GDPR: The New PPI?

EDDIE LAWSON – Risk and Compliance Professional

E.LAWSON ADVISORY

GIROUX

ENHANCING BUSINESS DECISIONS

Agenda

- Overview
- The new PPI?
- Who does it apply to?
- Why do I care?
- Data protection principles
- What is personal data?
- Consent
- Rights and obligations
- E-Privacy
- Setting up a compliance program
- The Insurance market

Overview

- GDPR will replace UK Data Protection Act 1998
- 25th May 2018
- GDPR designed to enhance the protection of individuals
- Bringing data protection laws into the 21st century

- Equifax – millions of social security numbers
- AMP – 25,000 staff records
- Paradise Papers

The new PPI?

- Basis for general public to make a claim
- Scope for damage and loss of reputation
- Possible traps in the form of individual rights – right to access, rectification, erasure and portability
- Have to respond within a reasonable time
- Failure to comply can result in fines

- Or…compliance can be a basis for creating a great reputation

Who does it apply to?

- Applies to “controllers” and “processors”
  - Controllers say HOW and WHY personal data is processed
  - Processors acts on controller’s behalf
- To organisations operating within the EU
- To organisations outside the EU that offer goods and services to individuals in the EU

Why do I care?

- 47% of 900 surveyed organisations believe they won't meet compliance guidelines
- Fines and penalties for breach of up to £17.9m or 4% of global annual turnover PER INCIDENT
- Under the GDPR your customers can request for their personal data to be transferred from you to a COMPETITOR.
- 72 hours to report breach.

Data protection principles

1. FAIR, LAWFUL and TRANSPARENT
2. Processing must have PURPOSE

Data must be:

- ADEQUATE RELEVANT AND LIMITED TO WHAT IS NECESSARY
- KEPT UP TO DATE
- Only held for AS LONG AS NECESSARY
- SECURELY PROTECTED

What is personal data?

- Anything that enables you to identify a person, whether alone or with other data you hold
- Now includes wider elements such as an IP address, email address, biometric data
- Does not matter if automated or manual filing system

Consent and lawful processing

- Processing is lawful if:
  - Consent – special rules for children's consent
  - Necessary for performance of a contract or to enter into a contract
  - Necessary for compliance with a legal obligation
  - Protection of vital interests of data subject or a third party
  - Necessary for public interest or official authority

- Special requirements for transfer of data outside the EU and sensitive data

Rights of individuals

- Informed about processing
- Access of information
- Rectification
- Erasure
- Restrict Processing
- Data Portability
- Object to processing
- Automated decision making

