matters –

- (a) the allocation of housing or other residential accommodation;
- (b) the provision of any benefit paid by the Minister for Social Security;
- (c) probation;
- (d) school attendance;
- (e) ensuring that children receive suitable education whether by attendance at school or otherwise;
- (f) guardianship;
- (g) a function under the Children (Jersey) Law 2002²⁷ or any legislation relating to mental health.

62 Credit reference agency as controller

- (1) If a controller is a credit reference agency, Article 28 applies in relation to that controller subject to this Article.
- (2) An individual may limit a request to a controller under Article 28 to personal data relevant to the financial standing of the individual, and is taken to have so limited the request unless the request shows a contrary intention.
- (3) If personal data are being processed by or on behalf of a controller who receives a request under Article 28 from an individual who is the data subject of those data, the obligation to supply information under that Article includes an obligation to give the individual a statement of any other rights arising in respect of a credit reference agency in any other enactment in such form, and to such extent, as may be prescribed by Regulations.
- (4) In this Article “credit reference agency” means a person who carries on the business of providing information about the financial standing of persons.

63 Unstructured personal data held by scheduled public authorities

- (1) A scheduled public authority is not obliged to comply with Article 28(1) in relation to any unstructured personal data unless the request under that Article contains a description of the data.
- (2) Even if a request contains a description of data as referred to in paragraph (1), a scheduled public authority is not obliged to comply with Article 28(1) in relation to unstructured personal data if the authority estimates that the cost of complying with the request in so far as it relates to those data would exceed a prescribed limit.
- (3) Paragraph (2) does not exempt the scheduled public authority from its obligation under Article 28(1) to inform an individual whether unstructured personal data of which that individual is the data subject are

being processed by or on behalf of the controller unless the estimated costs of complying with that obligation alone in relation to those data would exceed a limit specified by the States in Regulations.

- (4) Any estimate for the purposes of this Article must be made in accordance with Regulations under Article 16 of the Freedom of Information (Jersey) Law 2011²⁸ (whether or not any limit specified in Regulations for the purposes of this Article is the same as any amount determined in accordance with Regulations under that Article).
- (5) In this Article “unstructured personal data” means any personal data consisting of recorded information held by a scheduled public authority other than data that is –
 - (a) processed by automated means in response to instructions given for that purpose or recorded with the intention that it be so processed; or
 - (b) recorded as part of a filing system or with the intention that it should form part of a filing system.

DIVISION 4 – PERMISSIONS AND EXEMPTIONS BY REGULATIONS

64 Permitted processing for law enforcement, legal proceedings and public records purposes

- (1) Despite any provision of this Law the processing (including the disclosure) of personal data in either of the circumstances set out in paragraph (2) is permitted –
 - (a) for a purpose other than the purpose for which it was collected; and
 - (b) without the consent of the data subject.
- (2) The circumstances are –
 - (a) that the processing is for the purposes set out in Article 45(1); or
 - (b) where disclosure is made for the purposes of paragraph 12 of Schedule 2 (legal proceedings etc.).
- (3) Despite the data protection principles set out in Article 8(1)(c), (d) and (e), the processing (including disclosure) of personal data to which paragraph (4) applies is permitted.
- (4) This paragraph applies to information that the controller is obliged to make available to the public by or under any enactment, whether by making it available for inspection or publishing it in another manner, and whether it is available gratuitously or on the payment of a fee.

65 Exemptions by Regulations

- (1) Regulations may exempt the processing (including disclosure) of personal data from any provision of this Law.
- (2) However, the power to make Regulations under paragraph (1) may be exercised only to the extent that –

- (a) it is considered necessary for particular purposes, or in particular circumstances, that are in the public interest; or
 - (b) the public interest is not outweighed by the public interest in protecting the rights and freedoms of data subjects.
- (3) The power to make Regulations under this Article includes a power –
- (a) to modify or amend any enactment (including this Law) to the extent that it might otherwise prevent the processing (including disclosure) of personal data; and
 - (b) to put in place particular safeguards for the rights of data subjects or any other persons with respect to any processing carried out in furtherance of any new permission to process such data.
- (4) The States must consult the Authority before making any Regulations under paragraph (3).

PART 8

CROSS-BORDER DATA TRANSFERS

66 General principles for cross-border data transfers

- (1) A controller or a processor must not transfer personal data for processing or in circumstances where the controller or processor knew or should have known that it will be processed after the transfer to a third country or an international organization, unless that country or organization ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.
- (2) The level of protection referred to in paragraph (1) is adequate if –
- (a) the Commission has so decided, by means of an implementing act under Article 45 of the GDPR;
 - (b) there are appropriate safeguards in place that meet the requirements of Article 66; or
 - (c) the transfer falls within the exceptions set out in Schedule 3.
- (3) Regulations may –
- (a) amend Schedule 3;
 - (b) make further provision about international transfers of data.

67 Transfer subject to appropriate safeguards

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

-
- (2) The appropriate safeguards referred to in paragraph (1) may be provided for, without requiring any specific authorization from the Authority, by –
- (a) a legally binding and enforceable instrument between public authorities;
 - (b) binding corporate rules approved by the Authority as complying with Schedule 4 or approved by another competent supervisory authority under Article 46 of the GDPR, or equivalent statutory provisions;
 - (c) standard data protection clauses adopted by the Authority or by a competent supervisory authority and approved by the Commission in accordance with the examination procedure referred to in Article 93(2) of the GDPR;
 - (d) a code or any other code approved by another competent supervisory authority under Article 40 of the GDPR or equivalent statutory provisions, together with binding and enforceable commitments of the controller, processor or recipient in the third country or international organization to apply the appropriate safeguards, including as regards data subjects' rights; or
 - (e) the controller, processor or recipient in the third country having been certified in accordance with a certification mechanism either provided for in Regulations under Article 80 or approved by another competent supervisory authority under Article 42 of the GDPR.
- (3) Subject to specific authorization from the Authority and where there is a mechanism for data subjects to enforce their data subject rights and obtain effective legal remedies against the controller, processor or recipient of that personal data in the jurisdiction concerned, the appropriate safeguards referred to in paragraph (1) may also be provided for by –
- (a) contractual clauses between the controller or processor and the controller, processor or the recipient of the personal data in the third country or international organization; or
 - (b) where both the transferor and the controller, processor or recipient of the personal data in the third country or international organization concerned are public authorities, provisions in administrative arrangements between those public authorities that include enforceable and effective data subject rights.
- (4) In determining whether to authorize a transfer under this Article, the Authority must have regard to factors that include, but are not limited to, any opinions or decisions of the European Data Protection Board under Article 64, 65 or 66 of the GDPR that appear to the Authority to be relevant.

PART 9**REMEDIES AND ENFORCEMENT****68 Proceedings against controllers**

- (1) A data subject who considers that the transparency and subject rights provisions have been or will be contravened, may bring proceedings against the controller responsible for the contravention in the Royal Court under this Article.
- (2) Where the Royal Court is satisfied that those rights have been or will be contravened the court may make such order as it considers appropriate, including –
 - (a) an award of compensation for loss, damage or distress in respect of the contravention;
 - (b) an injunction (including an interim injunction) to restrain any actual or anticipated contravention;
 - (c) a declaration that the controller is responsible for the contravention or that a particular act, omission or course of conduct on the part of the controller would result in a contravention; and
 - (d) requiring the controller to give effect to the transparency and subject rights provisions.
- (3) Nothing in this Article limits any other right or remedy that a data subject may have against a controller or processor.
- (4) Where –
 - (a) a person has made a right of access request under Article 28; and
 - (b) the Royal Court is satisfied, on the application of a third party that compliance with that request is likely to cause the third party to suffer serious harm to his or her physical or mental health or condition,the court may order the controller not to comply with the request.

69 Compensation

- (1) Any person who suffers loss, damage or distress by reason of any contravention of this Law by a controller or processor is entitled to compensation.
- (2) Controllers or processors against whom any claim for compensation is made under this Article or Article 30 of the Authority Law who prove that they are not responsible for the event giving rise to the loss, damage or distress are exempt from any liability to pay that compensation.
- (3) A processor is exempt from liability for damages under any action for loss, damage or distress unless the processor –
 - (a) has contravened any obligation imposed on processors by this Law; or

- (b) has acted outside or contrary to lawful instructions given by the controller.
- (4) Where one or more controllers or processors are involved in the same processing that caused the loss, damage or distress, each such controller and processor is jointly and severally liable for the loss, damage or distress.
- (5) A controller or processor is entitled to reimbursement, in respect of compensation paid out by that controller or processor from each of the other controllers or processors involved in the processing that gave rise to the liability for compensation, of that part of the compensation corresponding to that other controller or processor's responsibility for the loss, damage or distress.

70 Representation of data subjects

- (1) Any person who has standing to make a complaint or commence proceedings under this Law or the Authority Law may authorize a data protection organization on that person's behalf to –
 - (a) make a complaint against the Authority under Article 19 of the Authority Law; or
 - (b) bring proceedings (including any appeal proceedings) in respect of a contravention of this Law by a controller or processor, or for compensation,and represent the person in any proceedings arising from that complaint or those proceedings and to exercise any right of the data subject on his or her behalf.
- (2) In this Article “data protection organization” means any non-profit association (as described in paragraph 10(a) of Schedule 2) properly constituted in accordance with relevant law that has objectives in the public interest and is active in the field of the protection of data subject rights.

71 Unlawful obtaining etc. of personal data

- (1) A person must not knowingly or recklessly, without the consent of the relevant controller –
 - (a) obtain or disclose personal data or the information contained in personal data; or
 - (b) procure the disclosure to another person of the information contained in personal data.
- (2) A person who contravenes paragraph (1) is guilty of an offence.
- (3) A person does not contravene paragraph (1) if the person shows that –
 - (a) the obtaining, disclosing or procuring was necessary for the purpose of preventing or detecting crime, or was required or authorized by or under any enactment, by any rule of law or by the order of a court;

- (b) the person acted in the reasonable belief that the person had in law the right to obtain or disclose the data or information or, as the case may be, to procure the disclosure of the information to the other person;
 - (c) the person acted in the reasonable belief that the person would have had the consent of the controller if the controller had known of the obtaining, disclosing or procuring and the circumstances of it; or
 - (d) in the circumstances of the case, the obtaining, disclosing or procuring was justified as being in the public interest.
- (4) A person who sells personal data is guilty of an offence if the person has obtained the data in contravention of paragraph (1).
- (5) A person who offers to sell personal data is guilty of an offence if –
- (a) the person has obtained the data in contravention of paragraph (1); or
 - (b) the person subsequently obtains the data in contravention of that paragraph.
- (6) For the purposes of paragraph (5), an advertisement indicating that personal data are or may be for sale is an offer to sell the data.
- (7) For the purposes of paragraphs (4) to (6), “personal data” includes information extracted from personal data.

