J.DPA

JERSEY DATA PROTECTION ASSOCIATION

THE GDPR AND FUNDS
NEW CHALLENGES IN GOVERNANCE

J.DPA
JERSEY DATA PROTECTION ASSOCIATION

- Introductions / Overview of J.DPA
- What is GDPR?
- Key Concepts
- GDPR – The Fundamentals
- Key Changes to the Current Regime
- Fund Services – Specific Issues
- Where to begin?
- Q&A

J.DPA
JERSEY DATA PROTECTION ASSOCIATION

David Carney
Director of Risk Assurance Services PwC
Chairman of the J.DPA
david.carney@pwc.com
07700 838266

pwc

Huw Thomas
Counsel Carey Olsen
Vice-Chairman of the J.DPA
huw.thomas@careyolsen.com
01534 822224

CAREY OLSEN

J.DPA
JERSEY DATA PROTECTION ASSOCIATION

Overview of JDPA

- The Jersey Data Protection Association was formed to help organisations , from large to small to understand, respond and comply with the ever increasing demands of customers, employees, suppliers and regulators in the field of data privacy and protection.

- Our aim is to provide a platform for those responsible or interested in data protection within their respective businesses, to improve their understanding of data protection through attendance at seminars, formal training and networking events where you will be encouraged to share experiences, concerns or materials which may be of interest to other members across industry.

J.DPA
JERSEY DATA PROTECTION ASSOCIATION

What's all the fuss about GDPR?

The current landscape

- Current EU data protection law is based on Directive 95/46/EC (the "**Directive**"), which was introduced in 1995
- EU Directive – so needed transposing into national law
- UK enacted the **Data Protection Act 1998**
- Part of Directive is a prohibition on data transfer outside EEA to jurisdictions which do not provide an "adequate" level of protection for personal data
- **Data Protection (Jersey) Law 2005** – almost identical to DPA
- 2008/393/EC: Commission Decision of 8 May 2008 that Jersey is an "adequate" jurisdiction
- **Guernsey** have followed a similar (and earlier) path to adequacy – under the **Data Protection (Bailiwick of Guernsey) Law 2001**

OUR CURRENT DATA PROTECTION REGIME IS BASED ON AN EU DIRECTIVE ISSUED IN 1995…

In December 1995, there were 16 million users of the internet

1% *of Europeans used the internet*

Amazon
had just launched

2 years *before Google was launched*

The common format for data storage was CD (700mb of data)

iPhone

12 years *Before the launch of the first iphone*

AND NOW…

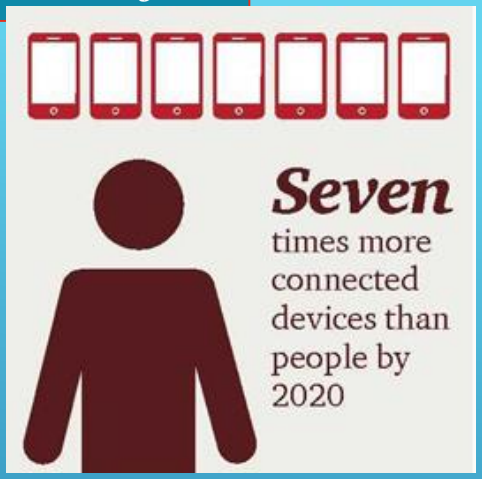
Yahoo!
Hackers stole personal data from 500m accounts

1.3 billion
Facebook – monthly users

TalkTalk Telecom Group PLC

Telecoms company TalkTalk has been issued with a record £400,000 fine by the ICO for security failings that allowed a cyber attacker to access customer data "with ease".

300 million
Monthly users of Instagram



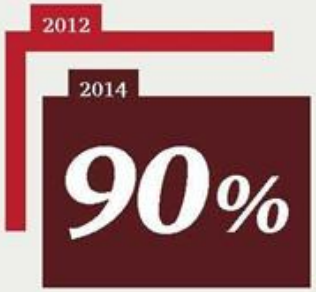
Seven times more connected devices than people by 2020

30 billion
Messages sent per day using WhatsApp – 4 for every single person in the world

