GDPR - HOW IS INDUSTRY ADDRESSING THE LEGISLATION

25 January 2017

https://www.surveymonkey.co.uk/r/7X9LWLZ

Agenda

1. Setting the scene
2. The major elements of the GDPR
3. Impact for organisations and approaches we are seeing to address the legislation
4. Areas of potential negotiation pre and post adoption
5. Additional data and processes that will be required
6. Data discovery and tooling
7. Not just a compliance checkbox exercise

SETTING THE SCENE…

1

What is the General Data Protection Regulation (GDPR)?

Previous state of the legislation:

- Previous national legislation was based on an EU directive from 1995 (95/46/EC)
- The directive had caused an uneven data protection level across Europe.

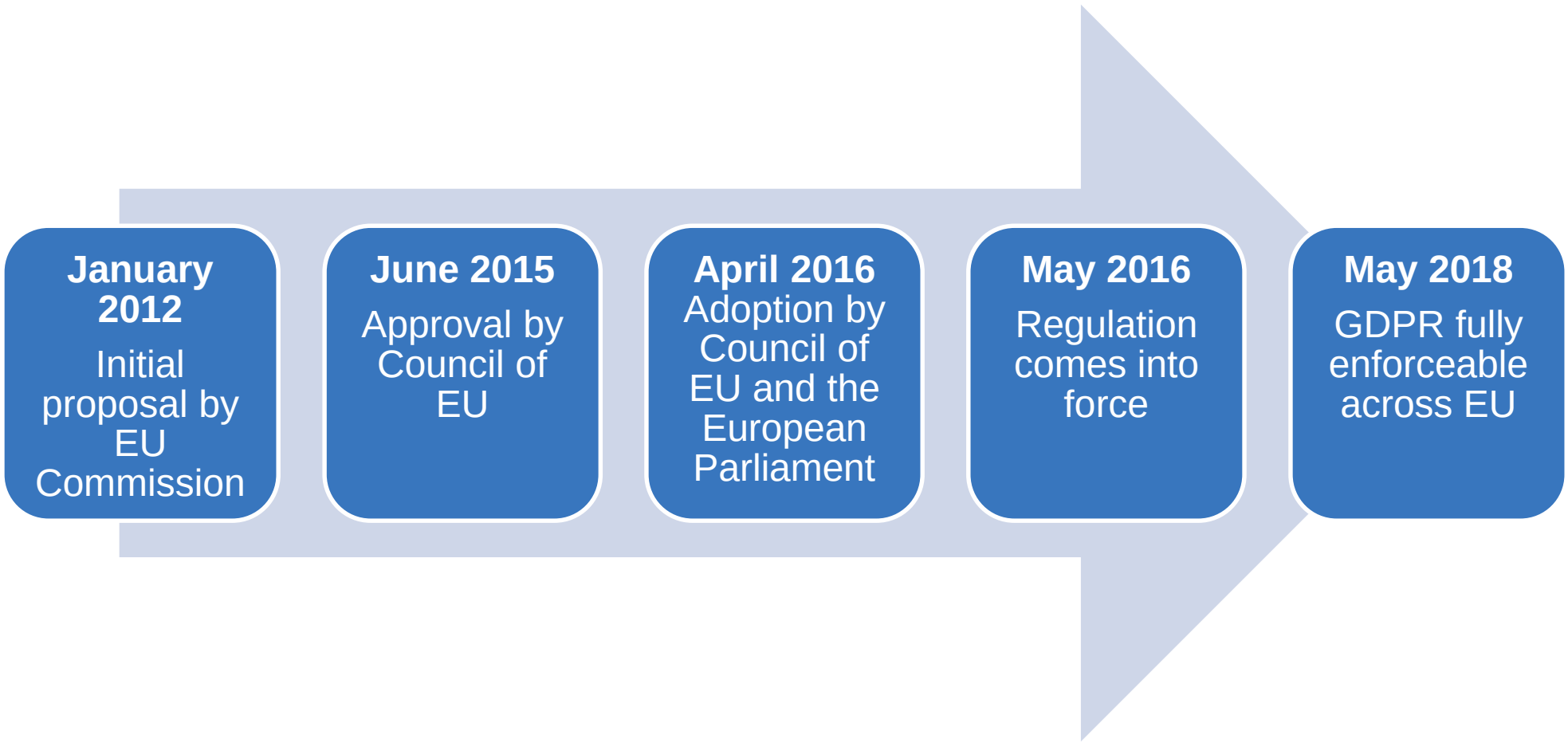
Challenges:

- Digital development had long surpassed the previous legislation
- Globalisation means that many of the players on the digital world market are subject to EU legislation

Purpose of the GDPR – a regulation, not a directive:

