Data protection webinar

All change?

New Data Protection Law in the Channel Islands –

an introduction to the new Guernsey and Jersey laws

8 December 2017

CAREY OLSEN

Introduction

Overview

- Background
- Genesis of the new laws
- Guernsey Law
- Jersey Law
- Recent Case Law
- Sources of Guidance

Q&A – Huw Thomas & Richard Field

CAREY OLSEN

Background

Why are we here?

- Data protection in the digital economy
- On 25th May 2018, the European Union's General Data Protection Regulation ("GDPR") and Law Enforcement Directive ("LED") will come into full effect in EU Member States

Background

The current regime

- Jersey and Guernsey data protection law is based on 1995 EU Directive & UK Data Protection Act 1998:
  - The Data Protection (Bailiwick of Guernsey) Law 2001 sets out the current Guernsey data protection law.
  - The Data Protection (Jersey) Law 2005 sets out Jersey's current data protection regime.
- Adequacy decisions of the European Commission –
  - **Guernsey -** 2003/821/EC (amended December 2016)
  - **Jersey** - 2008/393/EC (amended December 2016)

Background

Aims of the new regimes

- New Jersey and Guernsey legislation will provide equivalent domestic rights to those enjoyed by EU citizens.
- 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 and Guernsey already have adequacy decisions for the purposes of the GDPR - the new data protection legislation is required to maintain that status and achieve adequacy for LED purposes.
- Adequacy will permit data flows between Jersey/Guernsey and the EU to continue uninterrupted.

Background

Jersey and Guernsey

- Original intent was to continue with a single regulator with aligned legislation
- This has proven to be unachievable
- Legislation therefore similar but divergent
- Two regulators
- Recognition of inter-island equivalence?

Guernsey legislation

CAREY OLSEN

Genesis of the Guernsey law

Timeline

• GDPR published	May 2016
• First Policy Letter (GDPR overview/reappointment of DPC)	September 2016
• Second Policy Letter (GDPR legislation)	April 2017
• Draft legislation published	October 2017
• States Debate	November 2017
• Privy Council approval	TBC
• New Data Protection Law in place	May 2018

CAREY OLSEN

Secondary legislation

Ordinances and regulations

- Law Enforcement Ordinance
- Transitional provisions
- Data Protection Authority (structure, funding and related matters)
- Exemptions and exceptions (including Trusts/Employment, etc.)
- Regulations (including regulatory)

Core features and concepts

Where to start?

- Pull up a comfortable chair…… 267 pages, 26 Parts, 10 Schedules
- But……if you've been following GDPR, there are no surprises (think adequacy)
- Bear in mind
  - Object of the law (s.1)
  - Definitions (s.111) - Personal Data (see also Schedule 9, section 1)
  - Registration (s.39, also Schedule 4)
  - Levy on Controllers and Processors (s.40)

Core features and concepts

Territoriality

- Processing is in the context of a controller or processor established in the Bailiwick, or
- Personal data is that of a Bailiwick resident, and is processed in the context of:
  - the offering of goods or services to the resident (whether for payment or not); or
  - the monitoring of the resident's behaviour in the Bailiwick.
- The Law applies regardless of where the processing takes place, and has extra-territorial application unless the context requires otherwise.

Core features and concepts

Principles

- The Data Protection Principles (s.6) – controller "must"…..
  - Lawfulness, fairness and transparency (note Schedule 2, Part I, s.2 (a) – contract)
  - Purpose limitation
  - Minimisation
  - Accuracy
  - Storage Limitation
  - Integrity and Confidentiality
    - Accountability
- Rights and data export

Core features and concepts

Core concepts

- Data Controller
  - Reasonable steps to facilitate the exercise of data subjects' rights (s.25)
  - Must take reasonable steps to ensure compliance (and demonstrate it)(s.31)
    - Nature, scope, context and purpose of processing
    - Likelihood of risks to data subjects
    - Best practices in technical and organisational measures
    - Costs of implementation
- Joint controllers / relationship with processors (ss.33-34)

Core features and concepts

Core concepts

- Breach notification (s.42)
  - Processor to tell Controller “as soon as practicable”
  - Controller to tell Authority within 72 hours (unless not practicable)
  - Notify data subject if “high risk to significant interests”, unless:
    - Cannot be used by others
    - Threat neutralised
    - Notification involves disproportionate effort
  - Can publish a notice

Core features and concepts

Core concepts

- Overseas transfers (Part X)
  - Acceptable to authorised jurisdictions
    - Bailiwick, EU, “adequate” jurisdictions
    - UK (Brexit had to appear somewhere….)
  - Subject to safeguards (i.e. model contracts, BCRs, approved code, other agreements, approval of Authority)
  - Court Order, international agreement, consent, legal proceedings, vital interests, public register, etc.

