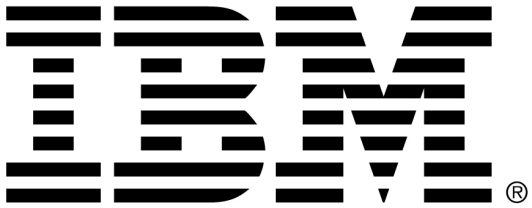

infosecurity
EUROPE
Security Workshops



Managing Privacy in a Changing Environment.

An Overview of the Compliance issues of Managing Privacy in a Data Rich World

Simon Rogers,
Security and Privacy

30/04/14

Background

A Data Centric View of the World – the case for change

[Personal] Data is the currency of the digital market. Like any currency it has to be stable and trustworthy.

Viviane Reding, Vice-President of the European Commission Responsible for Justice, Fundamental Rights and Citizenship.

Date: 25/01/2012

Data has Real World Value.

- According to the Boston Consulting Group, the digital economy accounts for 8.3% of UK's GDP, a higher share than any other EU country. The Group estimates that the benefits to the average UK consumer from the internet is £2,300 per annum.

- Commission's proposals would cost the UK anywhere between £100 million and £360 million per annum

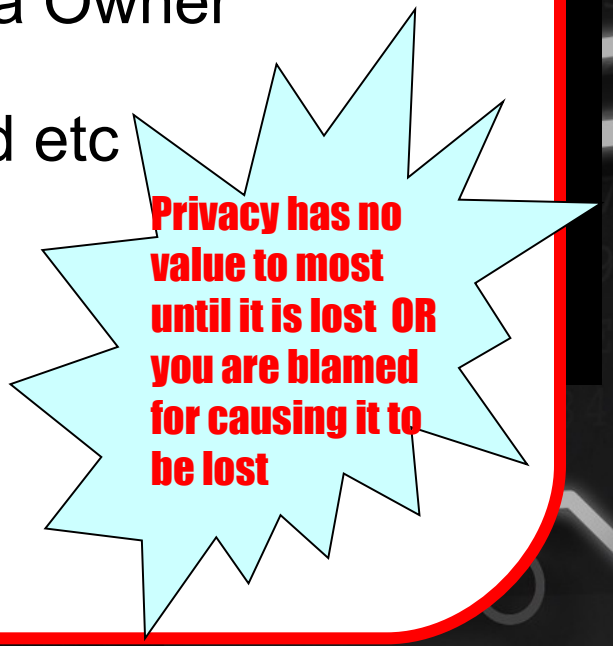
Figures quoted by the then Lord Mcnally, former Minister of State at the Ministry of Justice, March 2013

External Factors Driving Change

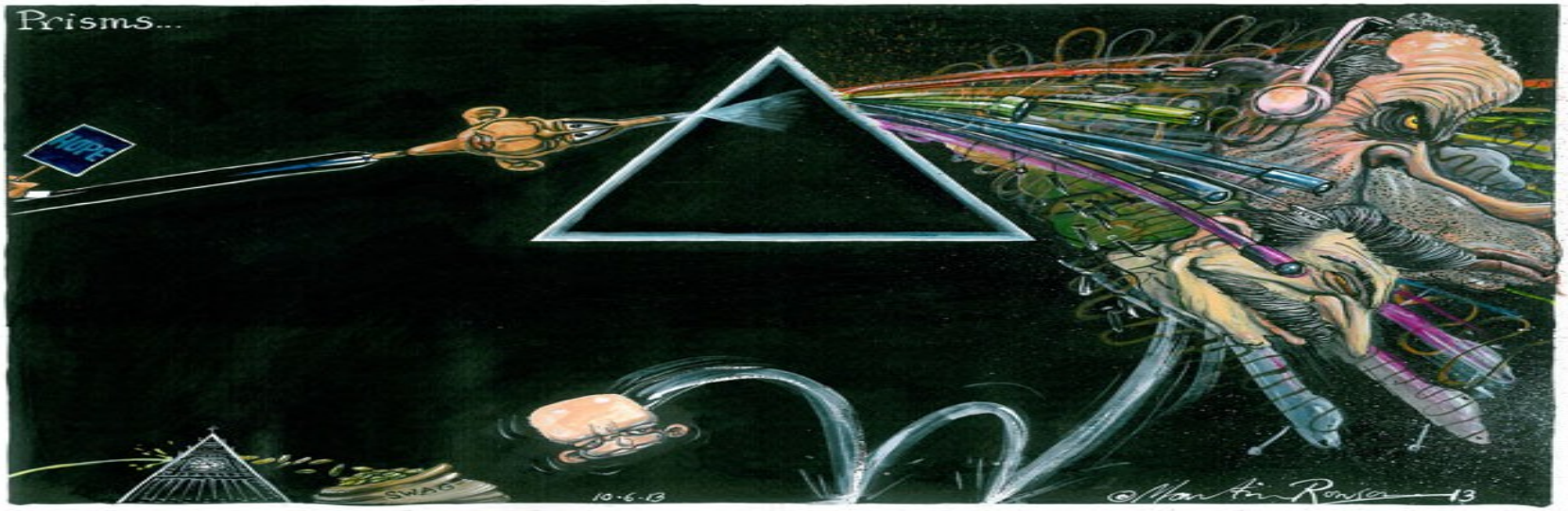
- **Technology**
  - Internet of Things
  - Big Data (Volume, Velocity, Variety and Veracity)
    - Data (Personal Data) Rich Society
    - Penetration into society
    - Volumes of collection
    - Immediacy of processing
    - Data as commodity
    - Blurring of work and private - BYOD