72 Requirement to produce certain records illegal

- (1) A person must not, in connection with –
- (a) the recruitment of another person as an employee;
 - (b) the continued employment of another person; or
 - (c) any contract for the provision of services to the person by another person,
- require that other person or a third party to supply or produce a relevant record to the first person.
- (2) A person concerned with the provision (for payment or not) of goods, facilities or services to the public (or a section of the public) must not, as a condition of providing or offering to provide any goods, facilities or services to another person, require that other person or a third party to supply or produce a relevant record to the first person.
- (3) A person does not contravene paragraph (1) or (2) if the person shows that –
- (a) the imposition of the requirement was required or authorized by or under any enactment, by any rule of law or by the order of a court; or
 - (b) in the particular circumstances the imposition of the requirement was justified as being in the public interest.
- (4) A person who contravenes paragraph (1) or (2) is guilty of an offence and liable to a fine of level 3 on the standard scale.

- (5) For the purposes of this Article, a record that states that a controller is not processing any personal data relating to a particular matter is taken to be a record containing information relating to that matter.
- (6) In this Article (including the Table to this Article) –
- “caution” means a caution given to any person in Jersey in respect of an offence that, at the time when the caution is given, is admitted;
- “conviction” has the same meaning as in the Rehabilitation of Offenders (Jersey) Law 2001²⁹;
- “employee” means an individual who works under a contract of employment, or holds any office, whether or not entitled to remuneration and “employment” shall be construed accordingly;
- “relevant record” means any record that –
- (a) has been or is to be obtained by a data subject from a controller specified in the first column of the Table to this Article in the exercise of the rights conferred by the transparency and subject rights provisions; and
- (b) contains information relating to a matter specified in relation to the controller in the second column of that Table,
- and includes a copy of such a record or a part of such a record.
- (7) A record is not a relevant record to the extent that it relates, or is to relate, only to personal data falling within paragraph (d) of the definition “data” in Article 1(1).
- (8) Regulations may amend the Table to this Article and the definitions of “caution” and “conviction” in paragraph (6).

TABLE	
<i>Controller</i>	<i>Subject-matter</i>
1. Chief Officer of the States of Jersey Police Force	Convictions, cautions
2. A member of the honorary police of any of the 12 Parishes of Jersey	Cautions
3. Minister for Home Affairs	Convictions, cautions, functions of that Minister under the Prison (Jersey) Law 1957
4. Minister for Social Security	Convictions, cautions, functions of that Minister under any enactment of Jersey

73 False information

- (1) A person who knowingly or recklessly provides the Authority, or any other person entitled to information under this Law, the Authority Law or Regulations made under those Laws, with information that is false or misleading in a material particular, is guilty of an offence.

-
- (2) However, no offence is committed under paragraph (1) unless the information is provided –
 - (a) in connection with an application under this Law or the Authority Law;
 - (b) in purported compliance with a requirement imposed under this Law, the Authority Law or under Regulations made under those Laws; or
 - (c) otherwise than as mentioned in paragraph (1) but in circumstances in which the person providing the information intends, or could reasonably be expected to know, that the information will be used by the Authority for the purpose of carrying out the Authority's functions under this Law or the Authority Law.
 - (3) A person guilty of an offence under this Article is liable to imprisonment for a term of 2 years and to a fine.

74 Obstruction

- (1) A person must not do any of the following in relation to any person to whom this paragraph applies –
 - (a) intentionally obstruct or impede the person;
 - (b) interfere with, or cause or knowingly permit to be interfered with, anything done by the person;
 - (c) fail to give to the person any assistance or information that is reasonably required;
 - (d) fail to produce a record when required to do so by the person;
 - (e) fail to co-operate with the exercise of any power under Schedule 1 to the Authority Law.
- (2) Paragraph (1) applies to the Authority and any other person acting in the execution or enforcement of this Law or the Authority Law.
- (3) A person who contravenes paragraph (1) is guilty of an offence and in the case of an offence under paragraph (1)(a) or (b), is liable to imprisonment for a term of 2 years and to a fine.

75 General provisions relating to offences

- (1) A person guilty of an offence under this Law is liable to a fine except where this Law otherwise provides.
- (2) Where an offence under this Law, or under Regulations made under this Law, committed by a limited liability partnership or body corporate or unincorporated body is proved to have been committed with the consent or connivance of, or to be attributable to any neglect on the part of –
 - (a) a person who is a partner of the limited liability partnership, or director, manager, secretary or other similar officer of the body corporate;
 - (b) in the case of any other partnership, any partner;

- (c) in the case of any other unincorporated body, any officer of that body who is bound to fulfil any duty of which the offence is a breach or, if there is no such officer, any member of the committee or other similar governing body; or
- (d) any person purporting to act in any capacity described in subparagraph (a), (b) or (c),

the person is also guilty of the offence and liable in the same manner as the partnership or body corporate to the penalty provided for that offence.

- (3) If the affairs of a body corporate are managed by its members, paragraph (2) applies in relation to acts and defaults of a member in connection with the member's functions of management as if the member were a director of the body corporate.
- (4) Where an offence under this Law is alleged to have been committed by an unincorporated body, proceedings for the offence must, without limiting paragraph (2), be brought in the name of the body and not in the name of any of its members.
- (5) A fine imposed on an unincorporated body on its conviction for an offence under this Law must be paid from the funds of the body.
- (6) A person who aids, abets, counsels or procures the commission of an offence under this Law is also guilty of the offence and liable in the same manner as a principal offender to the penalty provided for that offence.

76 Proceedings concerning unincorporated bodies

Subject to Article 75, where a contravention of this Law is alleged to have been committed by an unincorporated body, any complaint, investigation, action, order or notice, or other proceedings, for or otherwise in relation to the contravention must be brought, issued or (as the case may be) served in the name of the body and not in the name of any of its members.

77 Rules of Court

- (1) The power to make Rules of Court under Article 13 of the Royal Court (Jersey) Law 1948³⁰ includes the power to make Rules regulating the practice and procedure on any matter relating to the Royal Court under this Law.
- (2) The Rules may, in particular, make provision enabling –
 - (a) directions to be given to withhold material or restrict disclosure of any information relevant to proceedings under this Law from any party (including any representative of any party) to the proceedings; and
 - (b) the court to conduct such proceedings in the absence of any person, including a party to the proceedings (or any representative of a party to the proceedings).
- (3) In making the Rules, regard must be had to –
 - (a) the need to secure that the decisions that are the subject of such proceedings are properly reviewed; and

- (b) the need to secure that disclosures of information are not made where they would be contrary to the public interest.

PART 10

MISCELLANEOUS

78 Codes of conduct

- (1) The Authority may approve a code of conduct or an amendment or extension of a code of conduct, prepared by any person representing a category of controllers or processors for the purposes of –
 - (a) encouraging or facilitating compliance with this Law; or
 - (b) allowing controllers or processors that are not otherwise subject to this Law to demonstrate that they have appropriate safeguards for the protection of personal data, for the purposes of personal data transfers to third countries or international organizations under Article 67.
- (2) A code may include any provisions relating to the following –
 - (a) fair and transparent processing;
 - (b) the legitimate interests pursued by controllers in specific contexts;
 - (c) the collection of personal data;
 - (d) the pseudonymization of personal data;
 - (e) the information provided to the public and to data subjects;
 - (f) the exercise of the rights of data subjects;
 - (g) the information provided to, and the protection of, children, and the manner in which the consent of the persons with parental responsibility for children is to be obtained;
 - (h) any steps or measures required to be established, taken or carried out by controllers or processors under this Law;
 - (i) the notification of personal data breaches to supervisory authorities and the communication of such personal data breaches to data subjects;
 - (j) the transfer of personal data to third countries or international organizations;
 - (k) out-of-court proceedings and other dispute resolution procedures for resolving disputes between controllers and data subjects with regard to processing, without affecting the rights of data subjects under this Law; or
 - (l) any other matter relating to compliance with this Law or appropriate safeguards for the protection of personal data.
- (3) An approval under paragraph (1) is effected by the Authority's registering and publishing the code in any manner that the Authority considers fit.
- (4) The Authority must not approve a code unless –

-
- (a) the code provides for a person accredited by the Authority (or another competent supervisory authority) to monitor compliance with the code by controllers and processors who purport to apply or implement the code;
 - (b) the code requires any controller or processor established in a third country that purports to apply or implement the code to enter into legally binding and enforceable commitments to apply or implement provisions of the code;
 - (c) where the code relates to processing operations in a Member State, the Commission has, by way of an implementing act under the GDPR, stated that the code has general validity within the EU; and
 - (d) The Authority considers that –
 - (i) the contents of the code comply with this Law, and
 - (ii) the code provides appropriate safeguards for the protection of personal data.
- (5) In determining whether or not to approve a code, the Authority must take into account –
- (a) the particular circumstances of the various sectors in which processing or personal data takes place and to which the code relates; and
 - (b) the needs of different sizes of enterprises or establishments that are controllers or processors to which the code applies.

79 Accreditation and duties of accredited person

- (1) For the purposes of Article 78(4)(a), the Authority may accredit any person (the “accredited person”) to monitor compliance with a code if the Authority considers that the person has –
 - (a) adequate expertise and independence in relation to the subject-matter of the code;
 - (b) established procedures that allow it to assess the eligibility of controllers and processors concerned to apply the code, to monitor their compliance with its provisions and to review periodically the implementation of the code;
 - (c) established procedures and structures to handle complaints about infringements of the code or the manner in which the code has been, or is being, implemented by a controller or processor, and to make those procedures and structures transparent to data subjects and the public; and
 - (d) no conflict of interests in connection with the discharge or performance of its other tasks and duties.
- (2) In cases of infringement of the code by any controller or processor that purports to apply or implement the code, the accredited person must –
 - (a) take appropriate action including suspension or exclusion from the code where appropriate; and
 - (b) notify the Authority of any action taken by the person and the reasons for the action.

