DPAS

FROM BLOCKER…
…TO BUILDER!

Ralph T O'Brien
Principal
REINBO Consulting Ltd

WELCOME!

Ralph T O'Brien

Trainer & Consultant

Principal REINBO Consulting Ltd

Associate professor Maastricht University

Associate Trainer and Fellow IAPP

Putting the personal back into the data

Putting the human at the centre of IT

Possessing 25 years of experience, new ways of thinking

Promoting Innovation through good Data Management

FIP, CIPP/E, CIPM, CIPP/US, MBCS, CiISMP, CDPSE, Bsi Lead Assessor, CDPO Maastricht University, etc. etc. etc.

Its Friday about 1300, you come back from lunch…

- There's someone at your desk..

- They ask you if you are the Data Protection expert

- You say "*yes*"

- They tell you their team has been working…

…on a new cloud implementation
…that takes personal data from a number of systems…
…uses quantities of special category data…
…shares it with a number of organisations…
…uses a number of different suppliers…
…allows access from anywhere globally.

You say…
"*Happy to help, when are the meetings*"

THEY SAY….

A — Every Thursday, 0900

B — Whenever you can make it, we'll work around you

C — Oh, that's all done. It goes live at 1700!

HOW FAMILIAR IS THIS SCENARIO?

…& WHAT CAN WE DO ABOUT IT?

…OR ARE WE OUR OWN WORST ENEMY?

HOW DOES THE ORGANISATION SEE US?

MAYBE WE ARE THE ONES WHO NEED TO CHANGE?

ORGANISATIONAL MATURITY

LOW vs HIGH

|	
DP team engaged Late	**DP team engaged Early**
Seen as tick box exercise	Seen as a design concept
Seen as External threat	Seen as internal driver
Seen as legal compliance	Seen as competitive advantage
Privacy VS Functionality	Data Protection AS Functionality
Business at the Centre	**Human at the Centre**
DP as a cost/problem	DP as a benefit/advantage

UK GDPR Article 24

1. *Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary.*

1. *Where proportionate in relation to processing activities, the measures referred to in paragraph 1 shall include the implementation of appropriate data protection policies by the controller.*

DEMONSTRATE COMPLIANCE –
do your homework!