- Harmonise the data protection regulations of European Union (EU) member states and ensure the transparent processing of personal data
- Emphasise the rights of individuals and heighten the data protection level of European citizens acting on the digital world market.
- Create better conditions for uniform enforcement and harsher sanctions

The EU GDPR timeline



Impact of Brexit

- The EU's General Data Protection Regulation (GDPR) sets out a harmonised set of data privacy standards and regulations across the EU making it easier for businesses to work together within and trade with the EU
- Although, in time, the UK will be required to update its own data protection laws as a result of Britain's exit from the EU, in the short term nothing will change and, even in the longer term, substantial change is unlikely
- With so many businesses operating across borders, especially digital businesses, consistency with the EU approach to encourage and facilitate business with the UK will be a priority for the Information Commissioner's Office and GDPR Adequacy is very likely to be maintained
- In short, we believe that companies should proceed with their GDPR planning on the assumption that they would either have to adhere to GDPR anyway, because they process EU citizen data, or that the UK government will implement laws that are essentially identical to GDPR.

What data is in scope for GDPR?

Special Categories of personal data considered sensitive include:

- Any information relating to an identified or identifiable person
- Data concerning race or ethnic origin
- Data concerning political opinions
- Data concerning religious or philosophical beliefs
- Data concerning trade-union membership
- the processing of genetic data or biometric data to uniquely identify a person*
- Data concerning health, sex life, or sexual orientation*
- Identifiers such as location data or online identifiers

** Member States are given the right to introduce further conditions/limitations*

THE MAJOR ELEMENTS OF THE GDPR

2

Overview of the major changes

Who?

Reach outside of EU:

Applicable to data leaving the EU

Strengthening the individuals rights:

The right of erasure

Capabilities within the organisation:

Data Protection Officer

How?

Proactive third party information governance

Unambiguous consent

Privacy Impact Assessment

Privacy by Design/Default

What?

Liability extension

Breach notification

Higher fines for non-compliance

Broader territorial scope

Who?

- *Reach outside of EU:* **Applicable to data leaving the EU**
- *Strengthening the individuals rights:* **The right of erasure**
- *Capabilities within the organisation:* **Data Protection Officer**

The GDPR will apply to **all organisations that process personal data about EU citizens.**

- This implies that **organisations located outside of the EU**, will still need to observe the rights of individuals and comply with the obligations of controllers and processors of personal data set forth in the regulation.
- The extraterritorial effect entails that the GDPR will have a **broader application to the online activity of non-EU organisation**, who offer goods or services to EU citizens or who monitor the behaviour of EU citizens as part of their business.

The right to erasure ("right to be forgotten")

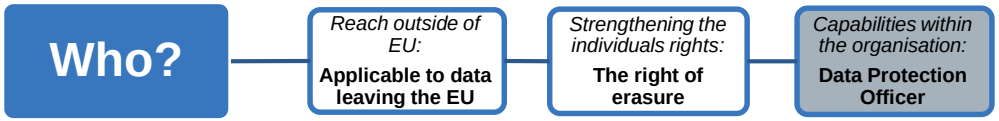
- The right to erasure **obligates the organisation to erase personal data**, if the individual puts forth a request for this
- This right is concerned with the **empowerment for individuals**, and not to erase past events or restrict freedom of the press.
- Individuals can make use of this right if, among other things;
  - The intended purpose for collection no longer exists
  - Consent is withdrawn
  - The individual objects to the processing
  - The data has been unlawfully processed

The right to be forgotten has already been affirmed by the European Court of Justice (ECJ) with its **Costeja decision** in 2014, where the Court ruled that **Google Spain** had to erase links to two pages on a Spanish newspaper's website from the results that were produced when Costeja's name was put into the search engine.

EU court backs 'right to be forgotten': Google must amend results on request

Individuals have right to control their data and can ask search engines to remove results, says European court

Data Protection Officer (DPO)



Designation of the DPO:

- Processing by **Public Authority or Body** (except for Courts)

Or **Core activity** concerns:

- **regular** or **systematic monitoring** of individuals on a **large scale**
- Processing **Sensitive Personal Data** (including data concerning **criminal convictions** and **offences**

If easily accessible, a single DPO may be designated for a **group of undertakings,** or **several public Authorities** or **Bodies**

Position of the DPO:

- Involved in **all data protection issues** (in a timely manner)
- **Contact point** for data subjects and the Supervisory Authority
- Must be **independent** and not receive instructions on tasks and must report directly to the **highest level of management.**

Tasks of the DPO:

- **Advise** within the organisation regarding the regulation and other Union or Member States data protection provisions
- **Monitor** compliance with the Regulation and other Union or Member State provisions and organisational policies or processes relating to the protection of personal data (Including assignment of responsibilities, awareness raising and training and audits).
- Ensure **notification** of DPAs and individuals regarding data breaches
- Advise upon the completion of **PIAs** when necessary.