Core features and concepts

Core concepts

- Subject Access Requests
  - ss.13 - 15 (information to be given, privacy notices), exceptions involving disclosure of a third party's personal data
  - ss.27-29 (one month to respond, potentially extend up to two months, no fee)
  - exemptions remain
- Right to erasure – but subject to usual limitations (Schedule 2)

Core features and concepts

Core concepts

- Data security (s.41)
  - Reasonable steps, but be aware of s.31 factors (including “best practice”)
  - Can include pseudonymisation and encryption
- Data Protection Officers (s.47)
  - Mandatory where
    - Processing is part of a core activity and requires or involves
      - Large-scale and systematic monitoring of data subjects; or
      - Large-scale processing of special category data
  - Voluntary

Core features and concepts

Core concepts

- The Data Protection Authority (Part XI)
  - Much more proactive role
  - Levy to fund
  - Extensive powers
  - Transitional provisions
  - Opinions and guidance
  - Publication (includes breach notifications, complaints, investigations, etc. s.74)
    - "Because of the gravity of the matter, or other exceptional circumstances"

Core features and concepts

Core concepts

- Sanctions
  - Fines are only one part
  - Ban on processing can hurt you more
  - Fines
    - Consider factors affecting gravity
    - Can be recovered as civil debt
    - Paid to States of Guernsey

CAREY OLSEN

Core features and concepts

Core concepts

- Fines (s.75)
  - £5million (higher limits may be prescribed via Ordinance)
    - Child consent / failure to inform of anonymisation / breach of Data Protection Principles / Duties of Controller and Processor / Administrative duties (such as registration) / security / DPIA / DPO
  - £10million (higher limits may be prescribed via Ordinance)
    - Lawfulness of processing / data subjects' rights / overseas transfer / breach of Ordinance or Regulations made under the law

Core features and concepts

Core concepts

- Fines (s.75)
  - £300,000 limit unless fine is less than 10% of total global annual turnover or total global gross income for preceding financial year for that person
  - Fine limited to 10% of global annual turnover or total global gross income of the person during the period of breach, up to a maximum period of 3 years
  - Limits to be applied in aggregate

Core features and concepts

Core concepts

- Others
  - Civil action for breach of duty (damages, injunction, declaration) (s.79)
  - An award for distress, inconvenience or other adverse effect can be made, even if no actual physical or financial loss or damage is suffered
  - Possibility of class action lawsuits by data subjects (s.97)
  - Power of States to make further Ordinances and Regulations (ss.104-109)

Core features and concepts

Core concepts

- Others
  - Appeals (ss.81-84)
  - Criminal liability of directors (s.92)
  - Criminal penalties
    - Summary - 12 months or level 5 fine, or both
    - Indictment – 2 years or level 5 fine, or both

Jersey legislation

CAREY OLSEN

Structure and timetable

- Data Protection (Jersey) Law 20-
- Data Protection Authority (Jersey) Law 20-
- Proposed legislative 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.

Data Protection (Jersey) Law 20-

- Repeals and replaces existing Data Protection (Jersey) Law 2005
- Evolutionary not revolutionary
- Familiar from GDPR

CAREY OLSEN

Data Protection (Jersey) Law 20-

Fairly Vanilla…

- Material application tracks GDPR
- Excludes purely domestic processing

Data Protection (Jersey) Law 20-

Fairly Vanilla…

Territorial application – includes processing:

- in the context of a controller or processor established in Jersey;
- 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
- by a controller or processor not established in Jersey where the processing –
  - relates to data subjects who are in Jersey, and
  - is for the purpose of offering goods or services to persons in Jersey or monitoring the behaviour of such persons.