- (3) The Authority may suspend or revoke an accreditation under paragraph (1) if –
 - (a) the conditions for accreditation are not, or are no longer, met; or
 - (b) the accredited person contravenes paragraph (2).

80 Regulations establishing certification mechanism

- (1) Regulations may provide for the establishment of mechanisms, seals or marks to certify or signify –
 - (a) that particular processing operations by controllers or processors comply with this Law; or
 - (b) the existence of appropriate safeguards for the protection of personal data provided by controllers or processors established in a third country for the purposes of personal data transfers to third countries or international organizations as provided for by Article 66.
- (2) Regulations made under paragraph (1) may amend the Authority Law so as to confer or impose functions on the Authority in consequence of the Regulations.

81 Application to public sector

- (1) This Law binds the Crown.
- (2) The application of this Law extends to the States and any Minister, department, or administration, of the States, and each such department, or administration is taken to be a separate person.
- (3) For the purposes of this Law, if an order, requirement, direction, notice or other instrument is imposed or served on the head of a department of the States or the head of an administration of the States –
 - (a) it is taken to have been imposed or served on the department or administration of which that person is the head; and
 - (b) if it requires compliance, the head must ensure that it is complied with.

82 Service of notices etc.

- (1) A notice required by this Law to be given to the Authority is not regarded as given until it is in fact received by the Authority.
- (2) A notice or other document required or authorized under this Law or under Regulations made under this Law to be given to the Authority may be given by electronic or any other means by which the Authority may obtain or recreate the notice or document in a form legible to the naked eye.
- (3) Any notice, direction or other document required or authorized by or under this Law to be given to or served on any person other than the Authority may be given or served –

-
- (a) by delivering it to the person;
 - (b) by leaving it at the person's proper address;
 - (c) by sending it by post to the person at that address; or
 - (d) by sending it to the person at that address by electronic or any other means by which the notice, direction or document may be obtained or recreated in a form legible to the naked eye.
 - (4) Without limiting the generality of paragraph (3), any such notice, direction or other document may be given to or served on a partnership, company incorporated outside Jersey or an unincorporated association by being given to or served –
 - (a) in any case, on a person who is, or purports (under whatever description) to act as, its secretary, clerk or other similar officer;
 - (b) in the case of a partnership, on the person having the control or management of the partnership business;
 - (c) in the case of a partnership or company incorporated outside Jersey, on a person who is a principal person in relation to it (within the meaning of the Financial Services (Jersey) Law 1998); or
 - (d) by being delivered to the registered or administrative office of a person referred to in sub-paragraph (a), (b) or (c) if the person is a body corporate.
 - (5) For the purposes of this Article and of Article 7 of the Interpretation (Jersey) Law 1954³¹, the proper address of any person to or on whom a notice, direction or other document is to be given or served by post is the person's last known address, except that –
 - (a) in the case of a company (or person referred to in paragraph (4) in relation to a company incorporated outside Jersey) it is the address of the registered or principal office of the company in Jersey; and
 - (b) in the case of a partnership (or person referred to in paragraph (4) in relation to a partnership) it is the address of the principal office of the partnership in Jersey.
 - (6) If the person to or on whom any notice, direction or other document referred to in paragraph (3) is to be given or served has notified the Authority of an address within Jersey, other than the person's proper address within the meaning of paragraph (5), as the one at which the person or someone on the person's behalf will accept documents of the same description as that notice, direction or other document, that address is also treated for the purposes of this Article and Article 7 of the Interpretation (Jersey) Law 1954 as the person's proper address.
 - (7) If the name or the address of any owner, lessee or occupier of premises on whom any notice, direction or other document referred to in paragraph (3) is to be served cannot after reasonable enquiry be ascertained it may be served by –
 - (a) addressing it to the person on whom it is to be served by the description of "owner", "lessee" or "occupier" of the premises;
 - (b) specifying the premises on it; and

- (c) delivering it to some responsible person resident or appearing to be resident on the premises or, if there is no person to whom it can be delivered, by affixing it, or a copy of it, to some conspicuous part of the premises.

83 Regulations – disclosure of information to improve public service delivery

- (1) Where they consider that to do so would improve the delivery of public services, the States may by Regulations prescribe the following matters –
 - (a) the prescribed persons, whether individually or by description, who may disclose to any other prescribed person information held in connection with any function;
 - (b) the purposes for which any prescribed person, or particular prescribed person may disclose data either to any other prescribed person or to particular prescribed persons;
 - (c) the safeguards and restrictions on the disclosure of the data by any or all prescribed persons and on the use of the information by any prescribed person;
 - (d) the circumstances in which information may be disclosed by a prescribed person to a person who is not a prescribed person and the safeguards and restrictions that may be imposed in respect of such disclosures, or further disclosures, as may be necessary or expedient to protect the rights of any person, whether natural or legal.
- (2) Before Regulations under paragraph (1) that permit the processing of personal data as part of the information disclosed may be made, the proposer of the Regulations –
 - (a) must prepare a data protection impact assessment under Article 16; and
 - (b) where the processing would pose a high risk to rights and freedoms of data subjects, consult the Authority in accordance with Article 17(2).
- (3) Regulations under this Article may amend or modify any enactment to the extent that it is necessary or expedient for the purposes of, or will enable the disclosure of, information intended to improve public service delivery other than –
 - (a) this Law or the Authority Law;
 - (b) the Police Procedures and Criminal Evidence (Jersey) Law 2003³²; or
 - (c) the Regulation of Investigatory Powers (Jersey) Law 2005³³.
- (4) A person who discloses or uses any information in contravention of Regulations under this Article is guilty of an offence and liable to imprisonment for a term of 2 years and to a fine.
- (5) For the purposes of paragraph (1) –

“function”, in the case of a person who is a prescribed person only because the person exercises the function of providing services to a public authority, means only that function;

“information” includes personal data and any other information, whether or not relating to identifiable corporate bodies;

“prescribed persons” means public authorities or States’ employees.

84 Regulations - constitution of Information Board

- (1) Regulations may provide that a public authority, States’ employee or any other person providing services to a public authority may individually or collectively constitute an Information Board for the purposes of –
 - (a) co-ordinating the disclosure of data by prescribed persons to improve the delivery of public services; and
 - (b) ensuring that the requirements of this Law and any Regulations made under it in relation to the disclosure of information are met.
- (2) The Regulations may –
 - (a) provide for the incorporation of the Information Board; and
 - (b) confer such rights, obligations and powers on the Board or on any person responsible for operating the Board as may be required to improve the delivery of public services and ensure the requirements of this Law and any Regulations made under it are met.

85 Regulations and Orders - general

- (1) The States may by Regulations and the Minister may by Order make provision for the purpose of carrying this Law into effect and including for or with respect to any matter that may be prescribed under this Law by Regulations or Orders as the case may be.
- (2) Without limiting the generality of paragraph (1) the States may by Regulations make any provision they think fit for any or all of the following purposes –
 - (a) requiring or authorizing a social security number or any other identification number issued by any public authority to be processed in a specified manner;
 - (b) requiring or authorizing the personal data of employees to be processed in a specified manner in the context of employment, including for the following purposes –
 - (i) recruitment,
 - (ii) the performance of a contract of employment, including discharge of obligations laid down by law,
 - (iii) management, planning and organization of work,
 - (iv) equality and diversity in the workplace,
 - (v) health and safety at work,
 - (vi) protection of the property of employers or customers,

- (vii) the exercise and enjoyment, on an individual or collective basis, of rights and benefits related to employment, or
 - (viii) the termination of the employment relationship;
 - (c) prohibiting a social security number or any other identification number issued by any public authority to be processed in a specified manner; or
 - (d) prohibiting the personal data of employees from being processed in a specified manner in the context of employment, including for any of the purposes specified in sub-paragraph (b).
- (3) Regulations made under paragraph (2) may include –
 - (a) safeguards for the rights and freedoms of data subjects;
 - (b) provisions relating to the transparency of processing;
 - (c) provisions relating to the transfer of personal data within a group of undertakings or within a group of enterprises engaged in a joint economic activity; or
 - (d) provisions relating to the monitoring of the application of the Regulations.
- (4) Regulations and Orders made under this Law may contain such transitional, consequential, incidental or supplementary provisions as appear to the States to be necessary or expedient for the purposes of the Regulations.
- (5) The power in paragraph (2), and in paragraph (4) in respect of Regulations, includes power to –
 - (a) repeal, revoke or amend any provision of an enactment (including this Law); and
 - (b) make any other consequential amendments to any other enactment as the States think fit.
- (6) Regulations made under this Law may create an offence punishable by a fine of up to level 3 on the standard scale.

86 Savings and transitional arrangements

- (1) Schedule 5 has effect.
- (2) Regulations may make provisions of a saving or transitional nature consequent on the enactment of this Law or the Authority Law.
- (3) Any provision of Regulations made under this Article may, if the Regulations so provide, come into force on the day on which Schedule 5 comes into force or on a later day.

87 Repeals and consequential and miscellaneous amendments

- (1) The Data Protection (Jersey) Law 2005³⁴ is repealed.
- (2) Schedule 6 contains amendments to other enactments.

88 Citation and commencement

- (1) This Law may be cited as the Data Protection (Jersey) Law 201- and subject to paragraphs (2) and (3) comes into force on 25th May 2018.
- (2) Part 5 comes into force on 25th November 2018 and Articles 17 and 18 come into force on 25th May 2019.
- (3) The modifications in paragraph 11 of Schedule 1, in so far as they relate to the insertion of paragraphs (3B), (3C) and (3D) into the modified version of Article 21, come into force on 6th May 2023.

SCHEDULE 1

(Article 4(5))

MODIFICATIONS OF LAW IN CASES OF PROCESSING BY COMPETENT AUTHORITIES**1 List of competent authorities**

The following are the competent authorities for the purposes of Article 4(7)(a) –

Andium Homes

Department of the Environment: Environmental Health, Marine Resources, Planning and Building Control, Sea Fisheries, States Vet, Water Resources.