The average time a US consumer spends using their smart phone a day

Hackers selling 117 million LinkedIn passwords

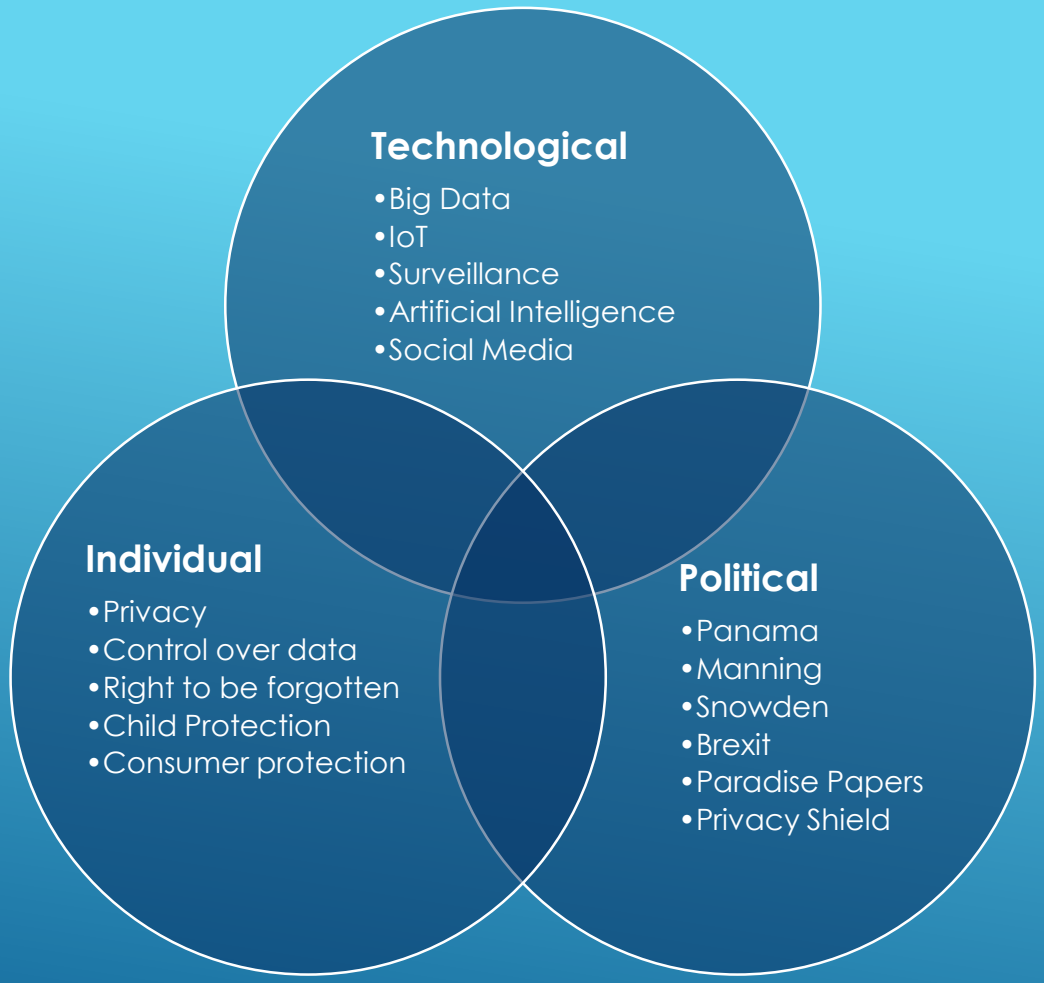
3 billion
Google searches per day



of the data that exists today was created in the last 2 years

284 million
Monthly users of Twitter

Drivers of Change



J.DPA
JERSEY DATA PROTECTION ASSOCIATION

What is GDPR?

GDPR is an abbreviation of the EU's General Data Protection Regulation, the largest change to the protection of personal data since the Directive in 1995. The objective of the GDPR is to bolster and unify data protection across the European Union. It will be enforceable from the 25th May 2018, replacing the Data Protection Act 1998 in the United Kingdom and equivalent legislation across EU Member States.

J.DPA
JERSEY DATA PROTECTION ASSOCIATION

Data Protection (Jersey) Law 2018

Following Privy Council approval, the Royal Court on 16th February registered new data protection legislation that will strengthen individuals' rights and enable Island businesses to continue accessing international markets.

The Data Protection (Jersey) Law 2018 and Data Protection (Authority) Jersey Law 2018 will come into effect on 25 May 2018.

The new Laws will enable data to continue moving freely between Jersey and the European Union, benefitting trade and helping law enforcement agencies cooperate with their counterparts in other jurisdictions.

J.DPA
JERSEY DATA PROTECTION ASSOCIATION

Key Concepts

What do we mean by personal data?

"**Personal data**" means any information relating to an identified or identifiable natural person (a '**data subject**')

So what is personal data?