Obligations under GDPR

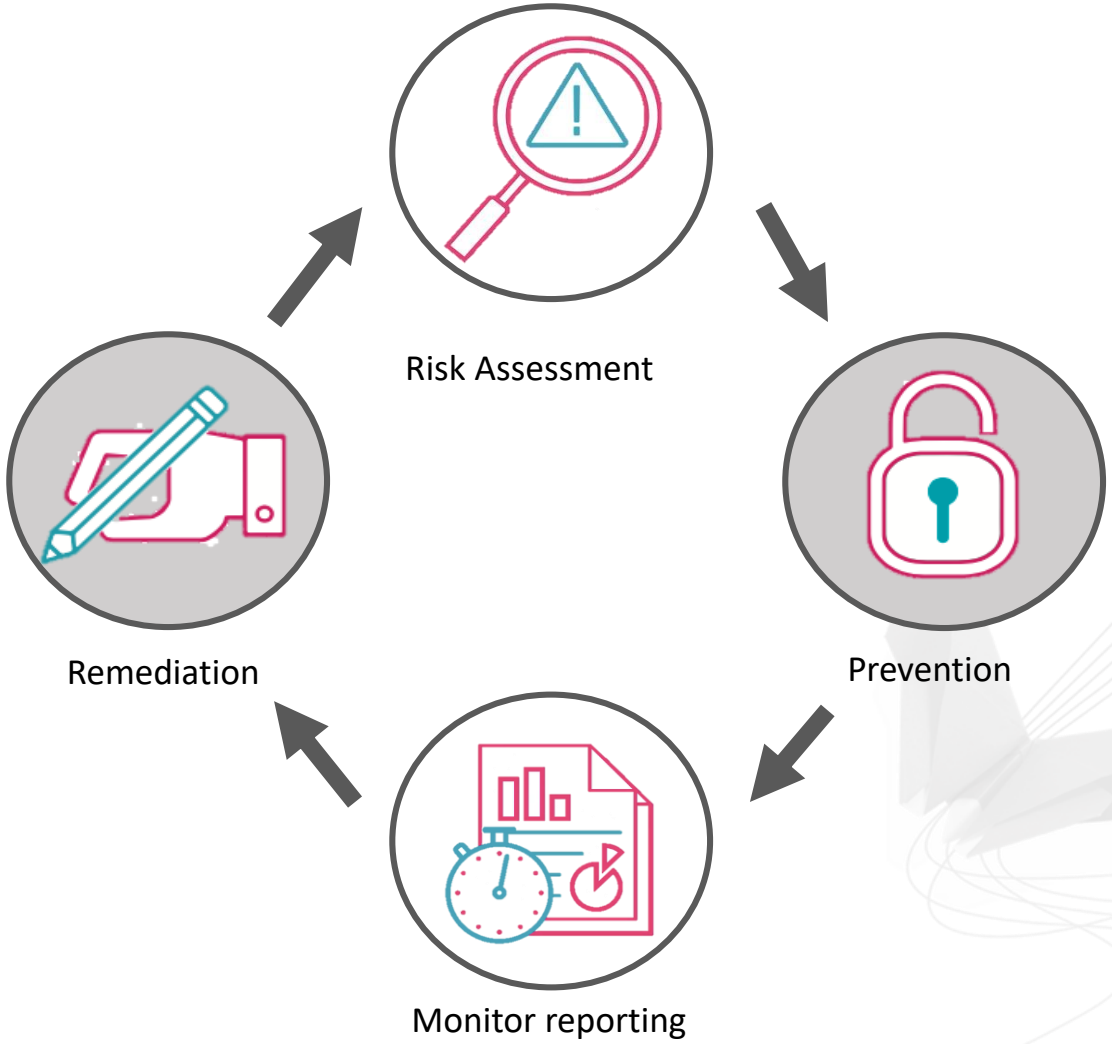
- Transparency
- Accountability and governance
- Full documentation of data processing activities
- Maybe appoint a DPO
- Data protection by design and default
- Breach notification

E-Privacy

- Proposals to operate alongside GDPR
- Regulates the way businesses communicate with individuals
- Cookies, direct marketing, email communications, cold calls
- Penalties will be of similar size to some GDPR penalties

- WATCH THIS SPACE…

Designing a compliance programme



Compliance programme key steps

- Senior management buy in
- Consider making privacy an essential strategic element!
- Data flow mapping
- Audit existing state of compliance
- Identify gaps
- Make a plan to improve compliance

- Not a ‘one time’ compliance project but must become a **‘living document’**

Special considerations for the insurance market

- Customer concerns about use of data by insurance companies
  - E.g. Admiral's plan to use Facebook data to set car insurance prices
- Possible use of social media to find evidence of fraudulent claims
- Could telematics assist with pricing policies?
- Data analytics to produce pinpoint marketing

Special considerations for the insurance market

- Review systems to make sure they incorporate “privacy by design”
- Review communications and consents especially for sensitive personal data (e.g. health and travel insurance)
  - Lloyds Market Association waiting for guidance from ICO on this
- Look into processes for data portability (e.g. from one insurer to another)
- More requirements around automated processing (and profiling) – need to explain, get informed consent. Customers can object.
- Cyber insurance an opportunity?