External Factors Driving Change 2

- **Globalisation of business and lengthening of Supplier Chain**
  - More data flows across borders
  - Lengthened supplier lines means Data Owner (Controller) loses sight of their data
  - ‘New’ less transparent services, Cloud etc
- **Access of Data – ethical concerns**
  - Recent allegations – NSA etc
  - Data mining/ profiling etc
  - Criminal activity



What Happens When It Goes Wrong



The Guardian

9 June 2013

Both Private and Public Sector

How Target knows when its shoppers are pregnant - and figured out a teen was before her father did…

By Nina Golgowski
UPDATED: 13:19, 18 February 2012

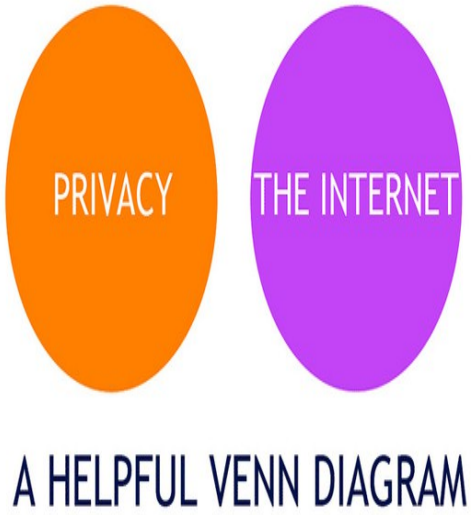
Are we redefining privacy …

- the real debate we should be having … is about what privacy in a cyber-connected world can realistically mean given the volumes of data we hand over to the private sector in return for our everyday convenience, and the continued need for warranted access for security and law enforcement".

  Sir David Omand, former head of GCHQ

- "Google spins an invisible web of our personal data."said Jacob Kohnstamm,

DPA (Dutch Data Protection Authority) chairman in a statement.



The result of CHANGE and the catalyst for CHANGE

- **Compliance Change**
  - European Regulation (wide ranging change)
    - Designed to modernise the Directive
    - Allow freer flow of data
    - Harmonise processes
    - Prevent back doors

20 Years is a long time …

- **Google 1996**
- **9/11 2001**
- **Facebook 2004**
- **iPhone 2008**
- **Snowden 2012**

Data Privacy Overview – The Current Compliance Picture

The Law We Operate Under … Key EU Directive etc.