Health and Social Services: Social Services Department

Department for Infrastructure: Driver and Vehicle Standards, Parking Control

Social Security Department

Health & Safety Inspectorate

Income Tax Department

Jersey Customs & Immigration Service

Jersey Financial Services Commission

Jersey Fire and Rescue Service

Jersey Gambling Commission

Jersey Police Complaints Authority

Jersey Probation Service

Judicial Greffe

The Law Officers' Department

Any Parish

Ports of Jersey

States of Jersey Police

Trading Standards

Viscount's Department.

2 Application and power to prescribe time limits

- (1) This Schedule applies to the processing of personal data by a controller that is a competent authority for a law enforcement purpose.
- (2) This Law applies to that processing subject to the modifications set out in this Schedule.

- (3) The Minister may prescribe specific time limits for the erasure or periodic review of the storage by competent authorities of data that are processed for law enforcement purposes.

3 Article 8 modified

In Article 8 –

- (a) for paragraph (1)(a) there is substituted the following sub-paragraph –
“(a) processed lawfully and fairly (‘lawfulness and fairness’);”;
- (b) after paragraph (2) there is added the following paragraph –
“(3) Contravention of any Order prescribing specific time limits for the erasure or periodic review of the storage by competent authorities of data that are processed for law enforcement purposes is taken to be a breach of the data protection principle relating to storage limitation.”.

4 Article 9 substituted

For Article 9 there is substituted the following Article –

“9 Lawful processing

- (1) The processing of personal data is lawful only if and to the extent that it is permitted by law and either –
- (a) the data subject has given consent to the processing for that purpose; or
 - (b) the processing is necessary for the performance of a task carried out by a controller for a law enforcement purpose.
- (2) The processing of special category data (other than data relating to a natural person’s criminal record or an alleged criminal activity) is lawful only if and to the extent that it is permitted by law and –
- (a) is strictly necessary, subject to appropriate safeguards for the rights and freedoms of the data subject;
 - (b) serves to protect the vital interests of the data subject or another individual; or
 - (c) the processing relates to data that are manifestly made public by the data subject.
- (3) For the purposes of paragraph (2)(a) processing is strictly necessary where it is necessary –
- (a) for the purposes of the administration of justice;
 - (b) for the performance of a function conferred on a person by any enactment;
 - (c) for the establishment, exercise or defence of a legal claim or whenever a court is acting in its judicial capacity;
 - (d) for the purposes of preventing any kind of fraud; or

- (e) for any of the purposes set out in paragraph 17 of Schedule 2 (archiving and research).
- (4) In the case of any of the purposes mentioned in paragraph (3)(e) processing is not permitted if it is carried out –
 - (a) for the purposes of, or in connection with, measures or decisions with respect to a particular data subject; or
 - (b) it is likely to cause substantial damage or substantial distress to an individual.”.

5 Article 10 modified

In Article 10(3) the words “and transparently” are omitted.

6 Article 12 substituted

For Article 12 there is substituted the following Article –

“12 Information to be provided to data subject

- (1) The controller must make available to data subjects the following information (whether by making the information generally available to the public or in any other way) –
 - (a) the identity and the contact details of the controller;
 - (b) where applicable, the contact details of the data protection officer;
 - (c) the purposes for which the controller processes personal data;
 - (d) the existence of the right to lodge a complaint with the Authority and the contact details of the Authority; and
 - (e) the existence of the rights of data subjects to request from the controller –
 - (i) access to personal data,
 - (ii) rectification of personal data, and
 - (iii) erasure of personal data or the restriction of its processing.
- (2) Except in relation to the processing of relevant personal data in the course of a criminal investigation or criminal proceedings, including proceedings for the purpose of enforcing a criminal penalty, the controller must also, in specific cases for the purpose of enabling the exercise of a data subject’s rights under this Part, give to the data subject the following further information to enable the exercise of his or her rights –
 - (a) the legal basis for the processing;
 - (b) the period for which the personal data will be stored, or where that is not possible, the criteria used to determine that period;

- (c) where applicable, the categories of recipients of the personal data, including third countries or international organizations;
 - (d) any further information that is necessary, having regard to the specific circumstances in which the data are or are to be processed, to enable processing in respect of the data subject to be fair.
- (3) The information required to be provided under this Article must be provided in an intelligible form using clear language.
- (4) The controller may delay, restrict or omit giving any of the information required by paragraph (2) to the extent that, and for as long as, it considers it necessary and proportionate to do so having regard to the fundamental rights and legitimate interests of the data subject concerned, in order to –
 - (a) avoid obstructing official or legal inquiries, investigations or procedures;
 - (b) avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties;
 - (c) protect public security;
 - (d) protect national security; or
 - (e) protect the rights and freedoms or others.
- (5) In paragraph (2), ‘relevant personal data’ means personal data contained in a judicial decision or in other documents relating to the investigation or proceedings which are created by or on behalf of a court or other judicial authority.”.

7 Article 13 substituted

For Article 13 there is substituted the following Article –

“13 Purposes of processing

- (1) Personal data collected for a law enforcement purpose may be processed for any other law enforcement purpose (whether by the controller that collected the data or by another controller) provided that –
 - (a) the controller is authorized by law to process the data for the other purpose; and
 - (b) the processing is necessary and proportionate to that other purpose.
- (2) Personal data collected for any of the law enforcement purposes may not be processed for a purpose that is not a law enforcement purpose unless the processing is authorized by law.
- (3) The controller must process personal data in a way that makes appropriate distinctions between data relating to different categories of data subjects, including persons suspected of

committing, or convicted of, an offence and victims and witnesses, whose data may be processed for different purposes.”.

8 Article 15 modified

After Article 15(5) there are added the following paragraphs –

- “(6) The controller, as far as practicable, must –
- (a) verify the quality of personal data before they are transmitted or made available;
 - (b) when transmitting the data, add such information as is necessary to enable the receiving authority to assess the degree of accuracy, completeness and reliability of that data.
- (7) Where incorrect personal data have been transmitted or personal data have been transmitted unlawfully the controller must notify the recipient and must rectify or erase the personal data or restrict processing without the need for any request from the data subject under Article 31 or 32.”.

9 Article 17 modified

At the end of Article 17(1) there are added the words “and the processing in question consists of a new collection of personal data”.

10 Article 20 modified

After Article 20(8) there is added the following paragraph –

- “(9) The communication to the data subject referred to in paragraph (6) may be delayed, restricted or omitted to the extent that, and for as long as, the restriction (whether whole or partial) is necessary and proportionate having regard to the fundamental rights and legitimate interests of the data subject concerned, in order to –
- (a) avoid obstructing official or legal inquiries, investigations or procedures;
 - (b) avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the enforcement of criminal penalties;
 - (c) protect public security;
 - (d) protect national security; or
 - (e) protect the rights and freedoms or others.”.

11 Article 21 modified

After Article 21(3) there are inserted the following paragraphs –

- “(3A) In respect of automated processing, the controller, having evaluated the risks, must implement measures designed to –

- (a) deny unauthorized persons access to processing equipment used for processing ('equipment access control');
 - (b) prevent the unauthorized reading, copying, modification or removal of data media ('data media control');
 - (c) prevent the unauthorized input of personal data and the unauthorized inspection, modification or deletion of stored personal data ('storage control');
 - (d) prevent the use of automated processing systems by unauthorized persons using data communication equipment ('user control');
 - (e) ensure that persons authorized to use an automated processing system have access only to the personal data covered by their access authorization ('data access control');
 - (f) ensure that it is possible to verify and establish the bodies to which personal data have been or may be transmitted or made available using data communication equipment ('communication control');
 - (g) ensure that it is subsequently possible to verify and establish which personal data have been input into automated processing systems and when and by whom the personal data were input ('input control');
 - (h) prevent the unauthorized reading, copying, modification or deletion of personal data during transfers of personal data or during transportation of data media ('transport control');
 - (i) ensure that installed systems may, in the case of interruption, be restored ('recovery');
 - (j) ensure that the functions of the system perform, that the appearance of faults in the functions is reported ('reliability') and that stored personal data cannot be corrupted by means of a malfunctioning of the system ('integrity').
- (3B) The controller must keep logs for processing operations in automated processing systems consisting of collection, alteration, consultation, disclosure including transfers, combination and erasure of personal data, and in the case of logs of consultation and disclosure, must enable –
- (a) the establishment of the justification, date and time of such operations; and
 - (b) as far as possible, the identification of the person who consulted or disclosed personal data, and the identity of the recipients of such personal data.
- (3C) The logs may be used solely for verification of the lawfulness of processing, self-monitoring, ensuring the integrity and security of the personal data, and for criminal proceedings.
- (3D) The controller and the processor must make the logs available to the Authority on request.”

12 Article 27 modified

In Article 27 –

- (a) the words in paragraph (1) after the word “undue delay” are omitted;
- (b) paragraph (2) is omitted;
- (c) in paragraph (4) the words “and at the latest within 4 weeks of receipt of the request” are omitted.

13 Article 28 modified

In Article 28 –

- (a) paragraph (1)(h) and (3)(b) are omitted;
- (b) after paragraph (7) there are added the following paragraphs –
 - “(8) The data subject’s right of access is restricted to the extent that, and for as long as, the restriction (whether whole or partial) is necessary and proportionate having regard to the fundamental rights and legitimate interests of the data subject concerned, in order to –
 - (a) avoid obstructing official or legal inquiries, investigations or procedures;
 - (b) avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties;
 - (c) protect public security;
 - (d) protect national security; or
 - (e) protect the rights and freedoms of others.
 - (9) The controller must assess, according to individual circumstances, the extent to which a data subject’s rights should be restricted under paragraph (8) and any such restriction must be notified in writing to the data subject with the factual or legal reasons for the restriction.”.

14 Article 31 modified

After Article 31(4) there are added the following paragraphs –

- “(5) The controller must inform the data subject in writing of any refusal of rectification of personal data and the reasons for the refusal unless it considers it necessary and proportionate not to do so having regard to the fundamental rights and legitimate interests of the data subject concerned, in order to –
 - (a) avoid obstructing official or legal inquiries, investigations or procedures;
 - (b) avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties;

- (c) protect public security;
 - (d) protect national security; or
 - (e) protect the rights and freedoms of others.
- (6) The controller must inform the data subject of his or her right to lodge a complaint with the Authority or to seek a judicial remedy.
- (7) The controller must communicate the rectification of inaccurate personal data to the controller from which the inaccurate personal data originate.
- (8) Where personal data has been rectified under this Article the controller must notify the recipients of the data and those recipients must rectify the personal data under their responsibility.
- (9) Where the controller would be required to rectify personal data under this Article but the personal data must be maintained for the purposes of evidence, the controller must (instead of rectifying the personal data) restrict its processing.”.