Proactive Third Party* Information Governance

How? | Proactive third party information governance | Unambiguous consent | Privacy Impact Assessment | Privacy by Design/Default

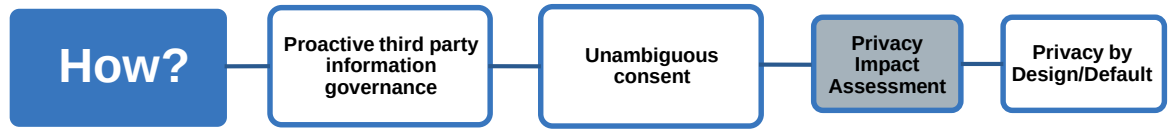
- With the growth of outsourced vendors and suppliers, regulation and standards are now focused on third parties and GDPR is no exception
- Governance of third parties processing information must be proactive
- Identification of where and how information is transmitted, processed and stored
- Clarity over the designation over the data controllers and data processors
- Cloud providers are designated as data processors
- Template MSA/data protection clauses and tender documentation should be updated

* Third Party means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data

Unambiguous consent

- Consent must be presented in such a manner that it is:
  - Clearly distinguishable from other forms/requests from the organisation
  - Intelligible
  - Easily accessible
  - Clear and plain language
- The **controller bears the burden of proof**
- In the instance of processing **children's personal data**, consent must be **given by the parent** or **holder of parental responsibility**
- Consent must be given **freely** and the data subject has the **right to withdraw** consent at any time
- Consent shall be **as easy** to withdraw as to provide

Privacy Impact Assessment



The need for a PIA

- Is the processing of data likely to result in a high risk for the rights or freedoms of individuals?

Information flow

- How does data flow from collection to processing to deletion?
- Likely number of affected individuals?
- Purpose of collection?
- Who has access to data?

Risks

- What risks does the processing entail for individual's privacy
- What corporate and compliance risks may be associated with the proposed processing?

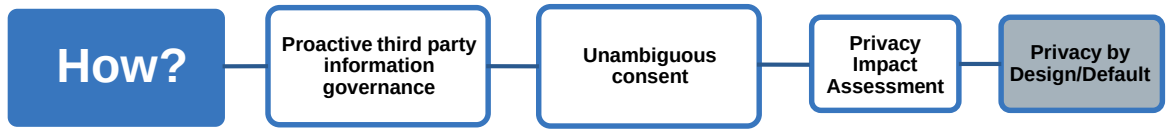
Mitigating measures

- What organisational and technical measures will be taken to mitigate the identified risks?

Sign off

- Who has approved the proposed processing and the identified associated risks?
- Who is responsible for the implementing the mitigating measures?

Privacy by Design and Privacy by Default



Privacy by Design

- Protection of personal data must be **embedded into the design and architecture** of IT systems and business processes.
- It must **not be an add-on**, after the fact.
- Privacy must become an **essential component of the core functionality** that is being delivered.
- This entails that protection of personal data is **integral to the system**, without diminishing functionality.

Privacy by Default

- Personal data must **automatically be protected** in any given IT system or business practice.
- If an individual **does nothing**, their privacy will still remain intact.
- **No action is required** on the part of the individual to protect their privacy – it is built into the system, by default.
- **Privacy settings** that limit the sharing of personal data must be **turned on** as a default setting.

Liability extension

- Liability is extended to the Data Processor as well as the Data Controller
- This liability extends to cloud provision
- The responsibility and liability of the Controller for any processing of personal data carried out by the Controller or on the Controller's behalf should be established.
- In addition, the regulation makes provision for **Joint-Controllers**, with each controller being liable for compliance with the regulation