Data Protection (Jersey) Law 20-

Fairly Vanilla

Most provisions of law reflect GDPR:

- Lawful processing (Art 9)
- Information provision (Article 12)
- Record keeping (Art 14)
- Data protection by Design/Default (Art 15)
- Data protection impact assessments (Art 16)
- Appointment of processors (Art 19)
- Breach notification (Art 20)
- Data security (Art 21)
- Processor responsibilities (Art 22)
- Appointment of DPO (Art 24)
- Rights of data subjects (Part 6 of Law)
- Cross border transfer (Part 7)

Data Protection (Jersey) Law 20-

Appointing representatives

- Obligation narrower than GDPR
- Applies only to 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

Data Protection (Jersey) Law 20-

Data protection principles

Article 8 lists 6 GDPR principles:

- lawfulness, fairness and transparency
- purpose limitation
- data minimization
- accuracy
- storage limitation
- integrity and confidentiality

Accountability not listed as principle (unlike GDPR) – listed at Article 6(1)

Data Protection (Jersey) Law 20-

Joint controllers

Article 7

- 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.
- 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.

Data Protection (Jersey) Law 20-

Joint controllers

Article 7

- Regardless of the terms and conditions of any arrangement –
  - a data subject may exercise any right that he or she has under this Law against any joint controller; and
  - each joint controller is jointly and severally liable for any damage caused by processing if it is in contravention of this Law.
- Where a joint controller proves that it had no responsibility for the damage, it may be exempted from liability.

Data Protection (Jersey) Law 20-

Children

- Children may give consent to information society services from 13
- However, note Age of Majority (Jersey) Law 1999 – age of majority 18
- Those below likely to lack contractual capacity (except for “necessaries” – Supply of Goods & Services (Jersey) Law 2009)

Data Protection (Jersey) Law 20-

Offences

- Unlawfully obtaining personal data (Article 71) (previously set out in Article 55 of the 2005 Law)
- Requiring a person to produce certain records in (Article 72) (previously set out in Article 56 of the 2005 Law)
- Providing false information (Article 73) (previously set out in Article 60 of the 2005 Law); and
- Obstruction (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).

Data Protection (Jersey) Law 20-

Offences

Article 75 – secondary liability for company officers/partners

CAREY OLSEN

Data Protection (Jersey) Law 20-

Transitional provisions

- Consents currently in force deemed to last until 25 May 2019
- Current Information provision/fair processing notices will also last until 25 May 2019

BUT – THIS WILL NOT SATISFY GDPR

Data Protection Authority (Jersey) Law 20-

Purpose of law

Provides investigatory and enforcement powers, including the power to impose administrative fines, which may be used to secure compliance with the draft Data Protection Law.

Deals with Authority's governance structure and oversight arrangements.

- A Board will be formed, becoming the principle corporate body responsible for regulating compliance.
- The Information Commissioner will become the Chief Executive Officer of the Authority.

Data Protection Authority (Jersey) Law 20-

Purpose of law

Provides investigatory and enforcement powers, including the power to impose administrative fines, which may be used to secure compliance with the draft Data Protection Law.

Deals with Authority's governance structure and oversight arrangements.

- A Board will be formed, becoming the principle corporate body responsible for regulating compliance.
- The Information Commissioner will become the Chief Executive Officer of the Authority.

Data Protection Authority (Jersey) Law 20-

Financing the regulator

Summary notes provide:

In view of the need for more independent, proactive and robust regulation, the annual cost of running the Authority, compared with the current Office of the Information Commissioner will increase by an estimated £1.1 million to £1.65 million per annum. There will also be a need for an additional £350,000 to support one-off implementation work.

However, from 2020 the increased annual costs will be offset by increased revenues from on business.

Data Protection Authority (Jersey) Law 20-

Financing the regulator

The recommendation is a risk-based tiered administrative charge. With this option, organisations acting as data processors or controllers would be assessed and classified according to the risk of their processing activities, then allocated to a tiered-band defined by their perceived risk. A flat annual fee for this tier would be then be levied against the organisation.