15 Article 32 modified

In Article 32 –

- (a) for paragraph (1) there is substituted the following paragraph –
- “(1) Where so required by the data subject the controller must erase personal data without undue delay where the processing breaches any of the data protection principles.”;
- (b) after paragraph (3) there are inserted the following paragraphs –
- “(3A) The controller must inform the data subject in writing of any refusal of erasure of personal data and the reasons for the refusal unless it considers it necessary and proportionate not to do so having regard to the fundamental rights and legitimate interests of the data subject concerned, in order to –
- (a) avoid obstructing official or legal inquiries, investigations or procedures;
 - (b) avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties;
 - (c) protect public security;
 - (d) protect national security; or
 - (e) protect the rights and freedoms of others.
- (3B) The controller must inform the data subject of his or her right to lodge a complaint with the Authority or to seek a judicial remedy.
- (3C) Where personal data has been erased under this Article the controller must notify the recipients of the data and those recipients must erase the personal data under their responsibility.
- (3D) Where the controller would be required to erase personal data under this Article but the personal data must be maintained for the

purposes of evidence, the controller must (instead of erasing the personal data) restrict its processing.”.

16 Article 33 modified

After Article 33(3) there are added the following paragraphs –

- “(4) The controller must restrict processing instead of erasing personal data where –
- (a) the accuracy of the personal data is contested by the data subject and the extent of the data’s accuracy cannot be ascertained;
 - (b) the personal data must be maintained for the purposes of evidence.
- (5) Where paragraph (4)(a) applies the controller must inform the data subject before lifting the restriction on processing.
- (6) The controller must inform the data subject in writing of any refusal of restriction of processing of personal data and the reasons for the refusal unless it considers it necessary and proportionate not to do so having regard to the fundamental rights and legitimate interests of the data subject concerned, in order to –
- (a) avoid obstructing official or legal inquiries, investigations or procedures;
 - (b) avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties;
 - (c) protect public security;
 - (d) protect national security; or
 - (e) protect the rights and freedoms of others.
- (7) The controller must inform the data subject of his or her right to lodge a complaint with the Authority or to seek a judicial remedy.
- (8) Where the processing of personal data has been restricted under this Article the controller must notify the recipients of the data and those recipients must restrict processing of the personal data under their responsibility.”.

17 Articles 34 to 37 omitted

Articles 34 to 37 are omitted.

18 Article 38 modified

For Article 38(1) to (4) there are substituted the following paragraphs –

- “(1) A decision based on automated processing that produces an adverse legal effect concerning the data subject or significantly affects the data subject, is prohibited unless –

- (a) the decision is authorized by the relevant law to which the controller is subject; and
 - (b) that law provides adequate safeguards for the rights and freedoms of the data subject, in particular the right to obtain human intervention on the part of the controller.
- (2) A decision mentioned in paragraph (1) must not be based on special category data as mentioned in Article 10(2) unless suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place."

19 Part 8 substituted

For Part 8 there is substituted the following Part –

“PART 8 CROSS-BORDER DATA TRANSFERS

66 General principles for cross-border data transfers

- (1) A controller must not transfer personal data to a third country or to an international organization unless –
- (a) the transfer is necessary for any of the law enforcement purposes;
 - (b) the conditions set out in paragraph (2) are met; and
 - (c) in a case where the personal data was originally transmitted or otherwise made available to the controller or another competent authority by a Member State, that Member State, or any person based in that Member State that is a competent authority for the purposes of the Law Enforcement Directive, has authorized the transfer in accordance with the law of the Member State.
- (2) The conditions are –
- (a) that the transfer is based on –
 - (i) an adequacy decision in accordance with Article 67,
 - (ii) there being appropriate safeguards as set out in Article 67A, or
 - (iii) the special circumstances set out in Article 67B; and
 - (b) the intended recipient is –
 - (i) a relevant authority in a third country or an international organization that is a relevant international organization, or
 - (ii) any other person and the additional conditions in Article 67C are met.
- (3) Authorization is not required as mentioned in paragraph (1)(c) if –

- (a) the transfer is necessary for the prevention of an immediate and serious threat either to the public security of Jersey or a Member State or a third country or to the essential interests of a Member State; and
 - (b) the authorization cannot be obtained in good time.
- (4) Where a transfer is made without the authorization mentioned in paragraph (1)(c), the authority in the Member State which would have been responsible for deciding whether to authorize the transfer must be informed without delay.
- (5) In this Article –
- ‘relevant authority’, in relation to a third country, means any person based in a third country that has (in that country) functions comparable to those of a competent authority;
- ‘relevant international organization’ means an international organization that carries out functions for any of the law enforcement purposes.

67 Transfers on the basis of an adequacy decision

A transfer of personal data to a third country or an international organization is based on an adequacy decision where –

- (a) the European Commission has decided, in accordance with Article 36 of the Law Enforcement Directive, that the third country or a territory or one or more specified sectors within that third country, or (as the case may be) the international organization, ensures an adequate level of protection of personal data; and
- (b) that decision has not been repealed or suspended, or amended in a way that demonstrates that the Commission no longer considers there to be an adequate level of protection of personal data.

67A Transfers on the basis of appropriate safeguards

- (1) A transfer of personal data to a third country or an international organization is based on there being appropriate safeguards where –
- (a) a legal instrument containing appropriate safeguards for the protection of personal data binds the intended recipient of the data; or
 - (b) the controller, having assessed all the circumstances surrounding transfers of that type of personal data to the third country or international organization, concludes that appropriate safeguards exist to protect the data.
- (2) The controller must inform the Authority about the categories of data transfers that take place in reliance on paragraph (1)(b).
- (3) Where a transfer of data takes place in reliance on paragraph (1) –
- (a) the transfer must be documented;

- (b) the documentation must be provided to the Authority on request;
- (c) the documentation must include, in particular –
 - (i) the date and time of the transfer,
 - (ii) the name of and any other pertinent information about the recipient,
 - (iii) the justification for the transfer, and
 - (iv) a description of the personal data transferred.

67B Transfers on the basis of special circumstances

- (1) A transfer of personal data to a third country or international organization is based on special circumstances where the transfer is necessary –
 - (a) to protect the vital interests of the data subject or another person;
 - (b) to safeguard the legitimate interests of the data subject;
 - (c) for the prevention of an immediate and serious threat to the public security of Jersey, a Member State or a third country;
 - (d) in individual cases for any of the law enforcement purposes; or
 - (e) in individual cases for a legal purpose.
- (2) But paragraph (1)(d) and (e) do not apply if the controller determines that fundamental rights and freedoms of the data subject override the public interest in the transfer.
- (3) Where a transfer of data takes place in reliance on paragraph (1) –
 - (a) the transfer must be documented;
 - (b) the documentation must be provided to the Authority on request; and
 - (c) the documentation must include, in particular –
 - (i) the date and time of the transfer,
 - (ii) the name of and any other pertinent information about the recipient,
 - (iii) the justification for the transfer, and
 - (iv) a description of the personal data transferred.
- (4) For the purposes of this Article, a transfer is necessary for a legal purpose if –
 - (a) it is necessary for the purpose of, or in connection with, any legal proceedings (including prospective legal proceedings) relating to any of the law enforcement purposes;
 - (b) it is necessary for the purpose of obtaining legal advice in relation to any of the law enforcement purposes; or

- (c) it is otherwise necessary for the purposes of establishing, exercising or defending legal rights in relation to any of the law enforcement purposes.

67C Transfers of personal data to persons other than relevant authorities

- (1) The additional conditions referred to in Article 66(2)(b)(ii) are that –
 - (a) the transfer is strictly necessary in a specific case for the performance of a task of the transferring controller as provided by law for any of the law enforcement purposes; and
 - (b) the transferring controller –
 - (i) has determined that there are no fundamental rights and freedoms of the data subject concerned that override the public interest necessitating the transfer,
 - (ii) considers that the transfer of the personal data to a relevant authority (within the meaning of Article 66) in the third country would be ineffective or inappropriate (for example, where the transfer could not be made in sufficient time to enable its purpose to be fulfilled), and
 - (iii) informs the intended recipient of the specific purpose or purposes for which the personal data may, so far as necessary, be processed.
- (2) Where personal data are transferred to a person in a third country other than a relevant authority, the transferring controller must inform a relevant authority in that third country without undue delay of the transfer, unless this would be ineffective or inappropriate.
- (3) The transferring controller must –
 - (a) document any transfer to a recipient in a third country other than a relevant authority; and
 - (b) inform the Authority of the transfer.
- (4) This Article does not affect the operation of any international agreement in force in respect of Jersey in the field of judicial co-operation in criminal matters and police co-operation.”.

SCHEDULE 2

(Article 9)

CONDITIONS FOR PROCESSING**PART 1 – CONDITIONS FOR PROCESSING PERSONAL DATA****1 Consent**

The data subject has consented to the processing of his or her data for one or more specific purposes.

2 Contract

The processing is necessary for –

- (a) the performance of a contract to which the data subject is a party; or
- (b) the taking of steps at the request of the data subject with a view to entering into a contract.

3 Vital interests

The processing is necessary to protect the vital interests of the data subject or any other natural person.

4 Public functions

The processing is necessary for –

- (a) the administration of justice;
- (b) the exercise of any functions conferred on any person by or under any enactment;
- (c) the exercise of any functions of the Crown, the States or any public authority; or
- (d) the exercise of any other functions of a public nature with a legal basis in Jersey law to which the controller is subject and exercised in the public interest by any person.

5 Legitimate interests

- (1) The processing is necessary for the purposes of legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, unless –
 - (a) the processing is unwarranted in any particular case by reason of prejudice to the rights and freedoms or legitimate interests of the data subject, in particular where the subject is a child; or
 - (b) the controller is a public authority.

- (2) The States may by Regulations specify particular circumstances in which the condition set out in sub-paragraph (1)(a) is, or is not, to be taken to be satisfied.

PART 2 – CONDITIONS FOR PROCESSING PERSONAL DATA AND SPECIAL CATEGORY DATA

6 Consent

The data subject has given explicit consent to the processing for one or more specific purposes.