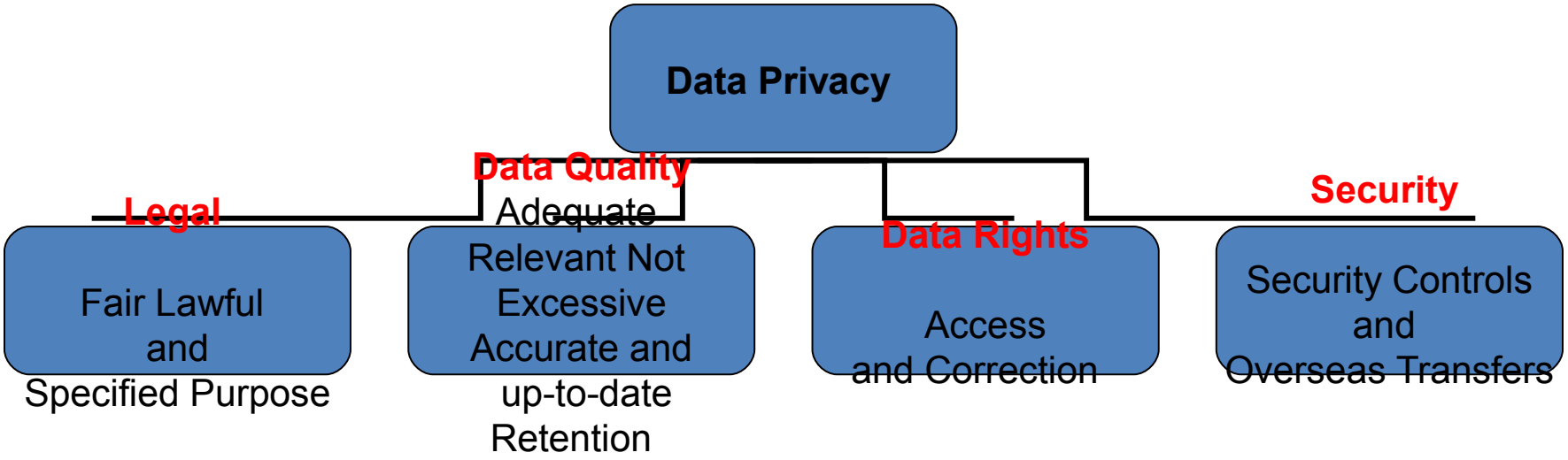
Directive 95/46/EC of the European Parliament and the Council of 24 October 1995

Human Rights Act (article 8)

UK Data Protection Act 1998 (Other EEA Countries equivalent)

The Privacy and Electronic Communications Regulations

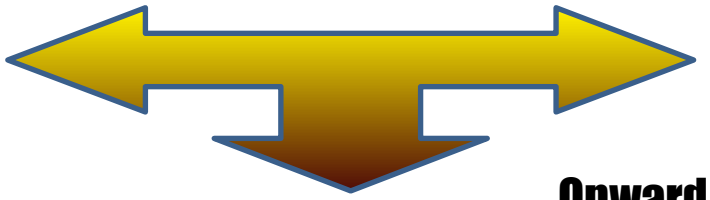
Fundamentals of Data Privacy



Data Protection Summary

- Relates to Personal Data – (throughout its lifecycle)

Collection **Destruction**

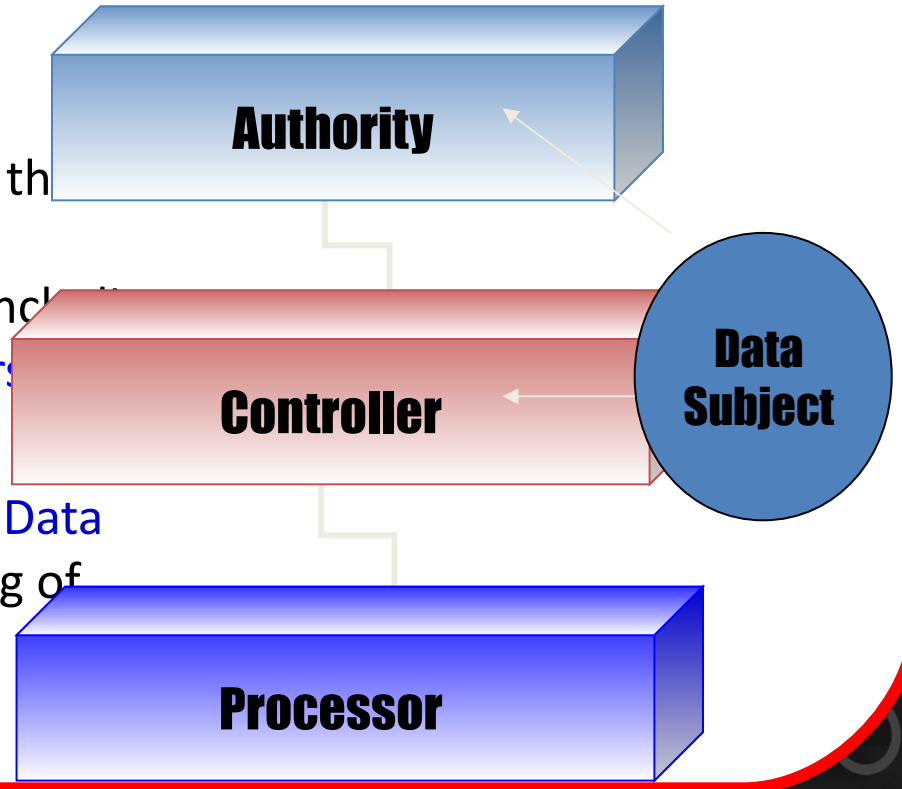


Onward Disclosure

- Provides Minimum Enforceable Standards
- Consequences of Failure
  - Fines (£500,000) and Criminal Penalties
  - Damage to Reputation

Chain of Responsibility and Rights

- Affects All data processed in the EEA
  - Places **Responsibilities** regarding th
    Processing of Personal Data by
    organisations (Data Controllers) incl
    their outsourcers (Data Processors
  - Gives **Rights** to living individuals (Data Subjects) regarding the processing of their data.