- '**Any information**' is understood to be literal. Information could be anything from a person's name to her location.
- '**Relating to**' refers to the information's purpose and impact on someone's privacy rights. Its juxtaposition with other content is also important. For example, a job title would not necessarily relate to a person, but a job title combined with a name likely would.
- '**Identified**' means that an individual person has been named or singled out—for example, by specific characteristics. 'Identifiable' includes **indirect identification**, taking into account all the 'means reasonably likely to be used' to identify the person.
- A '**natural person**' is a real human being, as distinguished from a corporation. This person is referred to as the **data subject**.

Sensitive Personal Data/ "Special Categories"

Expanded Definition

- Personal data revealing racial or ethnic origin
- Political opinions,
- Religious or philosophical beliefs, or
- Trade-union membership;
- Genetic or biometric data for the purpose of uniquely identifying a natural person; and
- Data concerning health, sex life or sexual orientation.
- (in Jersey) – Criminal record data

Data Controllers

The **Data Controller** is a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal **data** are, or are to be, processed.

In the Funds Service world, this would include the General Partner (or the Fund itself in the case of a listed fund) but also other parties where they process personal in their own right for their own purposes including Administrators, Managers and Advisers

Data Processor

Data processor, in relation to personal data, means any person (other than an employee of the data controller) who processes the data on behalf of the data controller.

In the Funds World, this will include Administrators, Adviser, Manager, Promoter and other potential service providers.

J.DPA
JERSEY DATA PROTECTION ASSOCIATION

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 law. Controllers will in particular be required to consider data protection standards when developing new systems, and to carry out data protection impact assessments, ensuing 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.

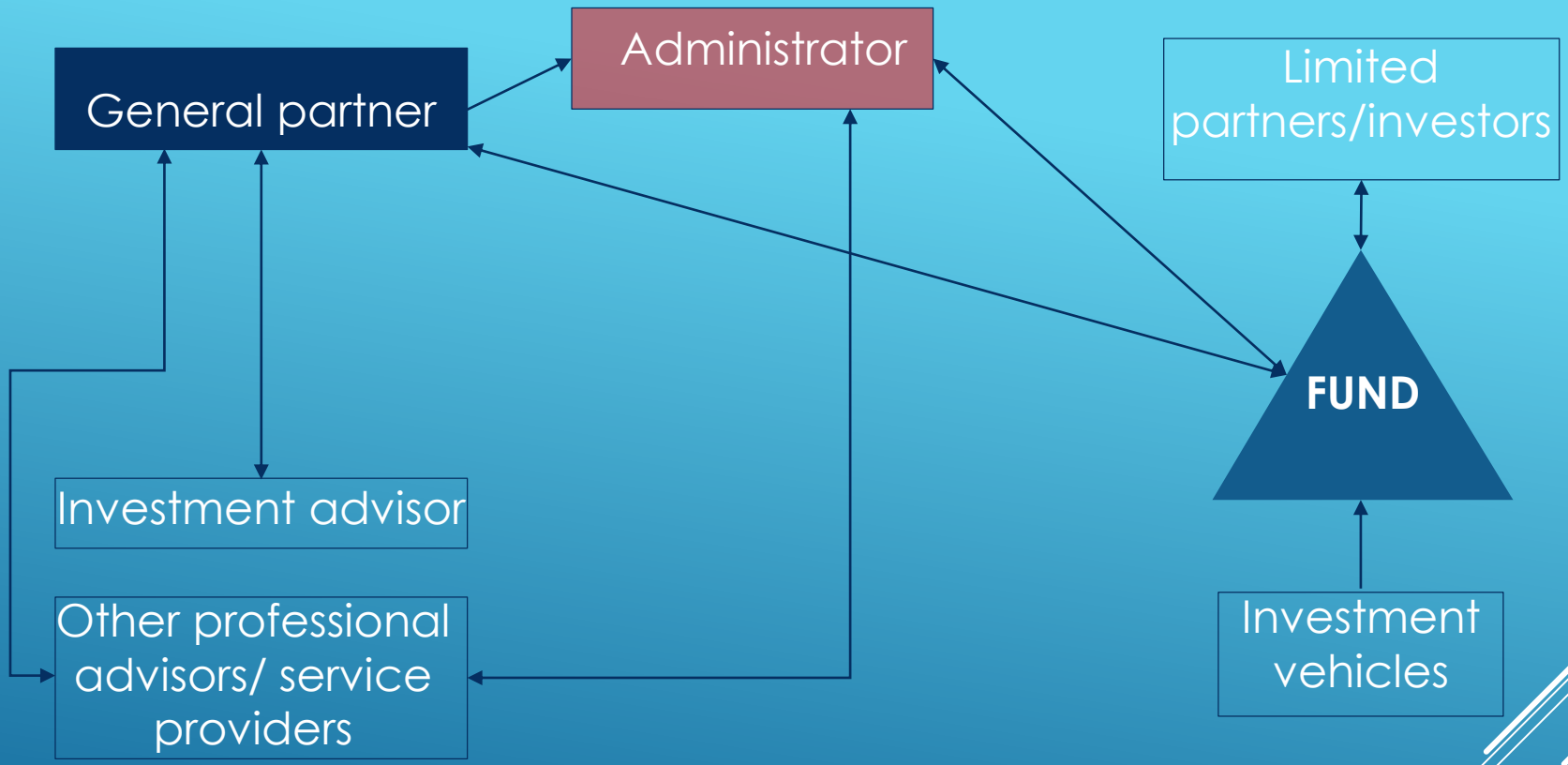
J.DPA
JERSEY DATA PROTECTION ASSOCIATION