7 Other legal obligations

The processing is necessary for compliance with a legal obligation, other than one imposed by contract, to which the controller is subject.

8 Employment and social fields

The processing is necessary for the purposes of exercising or performing any right, obligation or public function conferred or imposed by law on the controller in connection with employment, social security, social services or social care.

9 Vital interests

The processing is necessary in order to protect the vital interests of –

- (a) the data subject or another person, in a case where consent cannot be given by or on behalf of the data subject, or the controller cannot reasonably be expected to obtain the consent of the data subject; or
- (b) another person, in a case where consent by or on behalf of the data subject has been unreasonably withheld.

10 Non-profit associations

The processing –

- (a) is carried out in the course of its legitimate activities by any body, or association, that is not established or conducted for profit, and exists for political, philosophical, religious or trade union purposes;
- (b) is carried out with appropriate safeguards for the rights and freedoms of data subjects;
- (c) relates only to individuals who are members of the body or association or have regular contact with it in connection with its purposes; and
- (d) does not involve disclosure of the personal data to a third party without the consent of the data subject.

11 Information made public

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

12 Legal proceedings, etc.

The processing is necessary for the purposes of –

- (a) any legal proceedings;
- (b) obtaining legal advice; or
- (c) establishing, exercising or defending legal rights.

13 Public functions

The processing is necessary for –

- (a) the administration of justice;
- (b) the exercise of any functions conferred on any person by or under an enactment; or
- (c) the exercise of any functions of the Crown, the States, any administration of the States or any public authority.

14 Public interest

The processing is necessary for reasons of substantial public interest provided for by law and is subject to appropriate protections to protect the rights and interests of the data subject.

15 Medical purposes

- (1) The processing is necessary for medical purposes and is undertaken by –
 - (a) a health professional; or
 - (b) a person who in the circumstances owes a duty of confidentiality equivalent to that which would arise if that person were a health professional.
- (2) In paragraph (1) “medical purposes” includes the purposes of preventative medicine, medical diagnosis, medical research, the provision of care and treatment, the management of healthcare services, occupational medicine and the assessment of the working capacity of the employee.

16 Public health

The processing is necessary for reasons of public interest in the area of public health, including (but not limited to) protecting against cross border threats to health and ensuring a high standard of quality and safety of health care or social care where they are provided for by law and the processing is carried out with appropriate safeguards for the rights and freedoms of data subjects.

17 Archiving and research

The processing –

- (a) is in the public interest;
- (b) is necessary for the purposes of archiving or for statistical, scientific or historical research;
- (c) does not support measures or decisions with respect to any particular data subject otherwise than with the explicit consent of the data subject; and
- (d) is carried out with appropriate safeguards for the rights and freedoms of data subjects.

18 Avoidance of discrimination

(1) The processing –

- (a) consists of information as to –
 - (i) any protected characteristic within the meaning of the Discrimination (Jersey) Law 2013³⁵, or
 - (ii) a person's disability, or
 - (iii) a person's religious beliefs;
 - (b) is necessary for the purpose of identifying or keeping under review the existence or absence of equality of opportunity or treatment of persons on grounds of any characteristic described in clause (a)(i) to (iii) with a view to enabling such equality to be promoted or maintained;
 - (c) does not support measures or decisions with respect to any particular data subject otherwise than with the explicit consent of the data subject; and
 - (d) is carried out with appropriate safeguards for the rights and freedoms of data subjects.
- (2) The processing is not contrary to any notice in writing that an individual has given to the controller requiring the controller to cease processing personal data in respect of which the individual is the data subject, such notice taking effect at the end of a period that is reasonable in the circumstances or, if longer, the period specified in the notice.

19 Prevention of unlawful acts

The processing –

- (a) is in the substantial public interest;
- (b) is necessary for the purposes of the prevention or detection of any unlawful act or unlawful omission; and
- (c) in order not to prejudice those purposes, is required to be carried out without the controller's seeking the explicit consent of the data subject.

20 Protection against malpractice and mismanagement

The processing –

- (a) is in the substantial public interest;
- (b) is necessary for the discharge of any function that is designed for protecting members of the public against –
 - (i) dishonesty, malpractice, or other seriously improper conduct by, or the unfitness or incompetence of, any person, or
 - (ii) mismanagement in the administration of, or failures in services provided by, any body or association; and
- (c) in order not to prejudice the discharge of that function, is required to be carried out without the controller's seeking the explicit consent of the data subject.

21 Publication about malpractice and mismanagement

- (1) The processing –
 - (a) takes the form of disclosure;
 - (b) is in the substantial public interest;
 - (c) is in connection with –
 - (i) the commission by any person of any unlawful act, or unlawful omission, whether alleged or established,
 - (ii) dishonesty, malpractice, or other seriously improper conduct by, or the unfitness or incompetence of, any person, whether alleged or established, or
 - (iii) mismanagement in the administration of, or failures in services provided by, any body or association, whether the mismanagement or failures are alleged or established;
 - (d) is for the special purposes; and
 - (e) is made with a view to the publication of those data by any person.
- (2) The person who is the controller in relation to the processing reasonably believes that the publication would be in the public interest.

22 Counselling

- (1) The processing –
 - (a) is in the substantial public interest; and
 - (b) is necessary for the discharge of any function designed for the provision of confidential counselling, confidential advice, confidential support or a similar confidential service.
- (2) One or more of the following conditions is satisfied –
 - (a) the data subject cannot give consent to the processing;
 - (b) the controller cannot reasonably be expected to obtain the consent of the data subject to the processing; or

- (c) the processing must, in order not to prejudice the discharge of the function referred to in sub-paragraph (1)(b), be carried out without the controller's seeking the explicit consent of the data subject.

23 Insurance and pensions: general determinations

- (1) The processing –
 - (a) is necessary for the purpose of –
 - (i) carrying on insurance business falling within Class I, III or IV of Part 1 of Schedule 1 to the Insurance Business (Jersey) Law 1996³⁶, or within Class 1 or 2 of Part 2 of that Schedule, or
 - (ii) making determinations in connection with eligibility for, or benefits payable under, an occupational pension scheme, being a scheme, or arrangement, that is constituted in one or more instruments or agreements and 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; and
 - (b) does not support measures or decisions that relate in particular to the person who is the data subject in respect of the personal data.
- (2) The controller cannot reasonably be expected to obtain the explicit consent of that data subject to the processing and the controller is not aware of the data subject's withholding his or her consent to the processing.
- (3) The personal data consists of information relating to the physical or mental health or condition of a data subject who is the parent, grandparent, great-grandparent or sibling of –
 - (a) in the case of processing for the purpose referred to in sub-paragraph (1)(a)(i), a person insured (or seeking to be insured) in the course of the insurance business; or
 - (b) in the case of processing for the purpose referred to in sub-paragraph (1)(a)(ii), a person who is a member of the scheme or seeking to become a member of the scheme.

24 Insurance and pensions: current processing

- (1) The processing –
 - (a) was already under way in relation to the same data subject and by or on behalf of the same controller immediately before the coming into force of this Schedule; and
 - (b) is necessary for the purpose of –

-
- (i) carrying on insurance business falling within Class I, III or IV of Part 1 of Schedule 1 to the Insurance Business (Jersey) Law 1996, or
 - (ii) establishing or administering an occupational pension scheme, being a scheme, or arrangement, that is constituted in one or more instruments or agreements and 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.
- (2) One or both of the following conditions is satisfied –
- (a) the controller cannot reasonably be expected to obtain the explicit consent of the data subject to the processing and has not been informed by the data subject that the latter refuses consent to the processing;
 - (b) the processing must, in order not to prejudice the purpose referred to in sub-paragraph (1)(b), be carried out without the controller's seeking the explicit consent of the data subject.

25 Functions of a police officer

The processing is necessary for the exercise of any function conferred on a police officer by or under any enactment or other law.

26 Regulations

Regulations may –

- (a) specify further circumstances in which special category data are processed;
- (b) exclude the application of this Schedule in such cases as may be specified;
- (c) provide that, in such cases as may be specified, any condition in this Schedule is not to be regarded as satisfied unless such further conditions as may be specified in the Regulations are also satisfied; or
- (d) specify circumstances in which processing falling within paragraph 17(a) and (b) is, or is not, to be taken for the purposes of paragraph 17(d) to be carried out with appropriate safeguards for the rights and freedoms of data subjects.

SCHEDULE 3

(Article 66(2)(c))

EXCEPTIONS TO ADEQUACY REQUIREMENTS**1 Order of court, public authorities etc.**

The transfer is specifically required by –

- (a) an order or judgment of a court or tribunal having the force of law in Jersey;
- (b) an order or judgment of a court or tribunal of a country other than Jersey or a decision of a public authority of such a country having the force of law in Jersey that is based on an international agreement imposing an international obligation on Jersey; or
- (c) a decision of a public authority in Jersey that is based on such an international agreement.

2 Consent

The data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision under Article 45 of the GDPR and appropriate safeguards.

3 Contract between data subject and controller

The transfer is necessary for –

- (a) the performance of a contract between the data subject and the controller; or
- (b) the implementation of pre-contractual measures taken at the data subject's request.

4 Third-party contract in interest of data subject

The transfer is necessary for the conclusion or performance of a contract between the controller and a person other than the data subject.

5 Transfer by or on behalf of JFSC

The transfer is necessary for reasons of substantial public interest, which is taken to be the case if all the following circumstances apply –

- (a) the transfer is a disclosure that is permitted or required under an enactment in force in Jersey;
- (b) the transfer is made by or on behalf of the Jersey Financial Services Commission (the "JFSC"); and

- (c) the JFSC has taken reasonable steps to ensure that the transferee will not transfer the personal data to another person except –
 - (i) with the consent of the JFSC, or
 - (ii) in order to comply with an order of a court (whether or not a Jersey court) that directs the transferee to transfer the personal data to the other person.

6 Legal proceedings etc.

The transfer –

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

7 Vital interests

The transfer is necessary in order to protect the vital interests of the data subject or of other persons, where –

- (a) the data subject is physically or legally incapable of giving consent;
- (b) the data subject has unreasonably withheld consent; or
- (c) the controller or processor cannot reasonably be expected to obtain the explicit consent of the data subject.