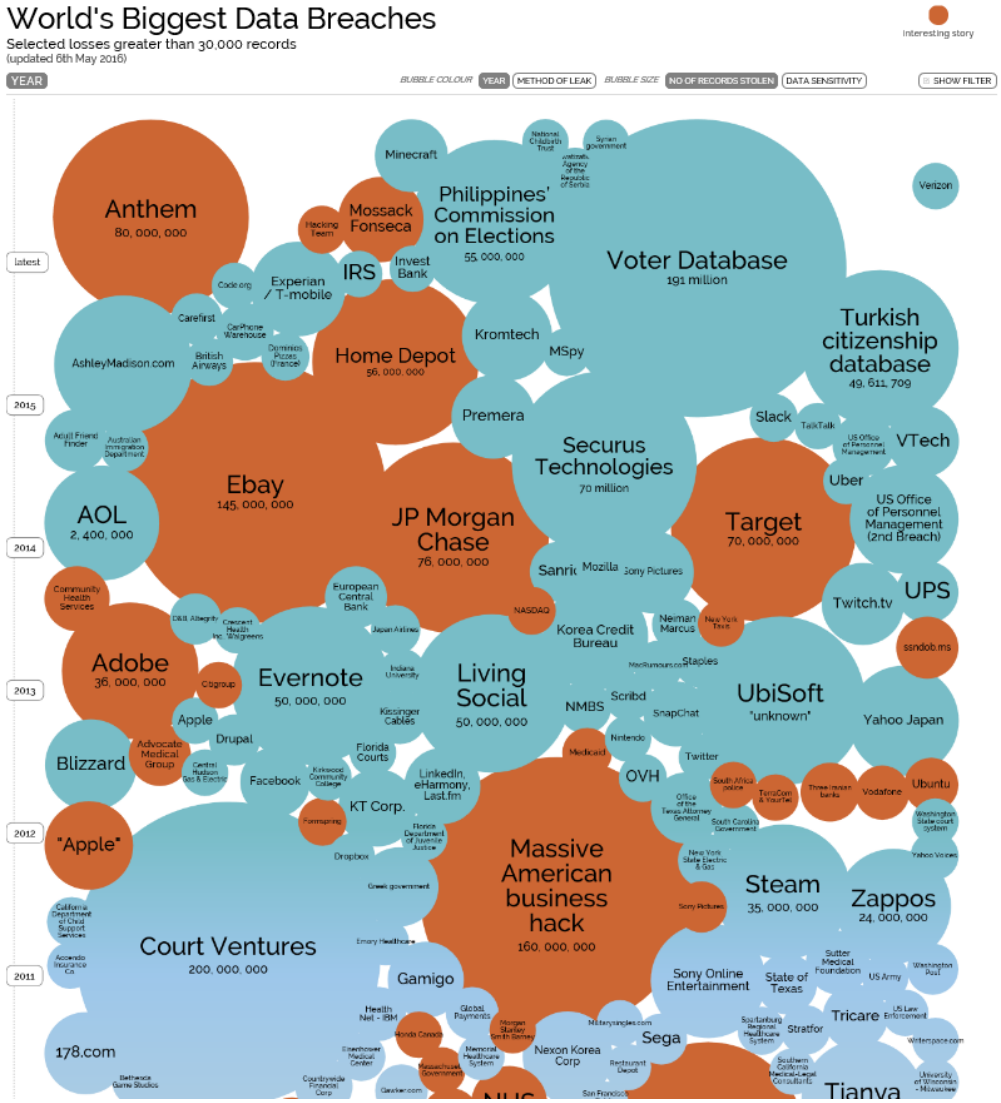
What? | Liability extension | Breach notification | Higher fines for non-compliance

Breach notification

Data breaches must be reported to the Data Protection Authority (DPA) within **72 hours** (where feasible) and affected individuals must be informed of the breach **'without undue delay'**.

The notification to DPAs (and affected individuals) must at least contain:

- A description of the nature of the breach
- The categories and number of affected individuals
- Contact details of the DPO/contact point
- The likely consequences of the breach
- Measures taken or proposed to be taken to address the breach
- An incident response team and procedure must be in place



Higher fines for non-compliance

- In the case of **non-compliance** the organisation risks fines of up to **4%** of the annual global turnover or **€20M**, whichever is greater
- In deciding the amount of the fine, the following will, among other things, be considered:
  - the **nature, gravity and duration** of the breach
  - the **character** of the breach, whether intentional or negligent
  - the **actions taken to mitigate** the damage suffered by individuals due to the breach
  - **previous breaches.**
  - Degree of co-operation with authorities to remedy the breach or mitigate the adverse effects

Some other concepts

- Subject Access Requests (Article 15) and Rectification (Article 16)
- Data Portability (Article 20)
- European Data Protection Board replacing Article 29 DP working party under GDPR and will issue guidance to controllers and processors on such elements as the data portability right, PIAs, certifications, and the role of DPO's
- Certification schemes, basic rules on the establishment and operation of "data protection certification mechanisms and of data protection seals and marks" are set out under GDPR (Articles 42 & 43)
- Pseudonymisation, "means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person"
- Record of processing activities (Article 30)

IMPACT ON ORGANISATIONS AND APPROACHES WE ARE SEEING TO ADDRESS THE LEGISLATION

3

Impact on Organisations

The GDPR contains changes of emphasis and substance which are intended to strengthen the rights of EU data subjects, to extend the territorial scope of protection of EU data subjects to controllers established outside the EU, to achieve consistency across member states, and to ensure compliance by strong sanctions.

These changes are of potential importance to all organisations which process the data of EU data subjects, wherever they are based, and they need to evaluate and if necessary act upon the new requirements now in order to be in a position to comply with the revised regime when it comes into force and to avoid potentially serious sanctions.