Fund Services Specific Issues

Sources of Personal Data

- Investors/subscribers – AML records could include sensitive categories of data
- Employees/officers/shareholders
- Employees of institutional investors
- Employees of intermediaries/counterparties
- Employees of advisors
- Marketing contacts
- UBOs/connected persons
- Could also be particularly sensitive records collated through due diligence performed on potential investments and associated parties, including personal opinions on individuals.
  Would you want this to be shared with the data subject?

Basic Fund Structure



Key Funds Issues

- The distributed nature of functions and governance within a funds structure – the standard funds structure presumes that the general partner (Controller) of a fund will outsource almost the entirety of fund functions to an administrator (Processor). **The Controller still remains Accountable.**
- One of the functions which is outsourced is data collection – meaning that information governance is often based on a range of outsourced agreements. The GDPR significantly enhances information governance requirements around outsourcing – in particular in relation to the amount of information which is expected to be included in data processing agreements.
- Information security more difficult in a distributed structure – different systems/standards
- Position of GP/fund entities different from service providers
- Don't overlook other data sharing arrangements – Advisers/Managers/Promoters/NEDs

Key Funds Issues

- Who does what?
  - GP/ Listed Funds likely to be data controllers.
  - Nature of "standard" governance/service model means that GP/Fund entity unlikely to have resources/infrastructure to achieve compliance
  - Likely to rely on service providers to provide data protection compliance
  - Will need to undertake a number of steps

J.DPA
JERSEY DATA PROTECTION ASSOCIATION

GDPR – The Fundamentals

GPDR – the principles

Mostly (but not all) familiar

Lawfulness, fairness and transparency

- Personal data shall be processed **lawfully**, **fairly** and in a **transparent** manner in relation to the data subject

Purpose limitation

- Personal data shall be collected for **specified**, **explicit** and **legitimate** purposes and not further processed in a manner that is incompatible with those purposes

GPDR – the principles

Mostly (but not all) familiar

Data Minimisation

- Personal data shall be **adequate**, **relevant** and **limited** to what is necessary in relation to the purposes for which they are processed

Accuracy

- Personal data shall be **accurate** and, where necessary, kept up to date

GPDR – the principles

Mostly (but not all) familiar

Storage Limitation

- Personal data shall be kept in a form which **permits identification of data subjects** for **no longer than is necessary** for the purposes for which the personal data are processed

Integrity & Confidentiality

- Personal data shall be processed in a manner that **ensures appropriate security of the personal data**, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, **using appropriate technical or organisational measures**

GPDR – the principles

…and one new one – particularly important for General Partners!

Accountability

- The **controller** shall be **responsible** for, and **be able to demonstrate compliance** with the GDPR

J.DPA
JERSEY DATA PROTECTION ASSOCIATION

Key Changes to the Current Regime

GDPR overview

"High impact" changes

- Extra territoriality
- Breach notification
- Sanctions
- Organisational measures:
  - Privacy by design / by default
  - Accountability
  - DPIAs
- Consent
- Data protection officers
- Enhanced individual rights - (Disclose/Delete/Freeze/Correct It)
- Duties on processors