8 Public register

- (1) The transfer is made from a register that –
 - (a) according to the relevant law is intended to provide information to the public; and
 - (b) is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest.
- (2) However, a transfer under this paragraph –
 - (a) may take place only to the extent that the conditions laid down by the relevant law for consultation are fulfilled in the particular case;
 - (b) must not involve the entirety of the personal data or entire categories of the personal data contained in the register; and
 - (c) where the register is intended for consultation by persons having a legitimate interest, may be made only at the request of those persons or where they are to be the recipients of the data.

9 Other exceptions

- (1) Where a transfer cannot be based on any other provision of this Law, a transfer to a third country or an international organization may take place only if –
 - (a) the transfer is not repetitive;
 - (b) the transfer concerns only a limited number of data subjects;
 - (c) the transfer is necessary for the purposes of compelling legitimate interests pursued by the controller which are not overridden by the interests or rights and freedoms of the data subject; and
 - (d) the controller has assessed all the circumstances surrounding the data transfer and has on the basis of that assessment provided appropriate safeguards with regard to the protection of personal data.
- (2) Where a transfer is to take place under this paragraph, the controller must –
 - (a) inform the Authority of the transfer as soon as practicable; and
 - (b) in addition to providing the information referred to in Article 12, inform the data subject of the transfer and the compelling legitimate interests pursued.

10 Public authorities

Paragraphs 2, 3, 4 and 9 do not apply to activities carried out by public authorities in the exercise of their public powers.

11 Recording of assessment

The controller or processor must document the assessment as well as the suitable safeguards referred to in paragraph 9(1)(d) in the records maintained under Article 14(3) or 22(1)(e).

SCHEDULE 4

(Article 67(2)(b))

BINDING CORPORATE RULES

- (1) The Authority must approve binding corporate rules, if those rules –
 - (a) are legally binding and apply to and are enforced by every member concerned of the group, including their employees;
 - (b) expressly confer enforceable rights on data subjects with regard to the processing of their personal data; and
 - (c) fulfil the requirements laid down in paragraph (2).
- (2) The rules must include the following content –
 - (a) the structure and contact details of the group and of each of its members;
 - (b) the data transfers or set of transfers, including the categories of personal data, the type of processing and its purposes, the type of data subjects affected and the identification of the third country or countries in question;
 - (c) a statement of their legally binding nature, both internally and externally;
 - (d) the application of the data protection principles, in particular those mentioned in Article 8(1)(b), (c) and (e), matters covered by Articles 15 and 21 and provisions relating to data quality, the legal basis for processing, processing of special categories of personal data and the requirements in respect of onward transfers to bodies not bound by the binding corporate rules;
 - (e) the rights of data subjects in regard to processing and the means to exercise those rights, including the right –
 - (i) not to be subject to decisions based solely on automated processing, in accordance with Article 38,
 - (ii) to lodge a complaint with the Authority under Article 19 of the Authority Law and to bring proceedings under Article 68 of this Law, and
 - (iii) to obtain redress and, where appropriate, compensation for a breach of the binding corporate rules;
 - (f) the acceptance by the controller or processor established on the territory of a Member State of liability for any breaches of the binding corporate rules by any member of the group, the controller or the processor being exempt from that liability, in whole or in part, only if it proves that that member is not responsible for the event giving rise to the breach;
 - (g) how the information on the binding corporate rules, in particular on the provisions referred to in sub-paragraphs (d), (e) and (f) is provided to the data subjects in addition to the matters required by Article 12;

-
- (h) the functions of any data protection officer appointed under Article 24 or any other person or entity in charge of monitoring compliance with the binding corporate rules within the group, as well as monitoring training and complaint-handling;
 - (i) the complaint procedures;
 - (j) the mechanisms within the group for ensuring the verification of compliance with the binding corporate rules, which mechanisms must include the following actions –
 - (i) data protection audits,
 - (ii) methods for ensuring corrective actions to protect the rights of the data subject,
 - (iii) communicating the results of such actions to the person or entity referred to in sub-paragraph (h) and to the board of the controlling undertaking of the group, and
 - (iv) making those results available upon request to the Authority;
 - (k) the mechanisms for reporting and recording changes to the rules and reporting those changes to the Authority;
 - (l) the mechanism for co-operating with the Authority to ensure compliance by any member of the group, in particular by making available to the Authority the results of the actions referred to in sub-paragraph (j)(i) and (ii);
 - (m) the mechanisms for reporting to the Authority any legal requirements to which a member of the group is subject in a third country that are likely to have a substantial adverse effect on the guarantees provided by the binding corporate rules; and
 - (n) the appropriate data protection training to personnel having permanent or regular access to personal data.
- (3) In this Schedule “group” means the group of undertakings, or group of enterprises engaged in a joint economic activity to which the binding corporate rules apply.
- (4) Regulations may amend the content that the rules must include under this Schedule.

SCHEDULE 5

(Article 86)

SAVINGS AND TRANSITIONAL ARRANGEMENTS**1 Interpretation**

In this Schedule “2005 Law” means the Data Protection (Jersey) Law 2005³⁷.

2 Processing underway at time of commencement of this Law

- (1) Where, at the time of commencement of Article 87, consent to the processing of personal data was obtained in compliance with the requirements of the 2005 Law, that consent, to the extent that it was not given in a manner that complies with this Law, has effect up to and including 25th May 2019.
- (2) Where, at the time of commencement of Article 87, the specified information (within the meaning of Article 12(4)) was provided by the controller to the data subject in compliance with the requirements of paragraph 2 of Part 2 of Schedule 1 to the 2005 Law, to the extent that the such compliance is not compliance with Article 12 of this Law, the controller is nevertheless treated as complying with it until 25th May 2019.

3 Request for information and copy of personal data

A request for information and a copy of personal data under Article 7 of the 2005 Law that has not been complied with on the commencement of Article 28 of this Law is treated as a request under Article 28 of this Law save that –

- (a) the controller has 40 days to answer the request; and
- (b) no fee paid is refundable.

4 Right to compensation for inaccuracy, loss or unauthorized disclosure

A claim for compensation under Article 13 of the 2005 Law that remains outstanding on the commencement of Article 69 of this Law is treated as if that Article 13 continued in force.

5 Application for rectification, blocking, erasure or destruction

An application for rectification, blocking, erasure or destruction under Article 14 of the 2005 Law that remains outstanding on the commencement of Articles 31 and 32 of this Law is treated as if that Article 14 continued in force.

6 Self-incrimination, etc.

- (1) In Article 58 of this Law and paragraph 1(9) of Schedule 1 to the Authority Law, any reference to an offence under this Law or the Authority Law includes a reference to an offence under the 2005 Law.
- (2) In Article 43(9), Article 44(10) and paragraph 11 of Schedule 7 of the 2005 Law, any reference to an offence under that Law includes a reference to an offence under this Law or the Authority Law.

7 General: references to Data Protection Commissioner

- (1) This paragraph is subject to any express provision, or implication, to the contrary in or under this Law or any other enactment, or in any agreement or other document.
- (2) A reference in any enactment, agreement or other document to the Data Protection Commissioner shall, on and from the commencement of the Authority Law, become a reference to the Data Protection Authority.
- (3) Accordingly, any application made to the Data Protection Commissioner, any proceedings commenced with the Data Protection Commissioner as party, or anything else involving the Data Protection Commissioner, being an application, proceedings or thing that has not been finally determined, or finished, when the Authority Law comes into force may be determined or continued by the Authority.
- (4) Furthermore, any record or requirement made by, any information given to, any document deposited with, any record kept by, or any statement made to, the Data Protection Commissioner in the exercise of any of the Commissioner's functions before the commencement of Article 2 of the Authority Law is taken, on and from that time, to have been made by, given to, deposited with, kept by or made to, the Authority.

8 General saving (except for Regulations, Rules or Orders)

- (1) Except as provided otherwise in this Schedule and Article 16(7) of, or Schedule 2 to, the Authority Law, anything made or done by any person under any provision of the 2005 Law (being a thing that still had force or effect immediately before the repeal of that provision by this Law), if there is a provision under this Law that gives power to make or do such a thing, is taken to have been made or done under the latter provision.
- (2) Subject to paragraph (1), Regulations, Rules, or any Order made under the 2005 Law cease to be in force when this paragraph comes into force.

SCHEDULE 6

(Article 87(2))

CONSEQUENTIAL AND MISCELLANEOUS AMENDMENTS**1 Consequential amendments to various enactments**

- (1) In the following provisions for the words “Data Protection (Jersey) Law 2005” there are substituted the words “Data Protection (Jersey) Law 201-” –
- (a) in Article 20(8) of the Civil Aviation (Jersey) Law 2008³⁸;
 - (b) in paragraph 7.5 of the Code set out in Schedule 3 to Regulation of Investigatory Powers (Codes of Practice) (Jersey) Order 2006³⁹;
 - (c) in Articles 12(3)(h)(iii), (4)(f) and 16(3)(a) of the Gambling (Jersey) Law 2012⁴⁰;
 - (d) in Article 113P(8) of the Companies (Jersey) Law 1991⁴¹;
 - (e) in Article 8(9) of the Companies (Takeovers and Mergers Panel) (Jersey) Law 2009⁴²;
 - (f) in Article 133(1) of the Bank (Recovery and Resolution) (Jersey) Law 2017⁴³;
 - (g) in Article 3(7) of the Register of Names and Addresses (Jersey) Law 2012⁴⁴;
 - (h) in Article 25(2)(a) of the Freedom of Information (Jersey) Law 2011⁴⁵;
 - (i) in Regulation 48(13) of the EU Legislation (Payment Services – SEPA) (Jersey) Regulations 2015⁴⁶;
 - (j) in paragraph 15(a)(i) and (b) of the EU Legislation (Information Accompanying Transfers of Funds) (Jersey) Regulations 2017⁴⁷;
 - (k) in Article 27(2)(a) of the Terrorist Asset-Freezing (Jersey) Law 2011⁴⁸;
 - (l) in paragraph 2(6) of Schedule 6 to the Medical Practitioners (Registration) (Responsible Officers) (Jersey) Order 2014⁴⁹;
 - (m) in the definition “health record” in Article 1(1) of the Medicines (Prescription Only) (Jersey) Order 1997⁵⁰;
 - (n) in Article 3(7) of the Planning and Building (Island Plan) (Jersey) Order 2009⁵¹;
 - (o) in Articles 7(8) and 27(4) of the Sex Offenders (Jersey) Law 2010⁵²;
 - (p) in Article 69(5) of the Goods and Services Tax (Jersey) Law 2007⁵³;
 - (q) in Article 1(1) (wherever occurring) and in Articles 20B(9), 27A(9) and 30(7) of the Health Insurance (Jersey) Law 1967⁵⁴;
 - (r) in Regulation 17(3) of the Health Insurance (Performers List for General Medical Practitioners) (Jersey) Regulations 2014⁵⁵.