The challenges for organisation include the specific topics which are outlined in the previous section, and meeting them is likely to require a consolidated effort between a number of stakeholders within the organisation such as Compliance, IT, Information Security, Legal, Marketing, Procurement, Finance and Audit functions.

Where to start

Conduct detailed gap assessment against GDPR requirements

⇩

Define and shape remediation programme as per gap assessment findings

Typical activities and workstreams include:

Appoint a DPO and set up roles and responsibilities	Update security policies and procedures	Locate personal data, Define information flows	Conduct PIAs
Incorporate privacy into Incident Management process	Determine appropriate control activities	Conduct awareness activities and training	Conduct Privacy by Design assurance activities
Review consent model	3rd party contract review	Data minimisation and accuracy	Manage rights of individuals

Security and data architecture

Compliance must be supported by appropriate technical tools, however such tools must not only be implemented as a technical solution, but be incorporated into business processes.

Locate personal data and define information flows First, organisations need to evaluate the personal data they have; categorising the data so they are clear where the personal and sensitive data resides and where other less important data sits in the company. GDPR demands a risk-based approach with the development of appropriate controls.

Identity and Access Governance is a set of tools and processes that allows an organisation to translate technical access rights into business language and to build business processes so that the right people have the right access to the right systems at the right time.

Data Management allows an organisation to manage information through the full data lifecycle – from collection to destruction.

E-discovery tools enables the organisation to identify where data is stored, as well as what it is used for, how it is distributed and by whom.

Policies and procedures

Privacy policy

- A specific policy to emphasise the importance of privacy. It must describe:
  - **why** data is collected (purpose)
  - **who** the data concerns (categories of data subjects and data)
  - **what** type of processing is done (storage, viewing, alteration etc.)
  - **where** data is stored (including use of 3rd parties)
  - **when** data must be destroyed (retention requirements)
- The policy must be supported by underlying procedures and guidelines.

Internal and external audit

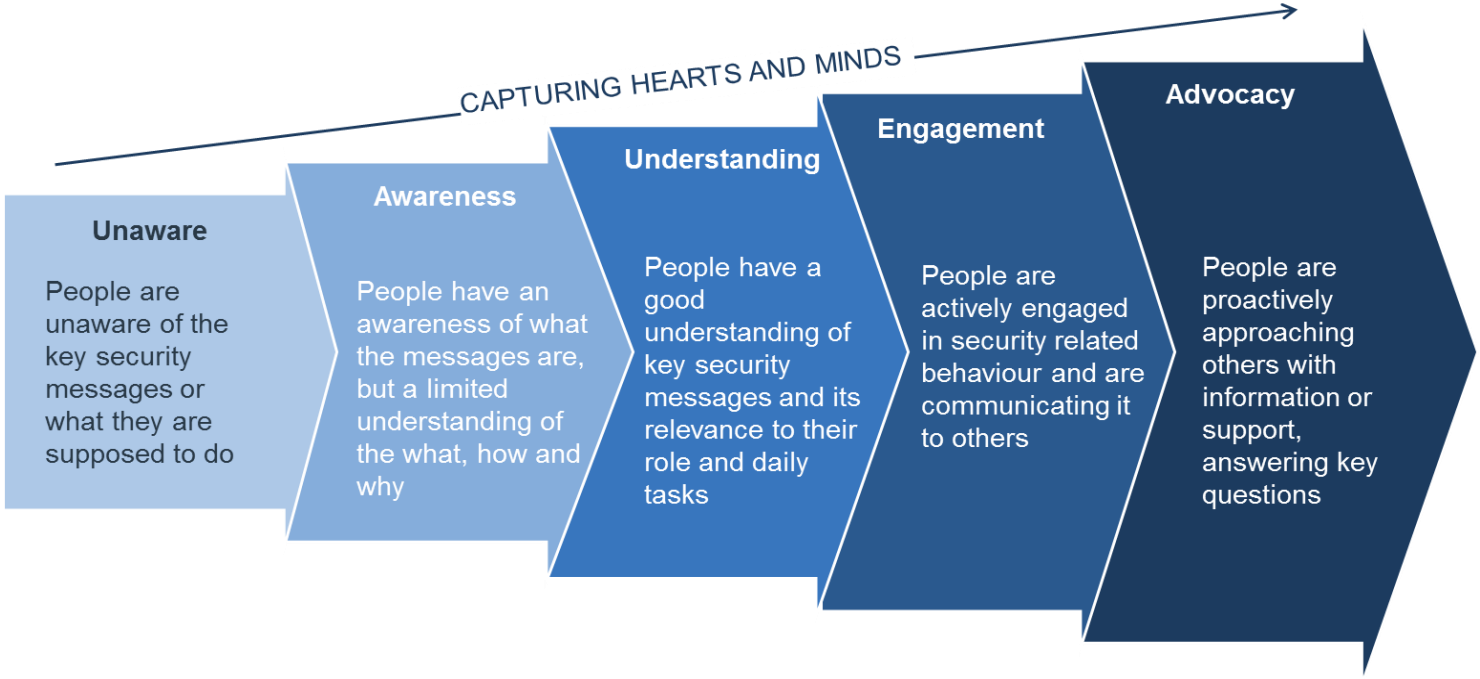
Documentation, policies and control activities are key, however **worthless** without internal monitoring and external control.