GDPR overview

Extra-territoriality

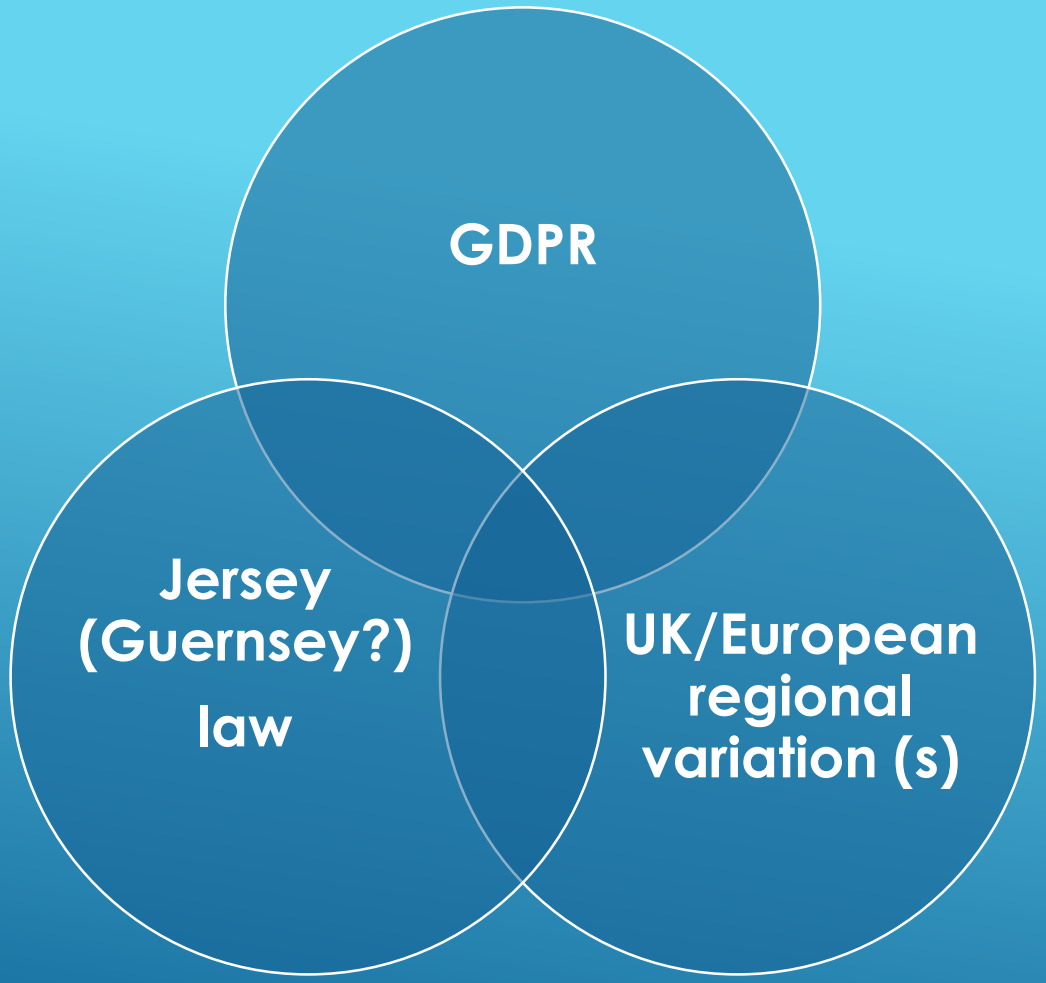
- If a controller or processor has an establishment within the EU and processing takes place "in the context" of that establishment, GDPR applies
  - Irrelevant where actual processing takes place
  - Legal form is not the determining factor
- Extends to non-EU controllers/processors where:
  - Offering goods or services to data subjects in the EU, whether connected to payment or not
  - Monitoring the behaviour of data subjects, if the behaviour is in the EU

GDPR overview

Extraterritoriality

- Offering goods or services
  - Intention to make them available to data subjects in the EU?
  - Mere accessibility of a website? Currency, language, etc.
- Monitoring behaviour
  - Tracking on internet, profiling techniques, used for what purposes?
- If outside the EU (i.e. Channel Islands), must appoint a representative in the EU in writing (some exceptions) (Article 27)

Which Law??



GDPR overview

Breach notification

- No current requirement in Jersey (although guidance on Information Commissioner's website)
- **Mandatory breach reporting to the Supervisory Authority** where risk of identity (or other) theft, financial loss, reversal of pseudonymisation, reputational damage, economic or social disadvantage, regulatory issues
- Strict timescale for notification (72 hours where "feasible"), unless breach unlikely to result in risk to rights and freedoms of data subject
- Explain if you need longer

GDPR overview

Breach notification

- **Notify individuals** if there is a "high risk" to their rights and freedoms, "without undue delay"
- Notification to data subjects must include nature of breach and recommendations to mitigate its impact
- **Processors have to report breaches to controllers**, irrespective of risk
- **Processors now have direct obligations** (records, security measures, written consent of controller for sub-processing, notify controller of security breach, etc.)