Examining the Scope of Change

Europe Recognises the Need for Change

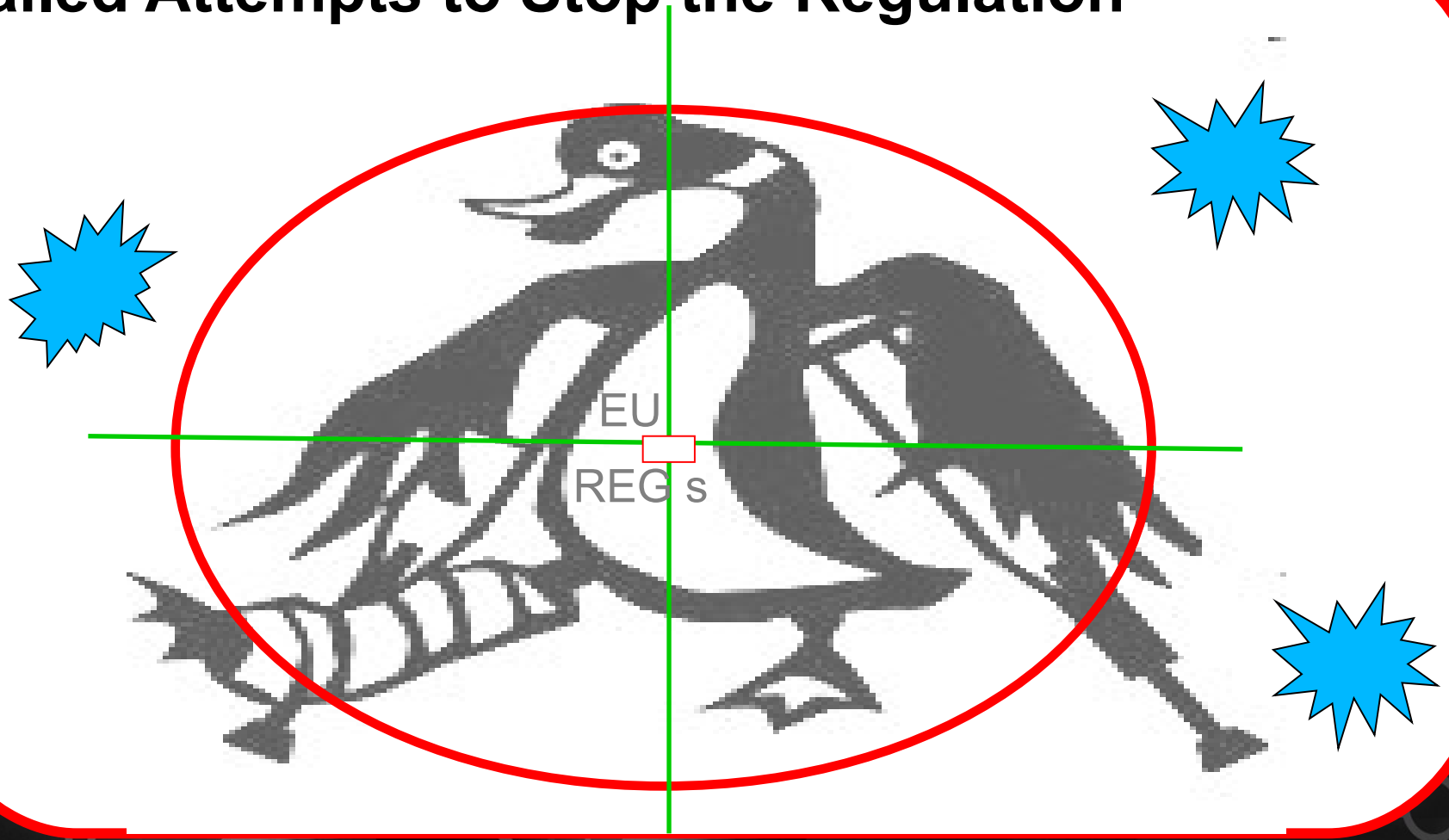
All those active on the European market should be held to essentially the same standards…in order to ensure effective and consistent protection of all European citizens across the EU.

