GDPR - building the shield and making it stick

Jenny Etherton CIPP/E
PwC UK GDPR Implementation Programme Director
26 April 2018

Think privacy

GDPR is coming:
How would you like *your* personal data to be treated?

One month to go….

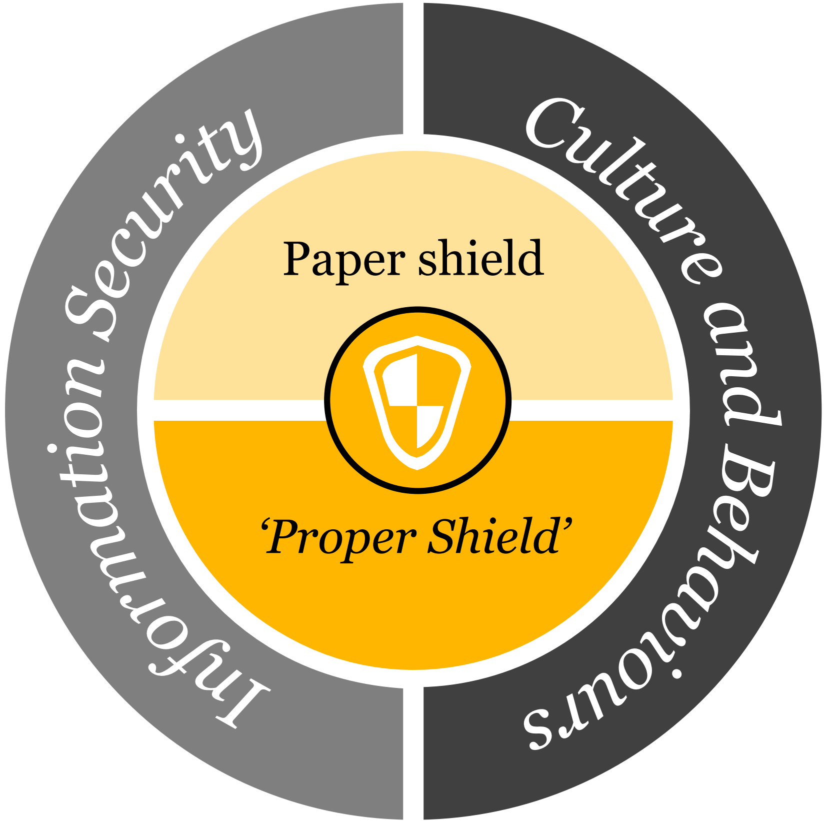
Elizabeth Denham's keynote speech at the IAPP Europe Data Protection Intensive 2018, London, 18 April 2018

"25 May will merely mark the end of the beginning of a very long journey for the data protection community."

"I have no intention of changing our proportionate and pragmatic approach after 25 May. My aim is to prevent harm, and to place support and compliance at the heart of our regulatory action. Voluntary compliance is the preferred route.

But we will back this up by tough action where necessary; hefty fines can and will be levied on those organisations that persistently, deliberately or negligently flout the law."

GDPR - building the shield…



Risk of a breach really arises from two main sources of failure:

- Insufficient / ineffective information security
- Vulnerabilities in how your people handle personal data

- The highest priority at this stage is to make sure that the personal data you do hold is secure and protected
- Once this is in place, then you can address other issues such as
  - creating your record of processing
  - updating your policies
  - lawful basis for holding it
  - minimising data so you only have what you need

A full compliance implementation programme covers this:

1. Governance	2. Risk / Compliance	3. Data Management	4. Legal	5. Change Management
1.1 Data Protection Governance	2.1 General Risk Assessment	3.1 Record of Processing / Data Mapping	4.1 Client / customer contracts	5.1 Change Management
1.2 GDPR Programme Governance	2.2 Policies	3.2 DP Impact Assessments	4.2 Data transfers	5.2 Communications
1.3 Monitoring of Compliance	2.3 Privacy Notices	3.3 People (Internal) - employees / applicants / contractors / alumni	4.3 3rd parties / supplier contracts	5.3 Training
1.4 Accountability: Evidencing GDPR compliance	2.4 Incident Response	3.4 People (External) - customers / clients		5.4 Awareness
	2.5 Information and System Security	3.5 Marketing		
		3.6 Data Subject Rights		
		3.7 Info Management, Disposal & Retention		
		3.8 Technical & Organisational Measures		

What are the key themes on organisational readiness

Vast difference in readiness across sectors

Lots of activity, it needs to converge to reduce risk

Many programmes have a very narrow focus

Insufficient investment, especially in technology

What are the operational crunch points for most organisations?