- (2) In the following provisions for the words “sensitive personal data” there are substituted the words “special category data” –
 - (a) in paragraph 2(6) of Schedule 6 to the Medical Practitioners (Registration) (Responsible Officers) (Jersey) Order 2014⁵⁶;
 - (b) in Articles 1(1), 20B(9), 27A(9) and 30(7) of the Health Insurance (Jersey) Law 1967⁵⁷;
 - (c) in Regulation 17(3) of the Health Insurance (Performers List for General Medical Practitioners) (Jersey) Regulations 2014⁵⁸.
- (3) In Article 1(1) of the Health Insurance (Jersey) Law 1967⁵⁹ the definition “special category data” is moved to its correct alphabetical order following the definition “Social Security Tribunal”.

2 Public Records (Jersey) Law 2002

Article 39 of the Public Records (Jersey) Law 2002⁶⁰ is repealed.

3 Freedom of Information (Jersey) Law 2011

After Article 25(2) of the Freedom of Information (Jersey) Law 2011⁶¹ there is added the following paragraph –

- “(3) In determining for the purposes of this Article whether the lawfulness principle in Article 8(1)(a) of the Data Protection (Jersey) Law 201-⁶² would be contravened by the disclosure of information, paragraph 5(1) of Schedule 2 to that Law (legitimate interests) is to be read as if sub-paragraph (b) (which disapplies the provision where the controller is a public authority) were omitted.

4 Medical Practitioners (Registration) (Jersey) Law 1960

In Article 10C(9) of the Medical Practitioners (Registration) (Jersey) Law 1960⁶³ for the words “a disclosure of personal data which is exempt from the non-disclosure provisions of the Data Protection (Jersey) Law 2005, by virtue of Article 35(1) of that Law” there are substituted the words “permitted by Article 63 of the Data Protection (Jersey) Law 201-⁶⁴”.

5 Firearms (General Provisions) (Jersey) Order 2011

In the forms in Schedules 1 and 2 of the Firearms (General Provisions) (Jersey) Order 2011⁶⁵ for the first sentence there is substituted the following text –

- “The Parish is registered with the Data Protection Authority and all information is collected and used in compliance with the Data Protection (Jersey) Law 201-⁶⁶ and the Firearms (Jersey) Law 2000⁶⁷”.

6 Goods and Services Tax (Jersey) Law 2007

In Article 69(3) of the Goods and Services Tax (Jersey) Law 2007⁶⁸, the words “, in the Data Protection (Jersey) Law 2005, in Regulations made under that Law,” are deleted.

7 Health Insurance (Jersey) Law 1967

For Article 20B(3)(e) of the Health Insurance (Jersey) Law 1967⁶⁹ there is substituted the following sub-paragraph –

“(e) require the contractor to make returns to the Minister of data concerning health as defined in Article 1(1) of the Data Protection (Jersey) Law 201^{-70;}”.

8 Miscellaneous amendment: Electronic Communications (Jersey) Law 2000

For Article 2 of the Electronic Communications (Jersey) Law 2000⁷¹ there is substituted the following Article –

“2 Power for Regulations to modify legislation

- (1) The States may make Regulations amending or extending the interpretation of any expression defined in this Law or defining any expression used in this Law if the States considers it necessary to do so to take into account a change or advancement in technology.
- (2) The States may by Regulations modify the provisions of –
 - (a) any enactment; or
 - (b) any scheme, licence, authorization or approval issued, granted or given by or under any enactment,in such manner as they may think fit for the purpose of authorizing or facilitating the use of electronic communications or electronic storage (instead of other forms of communication or storage) for any purpose mentioned in paragraph (3).
- (3) Those purposes are –
 - (a) the doing of anything which under any such provisions is required to be or may be done by post or other specified means of delivery;
 - (b) the doing of anything which under any such provisions is required to be or may be authorized by a person’s signature or seal, or is required to be delivered as a deed or witnessed;
 - (c) the making of any statement or declaration which under any such provisions is required to be made under oath or to be contained in a statutory declaration;
 - (d) the keeping, maintenance or preservation, for the purposes or in pursuance of any such provisions, of any account, record, notice, instrument or other document;
 - (e) the provision, production or publication under any such provisions of any information or other matter;

- (f) the making of any payment that is required to be or may be made under any such provisions.
- (4) The power to make Regulations under this Article includes, in particular, the power to provide for –
- (a) the electronic form to be taken by any electronic communications or electronic storage the use of which is authorized by the Regulations;
 - (b) the conditions subject to which the use of electronic communications or electronic storage is so authorized;
 - (c) in relation to cases in which any such conditions are not satisfied, for treating anything for the purposes of which the use of such communications or storage is so authorized as not having been done;
 - (d) in connection with anything so authorized, a person to be able to refuse to accept receipt of something in electronic form except in such circumstances as may be specified in or determined under the Regulations;
 - (e) in connection with any use of electronic communications so authorized, intermediaries to be used, or to be capable of being used, the transmission of any data or for establishing the authenticity or integrity of any data;
 - (f) in connection with any use of electronic storage so authorized, persons satisfying such conditions as may be specified in or determined under the Regulations to carry out functions in relation to the storage;
 - (g) in relation to cases in which the use of electronic communications or electronic storage is so authorized, the determination of any of the matters mentioned in paragraph (5), or as to the manner in which they may be proved in legal proceedings;
 - (h) in relation to cases in which fees or charges are or may be imposed in connection with anything for the purposes of which the use of electronic communications or electronic storage is so authorized, different fees or charges to apply where use is made of such communications or storage;
 - (i) in relation to any criminal or other liabilities that may arise (in respect of the making of false or misleading statements or otherwise) in connection with anything for the purposes of which the use of electronic communications or electronic storage is so authorized, corresponding liabilities to arise in corresponding circumstances where use is made of such communications or storage;
 - (j) persons to prepare and keep records in connection with any use of electronic communications or electronic storage which is so authorized;
 - (k) the production of the contents of any records kept in accordance with the Regulations;

(l) a requirement imposed by virtue of sub-paragraph (j) or (k) to be enforceable at the suit or instance of such person as may be specified in or determined in accordance with the Regulations.

(5) The matters referred to in paragraph (4)(g) are –

- (a) whether a thing has been done using an electronic communication or electronic storage;
- (b) the time at which, or date on which, a thing done using any such communication or storage was done;
- (c) the place where a thing done using such communication or storage was done;
- (d) the person by whom such a thing was done; and
- (e) the contents, authenticity or integrity of any electronic data.

(6) Regulations under this Article may –

- (a) provide for any conditions or requirements imposed by the Regulations to be framed by reference to the directions of such persons as may be specified in or determined in accordance with the Regulations;
- (b) provide that any such condition or requirement is to be satisfied only where a person so specified or determined is satisfied as to specified matters; and
- (c) make such incidental, supplemental, consequential and transitional provision as the States think fit,

and the provision that may be made by virtue of sub-paragraph (c) includes provision modifying any enactment or any scheme, licence, authorization or approval issued, granted or given by or under any enactment.”.

1	<i>P.117/2017</i>
2	<i>chapter 12.200</i>
3	<i>chapter 16.300</i>
4	<i>chapter 16.330</i>
5	<i>chapter 16.325</i>
6	<i>chapter 16.800</i>
7	<i>chapter 16.800.15</i>
8	<i>chapter 15.350</i>
9	<i>chapter 08.780</i>
10	<i>chapter 13.225</i>
11	<i>chapter 13.875</i>
12	<i>chapter 13.100</i>
13	<i>chapter 13.075</i>
14	<i>chapter 13.125</i>
15	<i>chapter 13.425</i>
16	<i>chapter 13.225</i>
17	<i>chapter 17.245.51</i>
18	<i>L.10/2017</i>
19	<i>chapter 08.785</i>
20	<i>chapter 13.255</i>
21	<i>chapter 13.250</i>
22	<i>chapter 13.125</i>
23	<i>chapter 12.050</i>
24	<i>chapter 08.680</i>
25	<i>chapter 08.780</i>
26	<i>chapter 17.860</i>
27	<i>chapter 12.200</i>
28	<i>chapter 16.330</i>
29	<i>chapter 08.840</i>
30	<i>chapter 07.770</i>
31	<i>chapter 15.360</i>
32	<i>chapter 23.750</i>
33	<i>chapter 08.830</i>
34	<i>L.2/2005 (chapter 15.240)</i>
35	<i>chapter 15.260</i>
36	<i>chapter 13.425</i>
37	<i>chapter 15.240</i>
38	<i>chapter 03.530</i>
39	<i>chapter 08.830.10</i>
40	<i>chapter 11.300</i>
41	<i>chapter 13.125</i>
42	<i>chapter 13.145</i>
43	<i>L.10/2017</i>
44	<i>chapter 15.660</i>
45	<i>chapter 16.330</i>
46	<i>chapter 17.245.54</i>
47	<i>R&O.57/2017</i>
48	<i>chapter 17.861</i>
49	<i>chapter 20.600.80</i>
50	<i>chapter 20.625.95</i>
51	<i>chapter 22.550.30</i>
52	<i>chapter 23.815</i>
53	<i>chapter 24.700</i>

54	<i>chapter 26.500</i>
55	<i>chapter 26.500.20</i>
56	<i>chapter 20.600.80</i>
57	<i>chapter 26.500</i>
58	<i>chapter 26.500.20</i>
59	<i>chapter 26.500</i>
60	<i>chapter 15.580</i>
61	<i>chapter 16.330</i>
62	<i>P.116/2017</i>
63	<i>chapter 20.600</i>
64	<i>P.116/2017</i>
65	<i>chapter 23.200.60</i>
66	<i>P.116/2017</i>
67	<i>chapter 23.200</i>
68	<i>chapter 24.700</i>
69	<i>chapter 26.500</i>
70	<i>P.116/2017</i>
71	<i>chapter 04.280</i>