Peter Hustinx
Data Protection Supervisor
21/06/2013

Justice Commissioner Viviane Reding said …"One continent, one law; that is what I call opening the market,"

BBC
6 June 2013

Failed Attempts to Stop the Regulation



The Legacy - Low Awareness in the UK

Half UK IT decision makers unaware of coming EU data laws, study shows

Computer Weekly
Warwick Ashford Thursday 24 April 2014 13:04

Recent research commissioned by Trend Micro Research

850 Candidates

Multiple European Countries

UK did not score as well as others…

Overview

- Move from Directive to Regulation
- Less Wiggle Room and Less Room to Hide
- Document and Demonstrate
- Tighter Control (sanctions)
- Increased Scope
- More Prescriptive
- SME Exemptions

INCREASED CORPORATE ACCOUNTABILITY

=

GREATER RESPONSIBILITIES: RIGHTS

New focus

Privacy by Design and Default

Transparency – Icons on websites more information to Data Subject

Data minimisation –storage and processing

Pseudonymisation and Anonymisation

Breach reporting

No registration

Consent and Legitimate Interests

European Data Protection Board

Lead Authority

No Charge for Subject Access

Right to Erasure (AKA Right to be Forgotten)

Data Portability

Monitoring and Profiling

Greater Scope – Data and Territorial

Not Just an EEA issue

This Regulation applies to the processing of personal data of data subjects in the Union by a controller ***or processor*** *not established in the Union, where the processing activities are related to:*

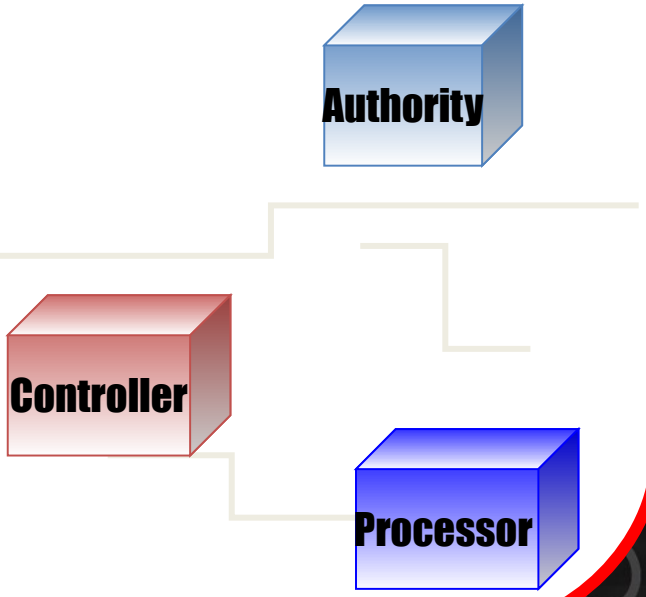
*(a) the offering of goods or services****, irrespective of whether a payment of the data subject is required,*** *to such data subjects in the Union;*
or
(b) the monitoring of ***such data subjects.***

More Clarity on Data

Identifiers provided by devices, applications or other online tools will be regarded as personal data, unless they do not relate to an identified or identifiable person.

Greater Scope – Data Processor

- Statutory underpinning and requirements to assist the Controller
- Notify the Controller of Breach without undue delay etc…
- May be deemed Controller - if a processor processes personal data other than as instructed by the controller or becomes the determining party in relation to the purposes and means of data processing,



Sanctions

Relate to anyone
Processor and Controller

Warning only when unintentional and 1st offence

Audits

Increased Fine 100,000,000 (100 Million) euro or 5%

Prevent Processing

Based on :

Intentional or negligent
Nature, impact (both financial and non financial) and duration
Financial gain from the breach (intended or gained)
Previous Breaches and or repetitive breaches
Degree of cooperation
Degree of action to mitigate damage
Technical and organisational measures implemented in line with the Act

Notification

- Data Breach Notification within **72 hours** and without undue delay

A personal data breach may, if not addressed in an adequate and timely manner, result in substantial economic loss and social harm, including identity fraud, to the individual concerned – so not minor issues

- **Can be mitigated by encryption**

Embedding Privacy

Privacy by Design – mandated

The principle of data protection by design require data protection to be embedded within the entire life cycle of the technology, from the very early design stage, right through to its ultimate deployment, use and final disposal. This should also include the responsibility for the products and services used by the controller or processor.

Privacy By Default

The principle of data protection by default requires privacy settings on services and products which should by default comply with the general principles of data protection, such as data minimisation and purpose limitation.