Conclusion

- Do not ignore GDPR
- Compliance programme needs to be put in place
- Flow mapping process to be documented ASAP

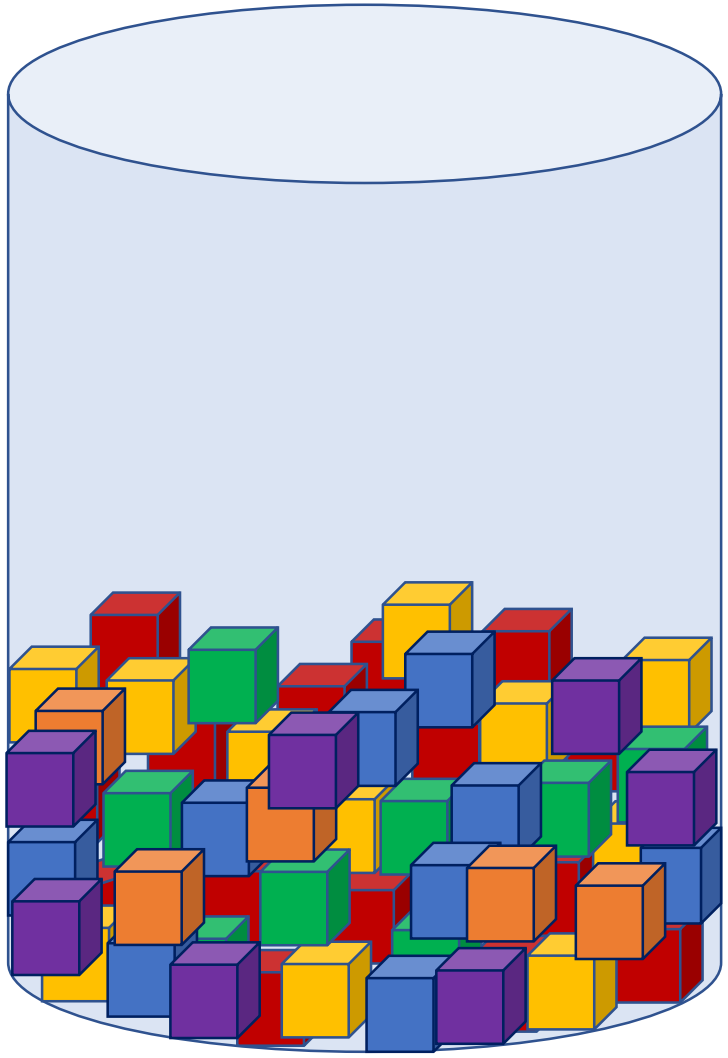

GDPR: The New PPI?
E.LAWSON ADVISORY
GIROUX
ENHANCING BUSINESS DECISIONS

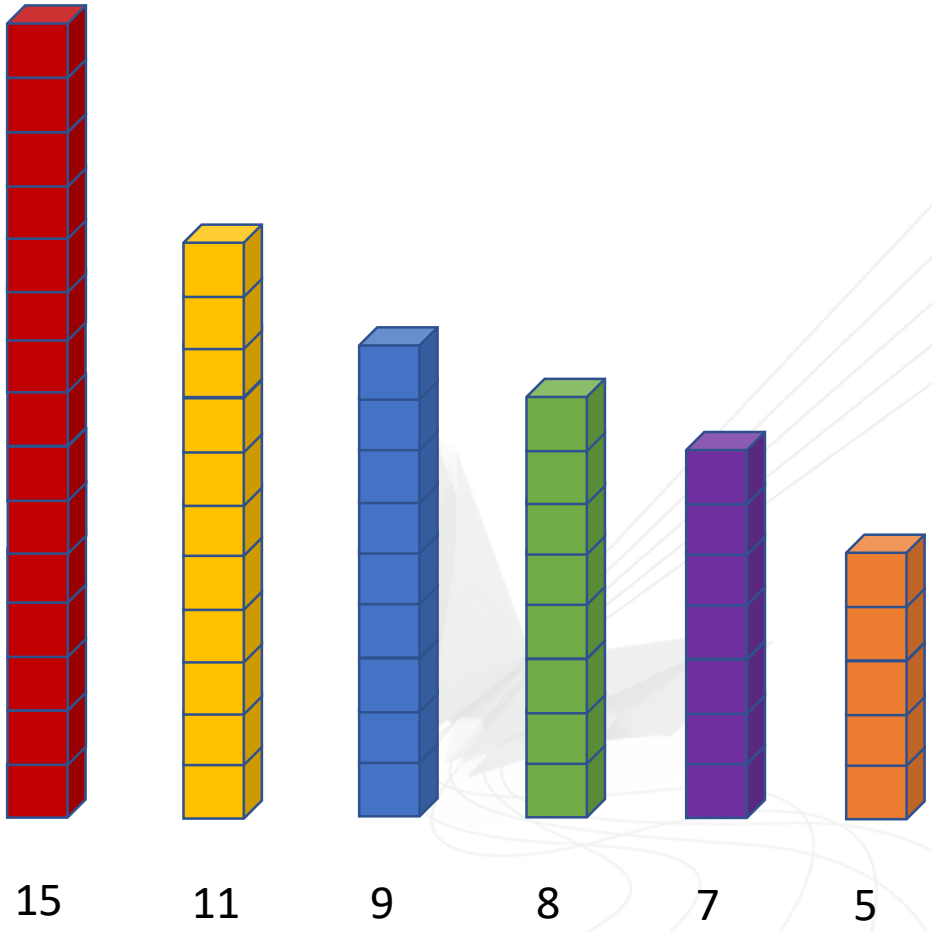

Preparing for GDPR with
GIROUX.
GIROUX
ENHANCING BUSINESS DECISIONS

Who are we?

"I founded Giroux with the intent of engineering data warehousing and analytics solutions that are more affordable and more efficient. I built the company out of frustration of failed analytics projects…Over ten years we have developed a team of experts capable of providing an end-to-end data analytics solution whose agility, flexibility and scalability are second to none. "