Data Protection Authority (Jersey) Law 20-

Financing the regulator

- Art 17(1) A controller or processor established in Jersey must not cause or permit personal data to be processed without being registered as a controller or processor
- Applies to controllers and processors
- Fund entities?
- Processors have 26 weeks to comply
- Controllers who have already notified can rely until renewal on existing notification

Data Protection Authority (Jersey) Law 20-

Article 15 – International Co-operation

The Authority must so far as practicable take steps to –

- develop international cooperation mechanisms to facilitate the effective enforcement of legislation for the protection of personal data
- **provide international mutual assistance in the enforcement of legislation for the protection of personal data, including through notification, complaint referral, investigative assistance and information exchange, subject to appropriate safeguards for the protection of personal data and the significant interests of data subjects**

Data Protection Authority (Jersey) Law 20-

Powers of regulator

Broad inquiry/audit powers – Articles 21-24

Art 25 - On breach determination – Authority may:

- issue a reprimand to the recipient
- issue a warning to the recipient that the intended processing or other act or omission is likely to contravene the Data Protection Law
- Order one of a number of interventions (25(3))

Data Protection Authority (Jersey) Law 20-

Intervention powers

May make order requiring recipient to:

- bring specified processing operations into compliance with the Law
- notify a data subject of any personal data breach
- comply with exercise a data subject right
- rectify or erase personal data
- restrict or limit the recipient's processing operations
- notify persons to whom the personal data has been disclosed of the rectification, erasure or temporary restriction on processing

Data Protection Authority (Jersey) Law 20-

Administrative fines

Article 27(1)

- Less serious infractions – up to £5 million
- More serious infractions – up to £10 million
- Subject to total cap of higher of £300,000 and 10% of annual global turnover
- An administrative fine ordered against any person whose processing of data that gave rise to the fine was in the public interest and not for profit must not exceed £10,000 – Whistleblowers?

Overlap with GDPR/Guernsey/UK fines?

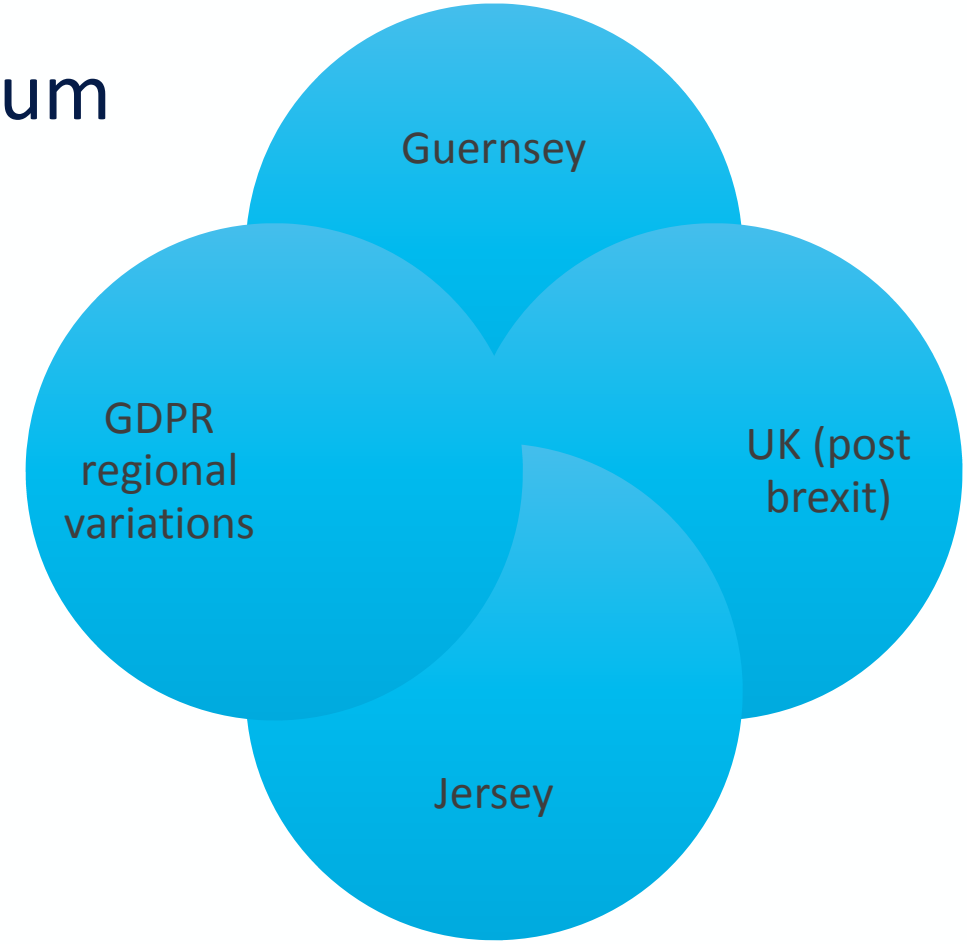
Administrative fines

Article 27(1)

- Less serious infractions – up to £5 million
- More serious infractions – up to £10 million
- Subject to total cap of higher of £300,000 and 10% of annual global turnover

Overlap with GDPR/Guernsey/UK fines?