STAKEHOLDER REQUIREMENTS & EXPECTATIONS

PLAN

ACT

DO

CHECK

MANAGED DELIVERY
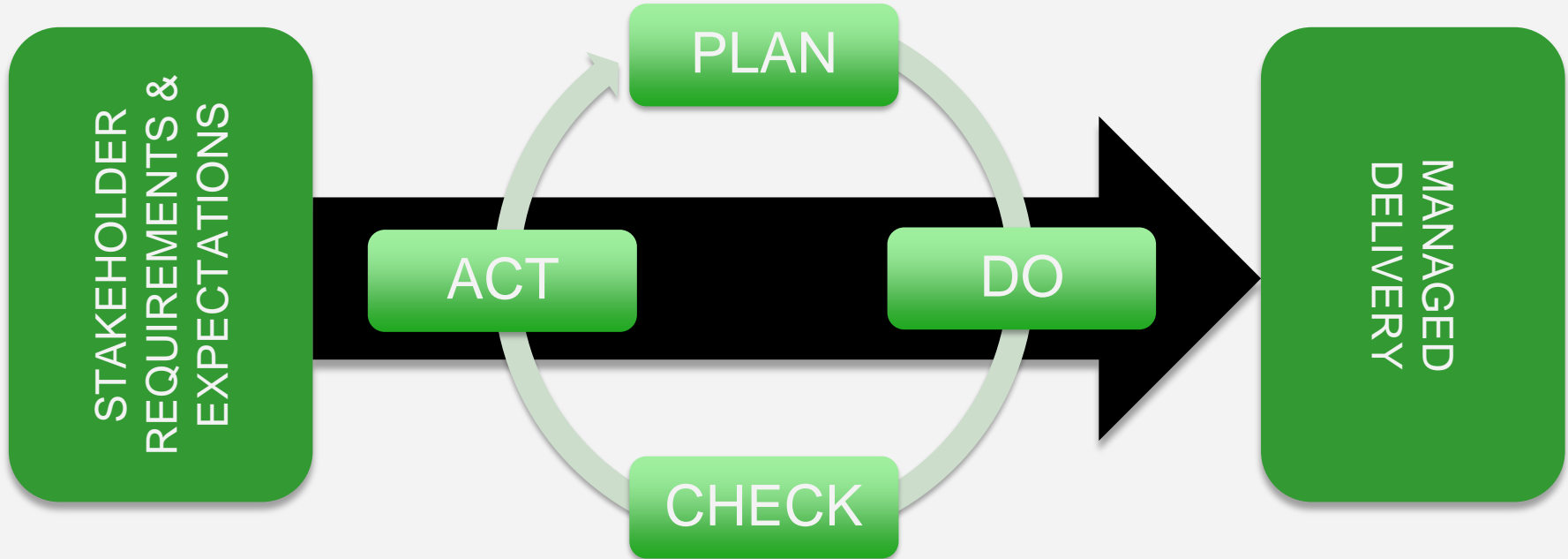
UK GDPR Article 25

1. *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.*

1. *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.*

Privacy by Design principles

**Ann Cavoukian
– 2006 Privacy commissioner of Ontario**

- *Proactive* not Reactive; *Preventative* not Remedial
- Privacy as the *Default Setting*
- Privacy *Embedded* into Design
- Full Functionality – *Positive-Sum*, not Zero-Sum
- End-to-End Security – *Full Lifecycle Protection*
- *Visibility* and *Transparency* – Keep it *Open*
- *Respect* for User Privacy – Keep it *User-Centric*

Risks to individuals

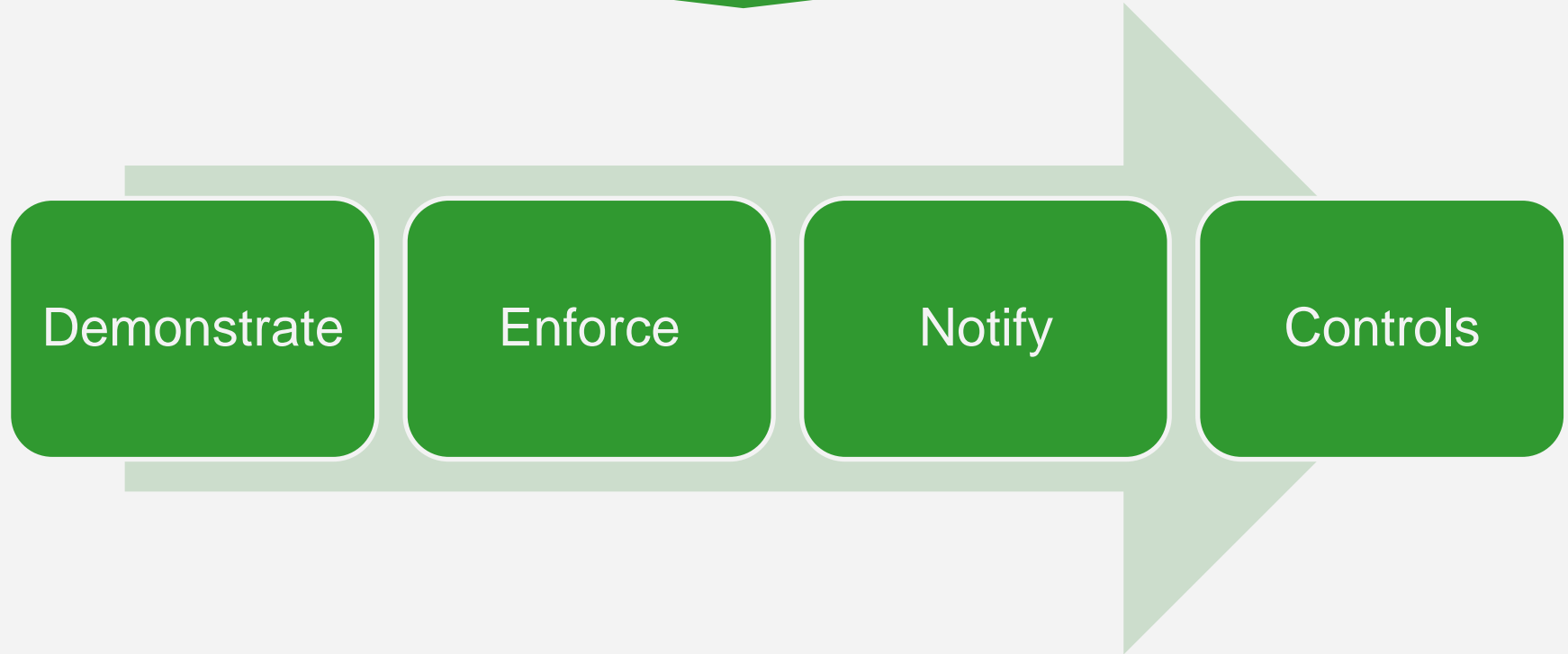|				
Interrogation	Surveillance	Insecurity	Identification	Data aggregation
Secondary uses	Exclusion/Discrimination	Disclosure/Doxing	Data Distortion	Breach of Confidentiality
Blackmail/Extortion/ Social Engineering	Identity Theft / Appropriation	Interference	Behavioural Advertising	Bullying