What do we do?





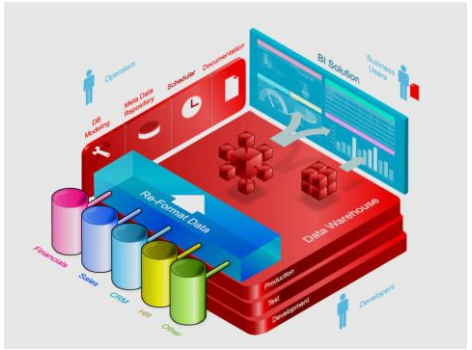
How can we help you comply?

Easy to eradicate data

Governed Information

Compliant to individual rights

Complete control



Monitoring

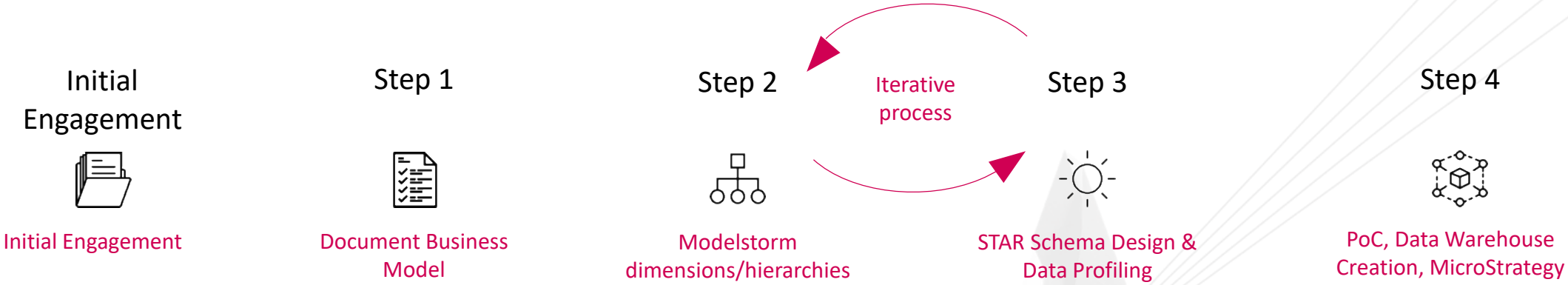
Documentation

Security

Compliant

How to get started?

6-8 Week Consulting Set-up To Get You Up And Running:



CONTACT DETAILS

Eddie Lawson Advisory

Eddie Lawson

Email: eddie@eladvisory.co.uk

M: +44 7977 662708

LinkedIn: eddie-lawson-0517454

GIROUX

Laura Knight

Email: laura@giroux.co.uk

M: +44 7715 343732

www.giroux.co.uk