A conundrum



CAREY OLSEN

Recent case law

CAREY OLSEN

Vicarious Liability - Morrisons

- In 2014, Andrew Skelton (a a senior auditor at Morrison's Bradford headquarters) leaked the payroll data of almost 100,000 Morrisons employees – including their names, addresses, national insurance numbers, bank accounts and salaries - putting them online and sending them to newspapers.
- His apparent motivation was that he was subjected to (minor) disciplinary action for an unrelated issue.
- The employee was ultimately given an eight-year prison sentence for various criminal offences as a result of his actions, including under the Computer Misuse Act 1990 and the UK Data Protection Act 1998 (**DPA**).

Vicarious Liability - Morrisons

- The data breach cost the company more than £2 million in professional and legal fees to rectify.
- A group of 5,518 former and current Morrisons employees lodged a claim for compensation for the upset and distress caused.
- The group claimed that the leak exposed them to the risk of identity theft and potential financial loss and that Morrisons was responsible for breaches of privacy, confidence and data protection laws.
- The group claimed that Morrisons were either directly liable as data controller or were vicariously liable for the actions of AS.

Vicarious Liability – Morrisons

Primary liability could not be imposed on Morrisons under the DPA, for breach of confidence or for misuse of private information. This finding was made on the basis that it was not Morrisons itself which caused the data breach – rather, the breach was caused by Mr. Skelton, acting without authority and criminally. As such, Morrisons did not directly misuse any information personal to the affected data subjects, nor did it authorise such misuse or permit it by carelessness.

Vicarious Liability – Morrisons

However, vicarious liability could be imposed on Morrisons in relation to the actions of Mr. Skelton:

- An employer such as Morrisons **can** be held liable for the acts of their employees "in the conduct of the employees' employment"; and
- Mr. Skelton's actions in leaking the data were committed in the conduct of his employment. The court gave this term the broad interpretation which the Supreme Court applied in 2016 (in an unrelated case in which Morrisons was also the defendant) in finding that there was "sufficient connection" between the position in which AS was employed and his wrongful conduct in leaking the data
- The drafting of the DPA does **not** preclude the imposition of vicarious liability on a company in circumstances where direct liability for a breach of the DPA would rest with an employee (in this case, AS).

Sources of Guidance

CAREY OLSEN

Guidance

Useful sources of further information

- Data Protection Commissioner's website
  - https://dataci.gg/
  - https://thinkgdpr.org/
- UK Information Commissioner's website
  - https://ico.org.uk/
- Article 29 Working Party guidance
  - http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083

Guidance

Useful sources of further information

- Advocate General's opinions/ECJ decisions
- Channel Islands Guide to GDPR
  - https://www.careyolsen.com/briefings/the-channel-islands-guide-to-the-general-data-protection-regulation
- Carey Olsen briefing notes/updates on LinkedIn
- Seminars/training
- E-Learning modules
  - http://www.gdprlearning.co.uk/?gclid=EAIaIQobChMIlIT43Kr11wIVLrftCh2LKg4gEAAYASAAEgLNhfD_BwE

CAREY OLSEN

Summary

Risk assessment

- Establish baseline risk appetite
- Assess controls/risks
  - Likelihood of a serious breach occurring?
  - Impact if such a breach occurred?
  - Legal
    - Regulatory
    - Customer/client
    - Counterparties

3 x 3 Risk Matrix

LIKELIHOOD				
	Likely	Medium Risk	High Risk	Extreme Risk
	Unlikely	Low Risk	Medium Risk	High Risk
	Highly Unlikely	Insignificant Risk	Low Risk	Medium Risk
		Slightly Harmful	Harmful	Extremely Harmful
		CONSEQUENCES		

Summary

What does this mean?

- Follows GDPR
- Cultural change is vital
- Engagement across the business
- Ensure staff have a basic understanding
- Risk assessments and prioritise
- Monitor guidance and updates

CAREY OLSEN

OFFSHORE LAW SPECIALISTS

BRITISH VIRGIN ISLANDS CAYMAN ISLANDS GUERNSEY JERSEY
CAPE TOWN HONG KONG LONDON SINGAPORE

careyolsen.com