Document and Demonstrate

Data Protection Risk Analysis yearly

5000 data subjects during any consecutive 12-month period;

processing of special categories of personal data, location data or data on children or employees in large scale filing systems;

profiling on which measures are based that produce legal effects processing of personal data for the provision of health care

automated monitoring of publicly accessible areas on a large scale

Document and Demonstrate

Impact Assessment

a systematic description of the envisaged processing and purpose

an assessment of the necessity and proportionality in relation to the purposes;

an assessment of the risks to the rights and freedoms of data subjects

a description of the measures envisaged to address the risks and minimise the volume of personal data which is processed,

a list of safeguards, security measures and mechanisms to ensure the protection of data

an explanation of data protection by design and default practices

Compliance Review every two years

Role of the Data Protection Officer

- **Removes some of the requirements to contact the Supervisory Authority**
- **Mandatory when**
  - the processing is carried out by a public authority or body; or
  - the processing is carried out by a legal person and relates to more than 5000 data subjects in any consecutive 12-month period or
  - monitoring of data subjects special categories of data pursuant to Article 9(1), location data or data on children or employees and in large scale filing systems.

Role of the Data Protection Officer

- Can be shared
- Fixed term 4 years or 2 if external.
- Independent role
- Must be skilled and qualified
- Must be free to act
- Oversees much of the compliance activities and is responsible for raising awareness etc

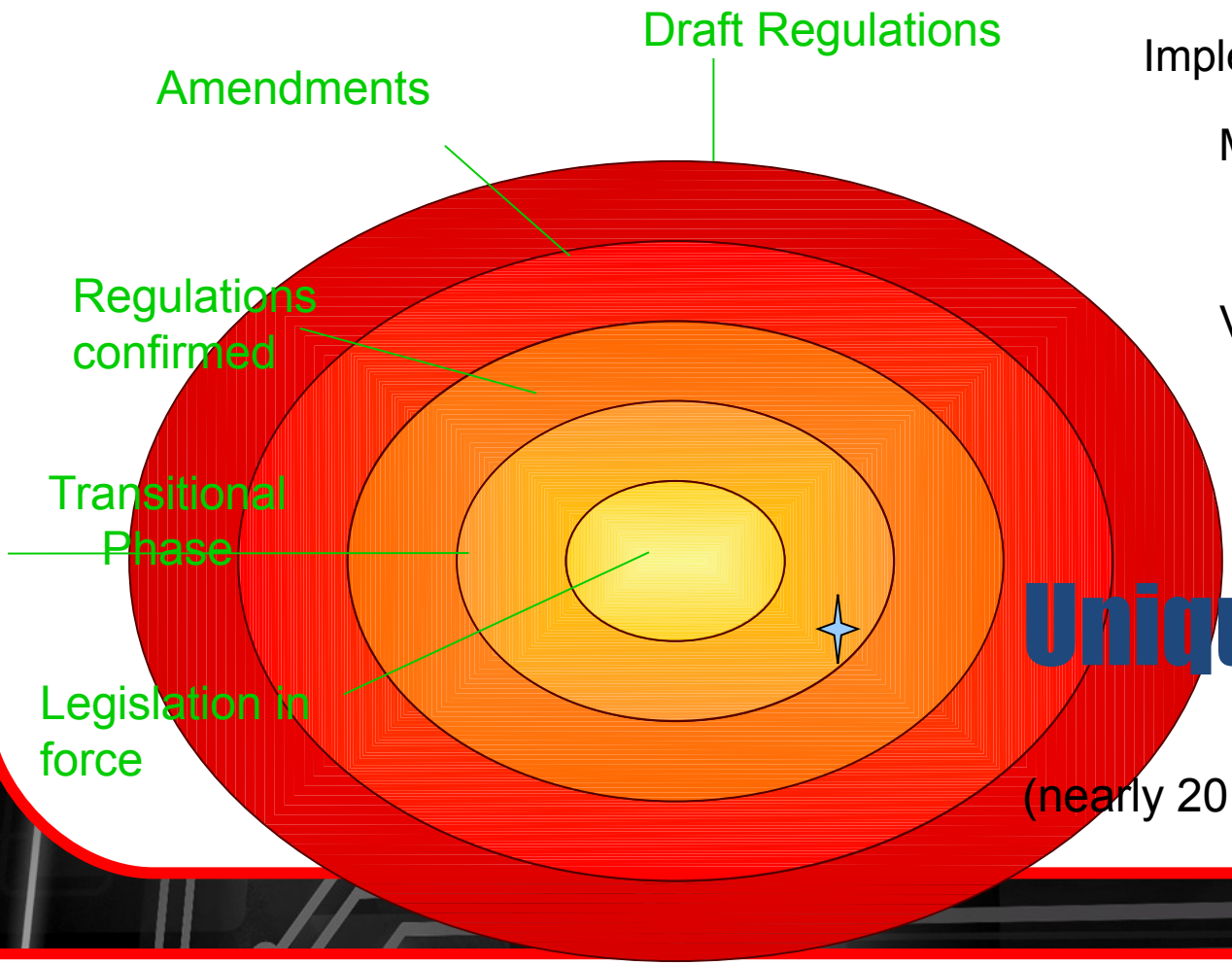
Certification

EU Privacy Seals

- Involve audit and external validation by an accredited company that your processing is compliant
- Can provide some protection in the case of a breach

Where are we going and how do we get there ?