Need to think about what this means for your structure – who needs to notify who?
When and how will the controller be informed.
Who needs to engage with the Supervisory Authority?

What if it all goes wrong?

Sanctions

- Up to **€20 million or 4% of annual global turnover** (prior year), whichever is greater, for more serious breaches
  - Basic conditions of processing, consent, data subjects' rights, international transfers, non-compliance with an order of a Supervising Authority
- Up to **€10 million or 2% of annual global turnover** (prior year), whichever is greater, for less serious breaches
  - Obligations of the controller/processor (design/default), representative of non-EU controller, choice of processor, record keeping, breach notification, data security, etc.)

What if it all goes wrong?

Jersey Sanctions

- **£5,000,000** for "lower category" issues
- **£10,000,000** for "upper category" issues
- Overall cap - an administrative fine must not exceed £300,000 or 10% of the person's total global annual turnover or total gross income in the preceding financial year, whichever is the higher.

GDPR overview

Cross border transfers

- General rules remain
- Transfers outside the EU prohibited unless recipient country is "adequate", companies have implemented a data transfer mechanism or there is a statutory derogation
- More stringent requirements for "adequacy" (not just about national regime)
- "Adequacy" is "essentially equivalent" to that guaranteed in the EU
- Jersey (and Guernsey) need to maintain "adequacy"
- Position of the UK….?

GDPR overview

Organisational measures

- Data Protection by design and by default (Article 23)
- Obligation to **maintain records of all processing activities** (Article 30), including the purposes of the processing
  - a description of the categories of data
  - a description of the categories of recipients, including recipients in third countries
  - where possible, the time limits for erasure
  - a description of the technical and organisational security measures

Need to cast the net wide when thinking about what personal data is being processed and by whom, beyond simply the administrator.
What about NEDs? Copies of data likely to be held and processed by advisers/managers. Board packs? Hard copy documents?

GDPR overview

Organisational measures

- **Obligation to appoint Data Protection Officer** if core activities consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale. Guidance suggests monitoring which is caught will include AML/CFT checks

GDPR overview

Organisational measures

- **Data Protection Impact Assessment**
  - A requirement in cases where processing likely to result in a high risk to rights and freedoms of individuals
  - Profiling activities
  - Processing of sensitive data on a large scale
  - Systematic monitoring of a publicly accessible area on a large scale
  - Consultation with Supervisory Authority required where Controller cannot mitigate the risk

Consent

Issues with consent

- Consent must be **freely given, specific, informed and unambiguous**
- The **onus is on the data controller** to show that the data subject gave consent
- If consent is given by means of a written declaration, the request must be made in a manner that is clearly distinguishable from other aspects of the document.
- An data subject **has the right to withdraw consent at any time** and must be told of this right by the data controller. **It must be as easy to withdraw consent as it is to give it**

Fair processing notices

Overview

- All information provided must be concise, transparent, easily accessible and given in plain language
- **Data controllers** must provide a significantly wider set of information

Rights of Data Subjects

Disclose/Delete/Freeze/Correct It

- Subject access
- The right to erasure or to be forgotten
- The right to rectification
- The right to restriction of processing.
- The right to object to processing
- Data portability
- Right to object to automated individual decision making (including profiling)
- Claims for loss/distress

Processors

GDPR has direct impact…

- Appointing a representative (if outside the EU);
- Record keeping;
- Breach notification;
- Appointing a DPO (where applicable);
- Sanctions; and
- Transfer of personal data outside of the EU.

Processing Agreements

Significantly enhanced obligations in respect of processing agreements

The controller must appoint the processor in the form of a **binding written agreement** that 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.

This will therefore directly impact agreements between GP and Manager, Advisers, Promoters, Administrator and any other potential service providers

Processing Agreements

The Agreement must provide that the processor will:

- only act on the controller's **documented** instructions (unless legally obliged to do otherwise);
- impose **confidentiality obligations** on all **personnel** who process the relevant data;
- ensure the **security** of the personal data that it processes;
- abide by the rules regarding appointment of **sub-processors** (see above**)** ;
- implement measures to assist the controller in complying with the rights of data subjects;

Processing Agreements

- assist the controller in:
  - complying with its **data security obligations**;
  - complying with its **personal data breach** obligations (both to a supervisory authority and individual data subjects); and
  - completing **Data Protection Impact Assessments** and in **obtaining approvals from Supervisory Authorities** where required;
- at the controller's election, either **return or destroy the personal data** at the end of the relationship (except as required by EU or Member State law); and
- provide the controller with **all information necessary** to demonstrate compliance with the GDPR – in practice, this means complying with an audit/inspection regime.