The DPO must build and maintain the privacy program, including supporting all privacy issues – **a strategic business function**.

External auditing must ensure the efficiency and effectiveness of the privacy program. Can play an important role in 3rd party reviews – **a controlling function**.

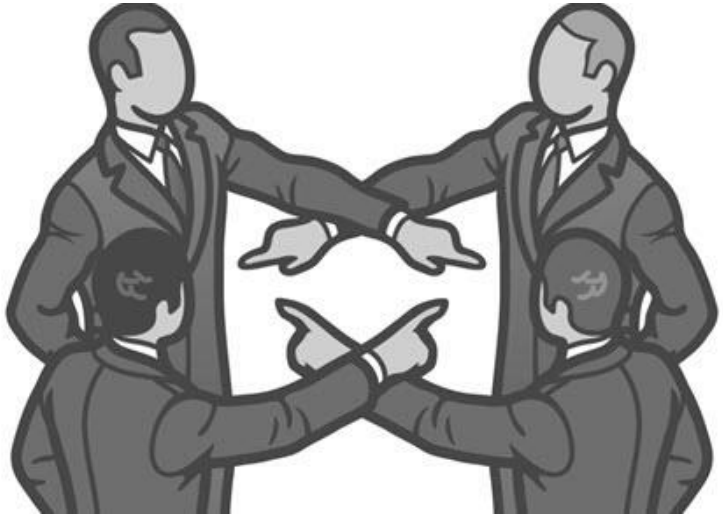
Privacy Awareness and training

Keeping on top of these challenges requires a combination of skills to not only shape, define and implement robust controls and defences, but also change user behaviour to build a positive, security conscious culture across the organisation by driving an adequate awareness and training programme



Accountability

- Overall compliance with the GDPR and, consequently, the implemented technical and organisational compliance and security measures
- Information flows – from collection to destruction
- Consent
- Personal Data Breach handing/documentation and notification to the Data Protection Authorities and data subjects



The burden of proof starts and stop with you.

Document ***how*** you do it and ***that*** you do it.

AREAS OF NEGOTIATION PRE AND POST ADOPTION

4

Areas of negotiation pre and post adoption 1/2

- Larger and established companies are taking the view that the procedures and processes will be in place in a future mode from adoption and are **not** necessarily taking **historic** and particularly **legacy** data stores into consideration
- Organisations are looking seriously at what data can be **exempted** from the regulation to protect themselves and their partners and staff
- Data Erasure is causing concern and organisations are looking at **member state exemptions** around unlawfully processing
- Although GDPR is a regulation rather than the existing directive, there are a number of instances where it does allow member states to legislate, such as where personal data is required to comply with a legal obligation and there are a number of articles that cite **member state law** may further specify or restrict
- Both Privacy by Design and Privacy by Default are topics for debate, for **Privacy by Default** especially around applications, who is responsible; the developer, the publisher, the distributor and it doesn't fit with mobile app where the rights are proportionate to the service received
- EU Commission will find '**balanced solutions**' to not make GDPR too onerous for businesses

Areas of negotiation pre and post adoption 2/2

- Throughout the four year period of construction of the regulation and continuing now the subject of **breach notification** was and is a hot topic and the definition, recipient and time period changed, where the notice period oscillated between 24 and 72 hours
- **Enforcement** under GDPR will need scrutiny and maturity
- GDPR will have to buck the current trend of **data localization**
- **Profiling** (article 22) has been a constant debate topic and is a compromise and interpretable provision
- **Big Data** seen by some as a facilitator of the regulation and by others as eroding data protection principles
- Although there are clear references to ensuring the security of the processing, there are **no technical details** such as levels of encryption
- GDPR complicates **outsourcing** arrangements and will a manageable solution be achieved
- It will be harder to use **cloud computing** to process personal data compliantly

ADDITIONAL DATA AND PROCESSES THAT WILL BE REQUIRED

5

Information requirements

The baseline information necessary for the Privacy Impact Assessment:

- Systematic description of the envisaged processing operations
- Description of the necessity and proportionality for the processing operations
- Measures envisaged to address the risks, including security mechanisms
- Documented data subject rights and freedoms assessment

- Overall data requirements and ability to prove effectiveness of:
  - Pseudonymisation (meaning that additional data that creates referenceable data is held separately) of personal data
  - Encryption of personal data
  - Confidentiality, integrity, availability and resilience of processing system
  - Ability to restore and process for regularly testing, assessing and evaluating effectiveness