The Challenge



Implement a Compliant Business

Manage Business Change

Understand the Impacts

Validate Existing Practices

Understand the Issue

Unique Challenge

(nearly 20 years since last change)

Be Realistic

Get a balanced and proportionate view of the change – there is a lot of hysteria out there (disclosing not using BCC and Dawn Raids by ICO).

Don't ignore it and hope for the best as change to the proposal is increasingly unlikely

Make sure the people at the top know – they never like surprises

- Corporate briefings
- Explain the impacts
- Build the issue into the business and horizon scan (NHS)
- IBM can support and help in managing these messages

Be honest about where you are as a business.

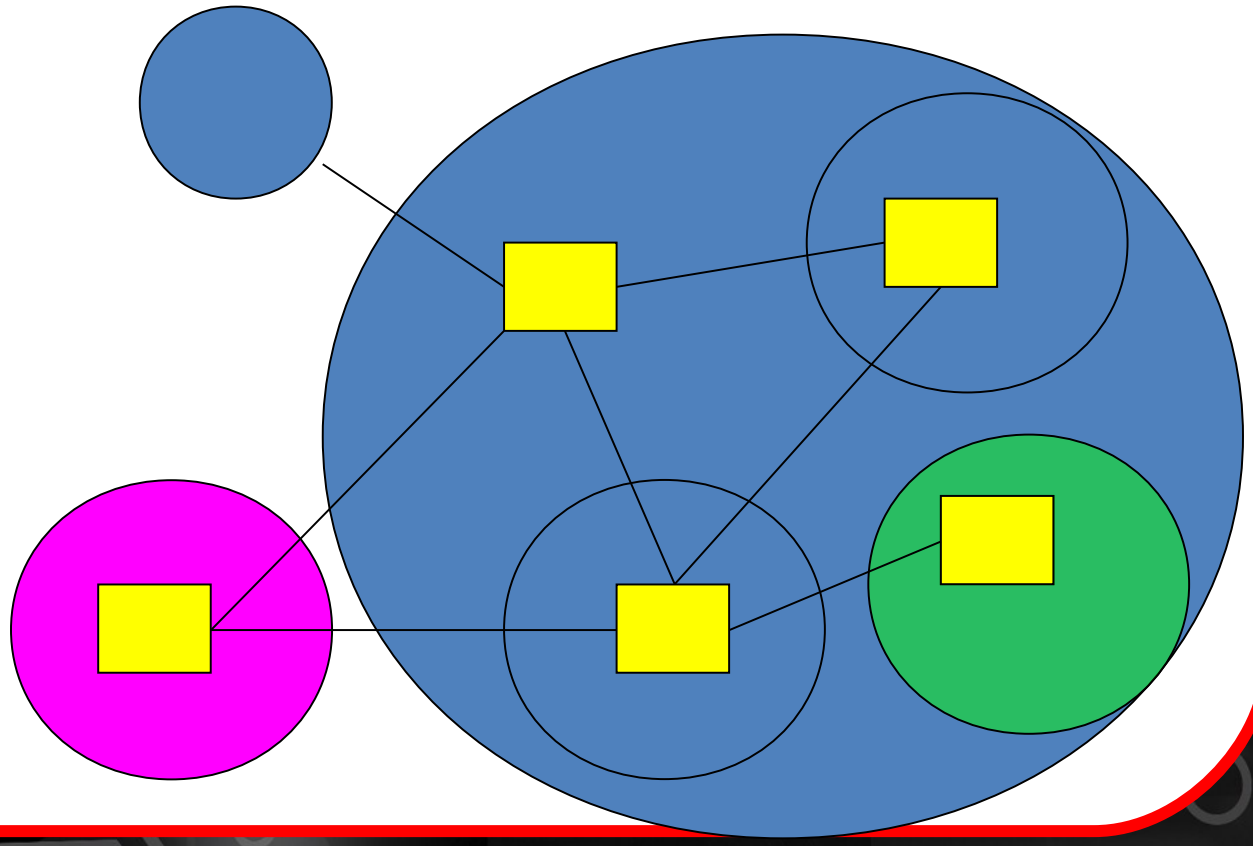
- Much of the Regulations are about a mature approach to Data Privacy - can you deliver that
- IBM provides a wide range of assurance services that can help in this area
- Don't confuse issues - 27001 certification is not the same thing

