Maintaining Compliance in a World of Constant Change

Mary Frawley

Senior Consultant, BDO Advisory

23rd March 2018

J.DPA
JERSEY DATA PROTECTION ASSOCIATION

J.DPA

JERSEY DATA PROTECTION ASSOCIATION

Maintaining Compliance in a World of Constant Change

Where are we now?

There is a rush to achieve GDPR compliance by 25th May 2018.

Maintaining Compliance in a World of Constant Change

What does 'compliance' mean in the context of GDPR?

- DPIA – *now this is an audit of what your data footprint looks like but going forward this should be a data impact assessment of changes*
- Appointment of DPO *(if relevant)*
- Review and remediation of policies *(i.e. your data rules)*
- Review and remediation of processes *(i.e. your data guidance)*
- Review and remediation of procedures *(i.e. fitting your data guidance to your operations)*
- Bridging the gap between the DPIA findings and the revised policies, processes & procedures
- Implementing the DPIA recommendations

- …….What about the data in the hard copy archives / on e-mails / held by past employees?

J.DPA
JERSEY DATA PROTECTION ASSOCIATION

Maintaining Compliance in a World of Constant Change

Lets consider the root causes of change that **will** affect businesses with respect to data:

Change outside of our control	Changes within our control
• New legalisation *Is GDPR the first of a 'new wave' of data laws?*	• Practice moves away from procedures *Why does this happen?*
• Advances in technology *Block Chain; AI; IoT; Mobile devices*	• Changes in work practices *Remote working; flexible working; outsourcing*
• Exponential growth in data generation *Connectivity growth; Big data; Data science*	• Continued ownership of data M&A activity – is the data you hold yours?

J.DPA
JERSEY DATA PROTECTION ASSOCIATION

Maintaining Compliance in a World of Constant Change

GDPR, Article 25 – part 1 (*equivalent for Jersey is Article 15 parts 1 & 2*; *for Guernsey Article 32*)

"Taking into account the state of the art, 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, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are* ***designed to implement data-protection principles****, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects."*

**replacing personally identifiable material with artificial identifiers*

Maintaining Compliance in a World of Constant Change

GDPR, Article 25 – part 2 (*equivalent for Jersey is Article 15 parts 3 & 4*; *for Guernsey Article 32*)

"The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility.

In particular, such measures shall ensure that ***by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons****."*

J.DPA
JERSEY DATA PROTECTION ASSOCIATION

Maintaining Compliance in a World of Constant Change

GDPR, Article 25 – part 3 (*equivalent for Jersey is Article 15 part 5*; *& for Guernsey Article 32*)

*"An **approved certification mechanism** pursuant to Article 42 **may be used** as an element **to demonstrate compliance** with the requirements set out in paragraphs 1 and 2 of this Article."*

42.1 The Member States, the supervisory authorities, the Board and the Commission shall encourage,…the establishment of data protection certification mechanisms and of data protection seals and marks, for the purpose of demonstrating compliance with this Regulation of processing operations by controllers and processors…..

42.3 The certification shall be voluntary and available via a process that is transparent.

42.7 Certification shall be issued to a controller or processor for a maximum period of three years and may be renewed, under the same conditions, provided that the relevant requirements continue to be met….

42.8 The Board shall collate all certification mechanisms and data protection seals and marks in a register and shall make them publicly available by any appropriate means.

J.DPA
JERSEY DATA PROTECTION ASSOCIATION

Maintaining Compliance in a World of Constant Change

How can we 'solutionalise' data protection sustainability?

- Privacy by design (25.1; Jsy 15.1 & 2)
- Privacy by default (25.2; Jsy 15.3 & 4)

PbD

J.DPA
JERSEY DATA PROTECTION ASSOCIATION

Maintaining Compliance in a World of Constant Change

How can we 'prove' data protection sustainability?

- Use of voluntary PbD certification (25.3; Jsy 15.5)

J.DPA
JERSEY DATA PROTECTION ASSOCIATION

Maintaining Compliance in a World of Constant Change

What does PbD mean?

- Information and Privacy Commissioner of Ontario – 7 principles of PbD

1. Pro-active not reactive / Prevention not remediation (i.e. get it right first time)
2. Privacy as the default setting (i.e. keep closed unless expressly allowed to share)
3. Privacy embedded into the design (i.e. design for privacy & security)
4. Full functionality – full sum, not zero sum (i.e. think of functionality and privacy as equals)
5. End-to-end security – full lifecycle protection (i.e. protection over & at each stage of the data lifecycle)
6. Visibility and transparency – keep it open (i.e. trust but verify)
7. Respect for user privacy – keep it user-centric (i.e. DS and user protection should take lead roles)

Maintaining Compliance in a World of Constant Change

- Consider the 'life-cycle of data'
  - Data collection
    - How many and what type of data collection points do you have versus what you need?
  - Data maintenance & storage
    - Is 100% of your data classified in line with your Information Classification Policy?
    - Is your data storage fit for purpose and secured by appropriate access controls?
    - Are you implementing your Data Retention Policy?
  - Data destruction
    - Is your Data Destruction Policy *(if you have one)* reflective of your actual practices?

Maintaining Compliance in a World of Constant Change

- PbD – what happens when it goes wrong?
  - Facebook – Beacon
    - An advertising system that fed users' activity detail to their FB news feed when they engaged in activity on 'partner' third party users sites.
  - Google - Buzz
    - A social network using Gmail users' formerly private contact lists.
  - Fitbit.com – S E X
    - Users activity was monitored and made public – one of the 800 activities tracked was sex

Maintaining Compliance in a World of Constant Change

- PbD – practical measures to ensure we get it right
  - Involve a ‘data champion’ during project early stages (consider as project team member / role)
  - Aim for data minimisation as standard
  - Aim for controlled data entry (reduce number and types of data collection points to suit needs)
  - Build pseudonymisation, encryption & meta-data in at START of data collection
  - Be transparent in your intended use of data and ADHERE to this

Maintaining Compliance in a World of Constant Change

- PbD – practical measures cont….
  - Classify 100% of your data in line with your Information Classification Policy & AUDIT this
  - Ensure that your data storage is fit for purpose
  - Ensure that your data storage is appropriately secured
  - Create and improve data security features on an ongoing basis
  - For security – consider least privilege model (grant access only to those that need access)

Maintaining Compliance in a World of Constant Change

- PbD – practical measures cont….
  - Employ strict data testing rules (only anonymised data to be used in test system environments)
  - Allow data subjects (DS) access to records concerning them
  - Ensure that data is archived in line with your Information Archiving Policy & AUDIT this
  - Ensure that data is destroyed in line with your Data Destruction Policy & AUDIT this

Questions?