Potential additional data needing to be captured

- Per type of data
  - Purposes of the processing for which the personal data are intended
  - Nature, scope, context and risks of processing
  - Period for which the personal data is stored and criteria on which that is based
  - The categories of personal concerned
  - The recipients or categories of recipients to whom the personal data will be disclosed
  - Documented processing instructions from controller to processor
  - Categories of data subject
- Per data subject (customer/employee/individual):
  - Explicit consent reference including date per data subject
  - History of data subject requests and responses

Potential additional processes needing to be created

- Remedial action per data subject:
  - Rectification of inaccurate data
  - Right of erasure
  - Right of data portability
  - Right to object particularly for direct marketing purposes
  - Right to not be subject to a decision based solely on automated processing, including profiling

DATA DISCOVERY AND TOOLING

6

The Challenge

- Identify whether the any of the described infrastructure, processes and data are in existence
  - Infrastructure review of architecture focussing on data flows and stores
  - Process documentation alignment review with existing personal information processes
  - Data Discovery mining exercise using interview/survey and Business Intelligence/Data Visualization/Data Loss Prevention tools (following slide)
  - Gap analysis report / Preliminary Privacy Impact Assessment (to position ‘before scenario’)

The Challenge

- Produce strategy to facilitate the changes into the environment
  - Taking the data discovery results set a priority risk-based schedule of costed activities with outcomes
  - New data structure creation within architecture to facilitate additional data and processes
  - Improved security measures adoption approach to address enhanced protection levels
  - Gain sponsorship support to expedite and maintain new eco-system

Tooling

- Data Discovery can be accomplished by traditional Business Intelligence (BI) tools (relatively expensive but powerful) that organisations may already have or by Data Visualization tools that have the advantage of being cheaper, agile and more user friendly or Data Loss Prevention (DLP) tools that lead to a more direct security based reporting or a combination of the tool types
  - BI examples: Oracle, IBM Cognos Express, MS PowerPivot, SAP Business Objects, Information Builders WebFocus Visual Discovery
  - Data Visualization: Tableau, TIBCO Spotfire, Qlik Sense
  - DLP – most of the major security tools vendors have DLP: Symantec(ex-Vontu), EMC RSA, Trend Micro, McAfee, Sophos, Websense, as well as more specialist vendors such as BullGuard, Devicelock and Digital Guardian.
  - Data Protection Laws services: DataGuidance, Nymity, Truste, OneTrust

NOT JUST A COMPLIANCE CHECKBOX EXERCISE

7

There are a number of difficult customer problems that GDPR may provide the catalyst to solve

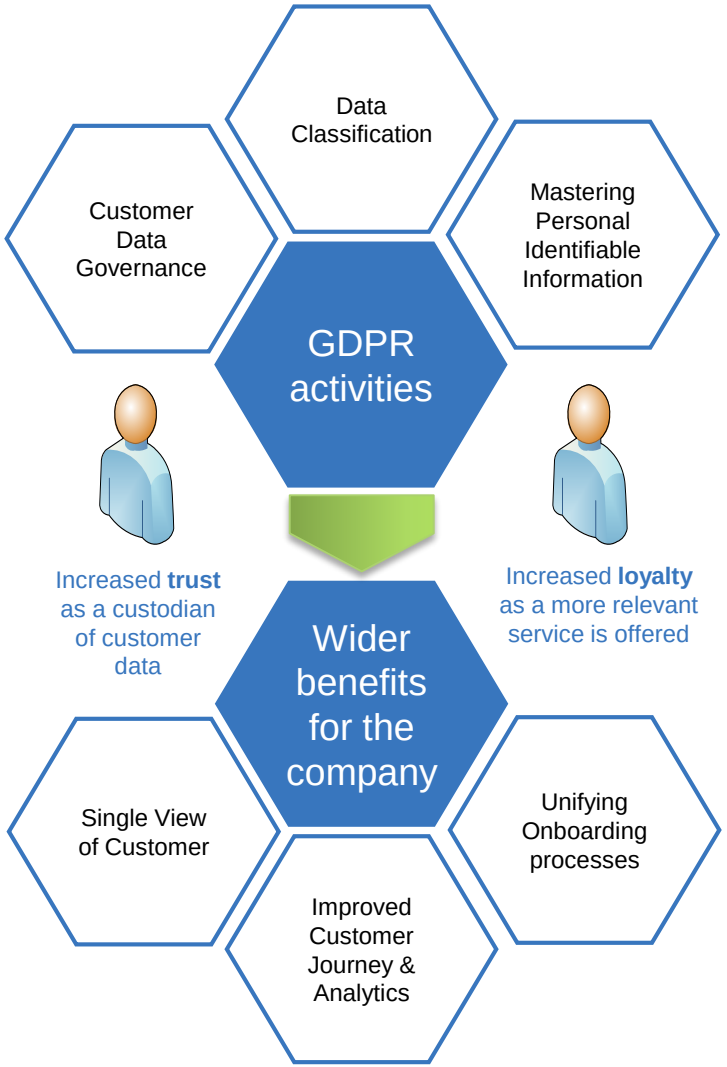
Thinking beyond compliance can create additional benefits

GDPR provides your customers with much greater autonomy over how you can use their data and interact with them.