Processing Agreements

Practical Issues

- Remediation of existing agreements?
- Charging – cost of business v additional fees?
- Who's standard terms?
- Which laws?
- Stop gap v long term fix

Information Security

- The Regulation requires **data controllers and data processors** to take a **risk based approach** to the implementation of **security measures** to protect against loss or unauthorised disclosure of personal data
  - Extends to behaviours of investors/subscribers/NEDS?
  - Personal security issues of individuals?
  - Recitals add new concept
    - **C**onfidentiality
    - **I**ntegrity
    - **A**vailability
    - **R**esilience (new concept)

Notification to the Information Commissioner

- GDPR no longer requires notification
- Data Protection (Jersey) Law 2018 requires notification of all processors and controllers

J.DPA
JERSEY DATA PROTECTION ASSOCIATION

What do I need to consider?

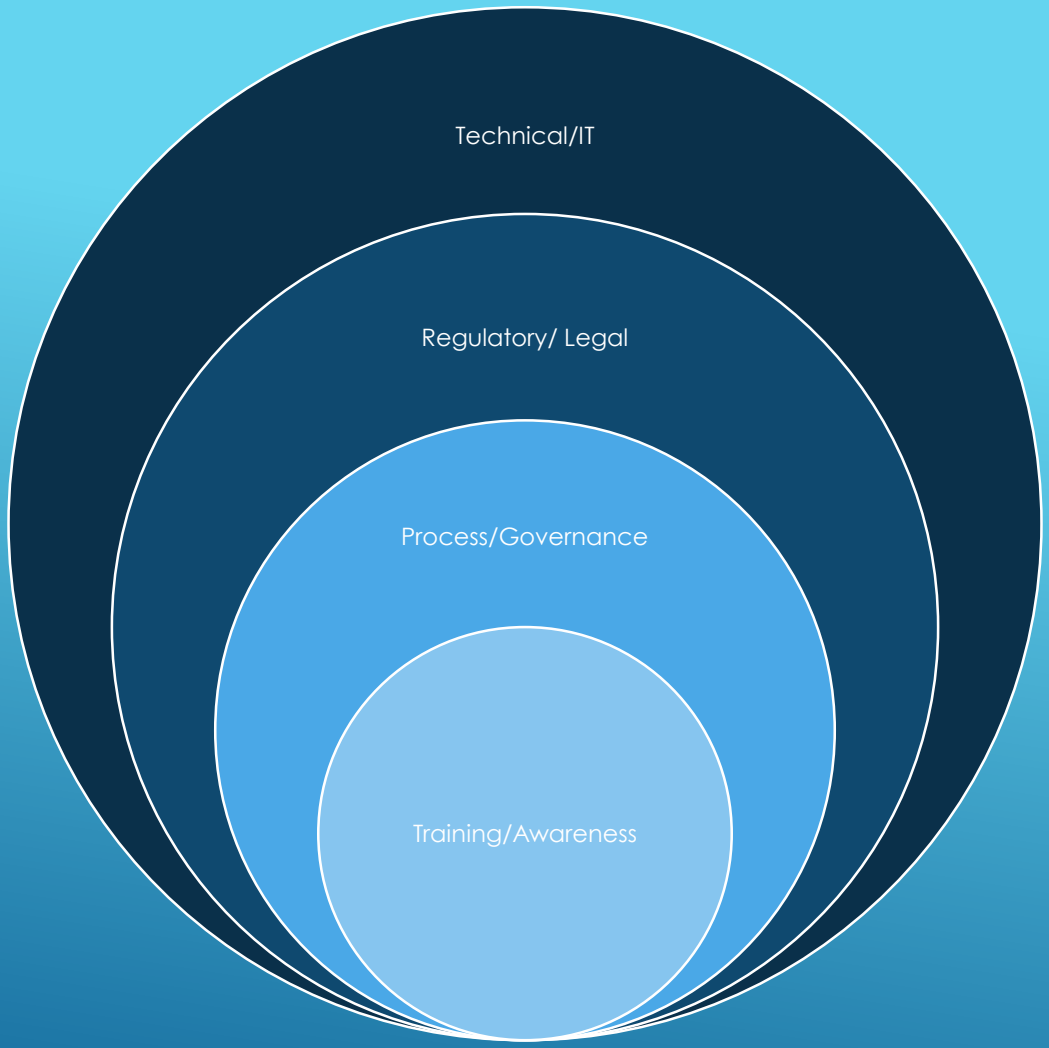
Funds – Areas for Consideration

- Raising awareness of the GDPR with key decision-makers
- Identifying the information held
- Identifying the basis upon which data is processed
- Processing agreements and terms and conditions.
- Reviewing prospectus/subscription agreements
- Communicating privacy information
- Compliance with individuals' rights
- Subject access request procedures
- Checking consent arrangements
- Data breach procedures
- Privacy impact assessments
- Data protection officers
- International arrangements
- Notifications
- Auditing & On-going governance