Credit: Prof. Daniel Solove; Taxonomy of Harms

PETS: Privacy Enhancing techniques

De-identification	Pseudonymisation	Anonymisation	Data Minimisation	Data classification
Data Inventory	Contracts and Agreements	Architecting privacy in IT	Encryption	Hashing
Tokenisation	Incident Response	Identity and Access Management	Authentication	Data Abstraction
Policy	Directives/	Administrative	Detective Controls (Logs / CCTV / Audit)	Masking / Obfuscation / Dummy data

Demonstrate | Enforce | Notify | Controls

Credit: Jason R Cronk; Privacy Engineering

Minimise

Hide

Aggregate

Separate

Credit: Jason R Cronk; Privacy Engineering

- **Scenario:**
- Rent a shed is an online company for people who wish to rent out storage space they have vacant.
- The company uses a cloud hoster, and matches people who need storage with storage providers through a mobile app and web site.
- Recently they have been accused of their platform allowing racial discrimination.

- **Task:**
- Design safeguards in to the platform to stop this racial discrimination.

IN PRACTICE
USING OUR STRATEGIES

Minimise	Hide	Aggregate	Separate
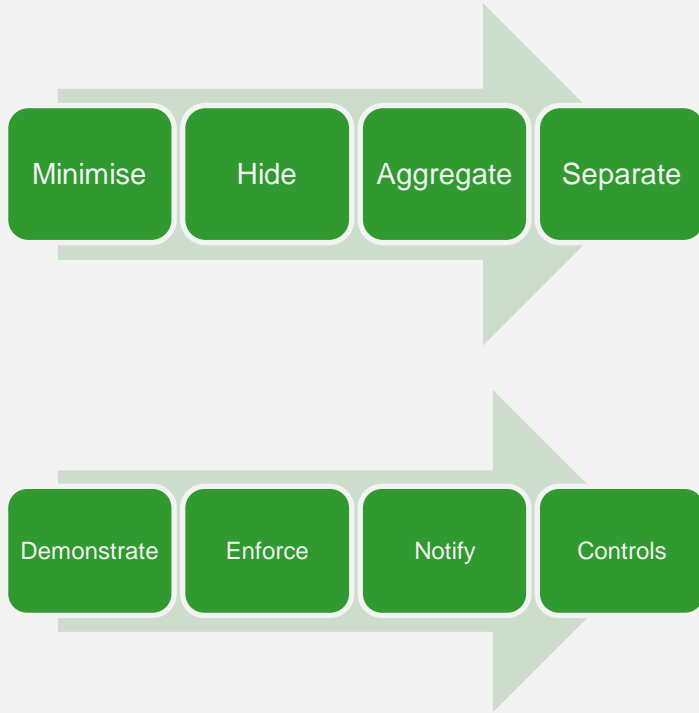
Minimise: Don't collect the data!
Hide: Don't show to other party
Aggregate: Pseudonymise or Categorise
Separate: Access Control

Demonstrate	Enforce	Notify	Controls

Demonstrate: Badges and Consultation
Enforce: Audit and remove non-compliant
Notify: Policy, T&C, Warnings
Controls: User preference dashboards

BING THE BUILDER

Don't be the NO
Be the Yes!

1
TIP

Do add value
and benefit and
functionality

3
TIP

Rely on skills,
not knowledge

5
TIP

2
TIP

Don't be a
black mailer,
be a designer

4
TIP

Get in early
and be positive

THANK YOU!

Does anyone have any questions?

robrien@reinboconsulting.com
+44(0)7920 107959
www.reinboconsulting.com

DPAS