Get a Data Centric View of the Business

If you don't know what Data you have or where it goes you can never comply (or work effectively as a business)

IBM can assist in the mapping of data and its classification

Using skilled resource tools such as StoredIQ

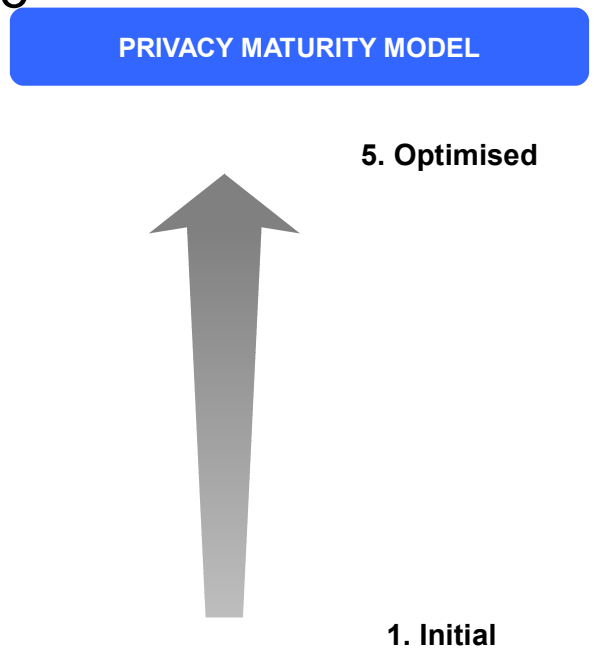


Baseline Now – its going to get more stringent

Understand where you are, where you need to get to, how to get there and what skills, tools and services you need to achieve that.

IBM utilises a Maturity Model that underpins its Assessments and Privacy Improvement Model

This is based on the concepts of Adequacy and Compliance and provides a ***real*** and ***granular*** picture of where the business is in respect of governance of the relevant issues and how to improve.

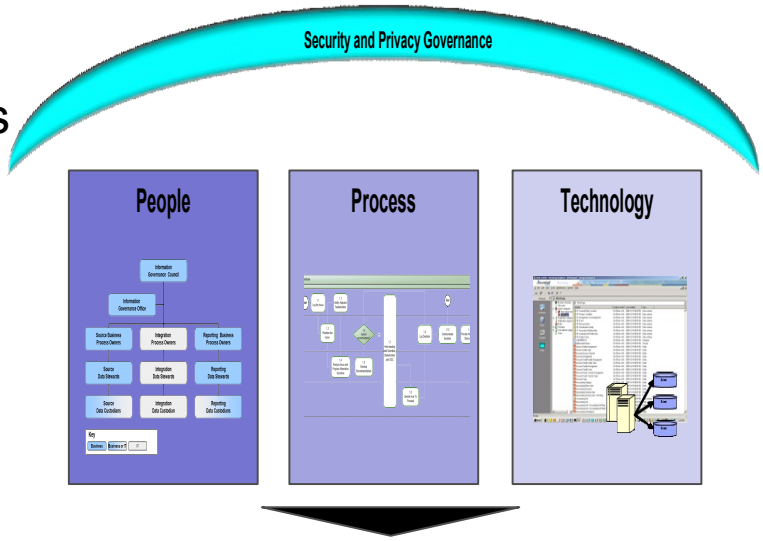


This is a Business Issue

This has strong IT elements but this is a business issue. Remember reengineering a business process (in 2 years) is as painful as reengineering an IT system (maybe more painful !!!).

Don't try and do it all yourself – it is a business issue that needs specialist support across a number of different areas.

Get the right (appropriate) tools to assist with Privacy issues- strong Identity and Access Management tools and processes and Data Loss Prevention Technology



Why You Need To Act

The Legislation will be ratified in the near future

But

In a world where the environment has changed so much shouldn't we be looking to mature our management of data anyway …

IBM Data Privacy Offerings Summary

Data Protection Resource (including Global Privacy and Data Protection Officers)
Training and Awareness Services and Board Briefings
Data Privacy Assurance Check and Full Compliance Review
Data Privacy Improvement Planning
Data Mapping
Privacy Impact Assessments
Privacy by Design Assistance and Tool Sets

Simon Rogers
Security & Privacy
Phone: 0778 9744568
E-mail: simon.rogers@uk.ibm.com

Any Questions