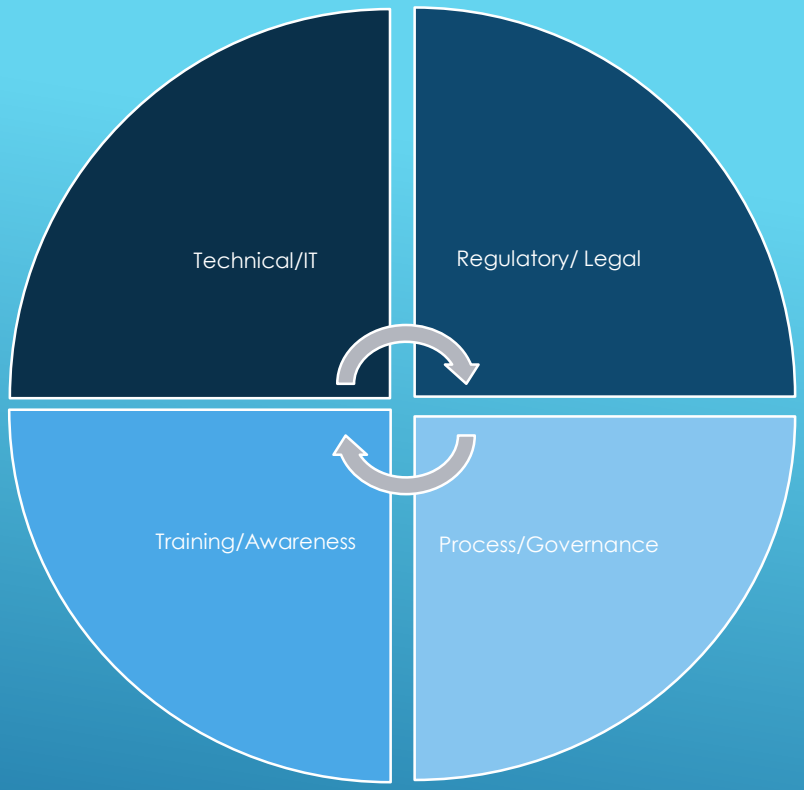
The Clock is ticking…

Full compliance – practicable?

- Remediation Plans – Priorities
  - Governance/compliance approach – who will do what?
  - Consider DPO
  - Data inventory/Mapping – prepopulated?
  - Gap analysis & Action Plan
  - Remediate main agreements
  - Adoption of compliance "suites"
  - Privacy Notices – standardised documents?
  - Documentation of issues & timescales for remediation


Technical/IT
Regulatory/ Legal
Process/Governance
Training/Awareness

- Data protection by design/Default
- Right to be forgotten
- Subject Access
- Data Portability
- Accountability – record keeping
- Security
- Breach management



- Monitoring guidance/developments
- Foreign legal systems
- Data Protection Officer
- Data processing agreements
- Data transfer
- Privacy notices
- Lawfulness of processing
- Data sharing/disclosure
- Subject Access
- Breach management
- Data Protection Impact Assessment

- Data Protection Officer
- Board
- Customers
- Third Parties
- Employees/prospective employees

- Board ownership
- Data Protection Impact Assessment
- HR processes
- Data sharing/disclosure
- Data transfer
- Data Protection Officer
- Data protection by design/Default
- Right to be forgotten
- Subject Access
- Accountability – record keeping

J.DPA
JERSEY DATA PROTECTION ASSOCIATION

Questions?

J.DPA
JERSEY DATA PROTECTION ASSOCIATION

For further information on GDPR / Jersey Data Protection, please also visit:

www.jdpa.org.je – J.DPA Website

https://oicjersey.org/ - Jersey Information Commissioners Website with local guidance
https://ico.org.uk/ - UK Information Commissioner (for UK specific guidance on GDPR)

http://pwc.blogs.com/data_protection/
https://www.careyolsen.com/services/corporate/cybersecurity-and-data-protection