Low / Medium intensity	High intensity (time / resource) activities
Policies	Record of processing
Privacy notices	Third party / supplier due diligence
Design of incident response procedures	Review of systems
Design of Data Subject Rights processes	DP Impact Assessments
Accountability framework	Information / Cyber Security
	Market consent re-papering
	Customer contract amendments / renegotiation
	Change management, communications, training, awareness

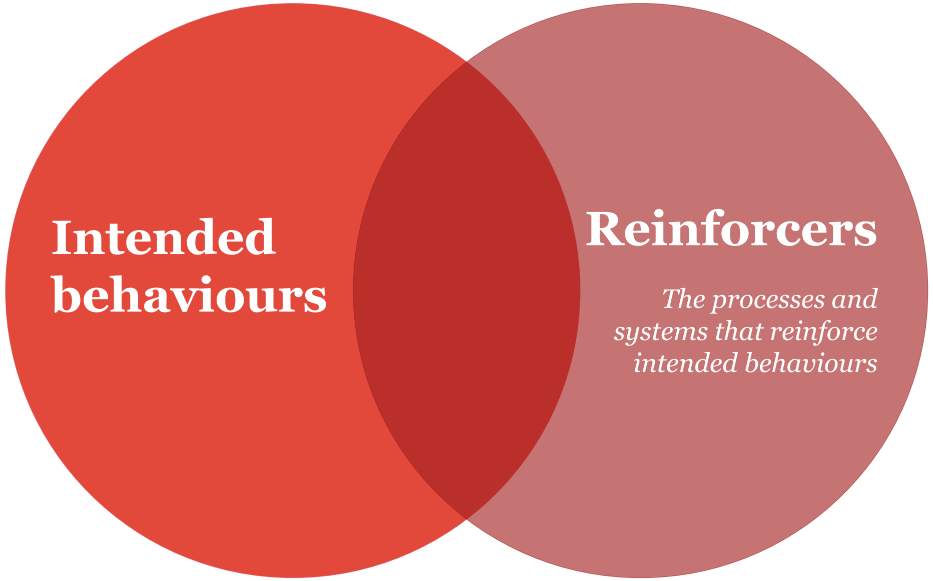
How do you change the behaviours of your people?

Make it easy for people to know what they should be doing

- Training
- Awareness raising
- Tone from the top

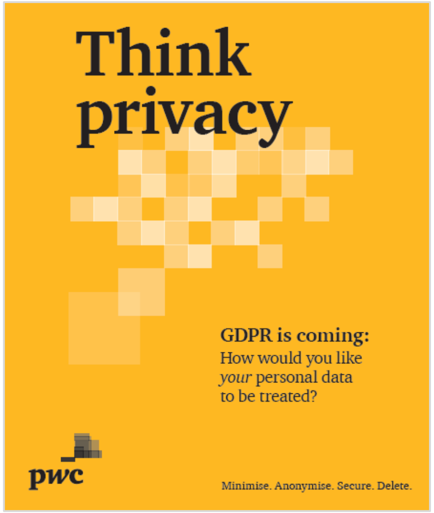
E.g.

- **Minimise**
- **Anonymise**
- **Secure**
- **Delete**


Intended behaviours
Reinforcers
The processes and systems that reinforce intended behaviours

Process and Technology

- Embed DP by design into new products, projects, applications – at the business case approval stage
- Use available technologies such as Data Leakage Prevention, discovery tools for unstructured data

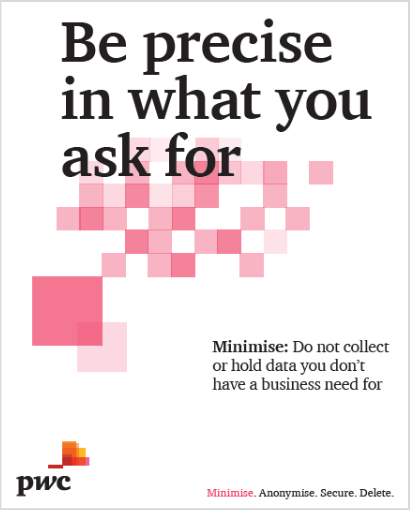


Think privacy

GDPR is coming:
How would you like *your* personal data to be treated?

pwc

Minimise. Anonymise. Secure. Delete.

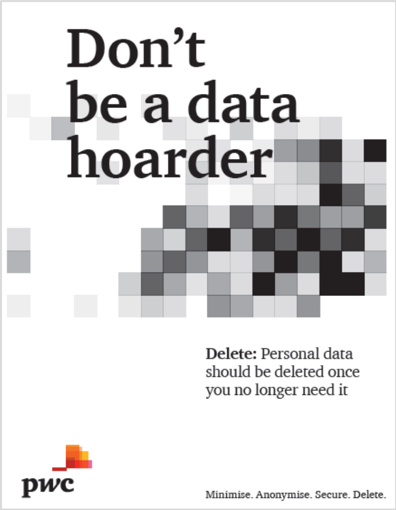


Be precise in what you ask for

Minimise: Do not collect or hold data you don't have a business need for

pwc

Minimise. Anonymise. Secure. Delete.



Don't be a data hoarder

Delete: Personal data should be deleted once you no longer need it

pwc

Minimise. Anonymise. Secure. Delete.