Your customers need to **trust** you with their data and feel they are getting **value** from allowing you to use it – or they will withdraw consent.

So while compliance is important, it is not enough if you want to create customer-centric products (you can be compliant, but customers can still withdraw consent…..and that's a poor commercial outcome).

Only Scoping your GDPR programme with the letter of the regulation in mind will miss opportunities to improve customer experience, engage wider stakeholders and therefore opportunities to accelerate.



A differentiator to standard compliance adherence

The advent of GDPR while giving an organisation a compliance imperative also facilitates a new approach to their information particularly customer data. If the exercise is undertaken sympathetically it may afford a number of initiatives that would result in corporate efficiencies such as:

- Single view of customer (individual/employee)
- Removal of redundant, duplicated and misleading information
- Metadata (descriptive, administrative, structural) construct (and or tagging)
- Complete view of data landscape
- Rationalisation of processes such as on-boarding
- More granular retention scheme

Why PA? PA has a comprehensive information and cyber security offering which includes Data Protection and GDPR expertise

Understand digital risks

Identify the assets, systems and processes that are critical to business operations and understand the impact of their loss/disruption to the business

- Threat identification
- Risk management
- Systems health checks
- Cyber maturity assessment
- GDPR, PCI-DSS, ISO27001 Compliance

Qatar Stock Exchange

PA example: Provided expert services to strengthen cyber security for a national stock exchange

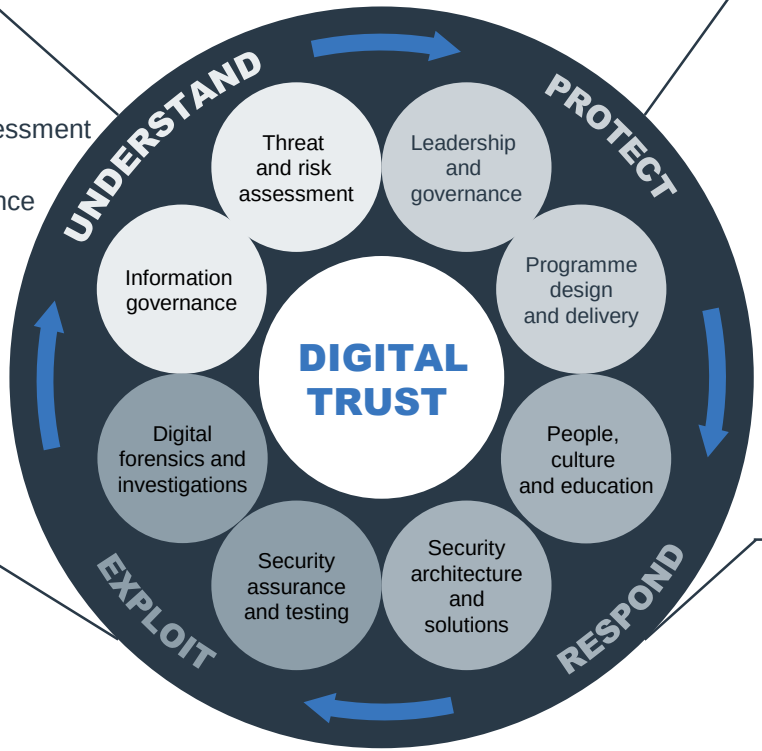
Exploit the value of information

Effective management and innovative exploitation of digital information assets to support business operations now and strategic planning for the future

- Knowledge management
- Data exploitation
- Secure information sharing

Government

PA example: Established a framework for safe, secure, collaboration with highly sensitive data



PA's offering in Information and Cyber Security

Protect data and critical assets

Define, design and deliver controls and improvements to protect the business, by ensuring that risks are addressed by all staff and business operations continue

- Governance & policy development
- Regulatory and legal compliance programmes
- Embed a staff security culture
- Security architecture & solutions
- Penetration & vulnerability testing

Nuclear

PA examples: Designed a programme to protect a nuclear power stations from cyber threats

Rail

Designed a multi year programme to safeguard Britain's rail network from cyber attack

Respond to incidents

Enable the business to detect, investigate and respond appropriately to incidents to minimise disruption and ensure a swift return to business as usual operations

- Cyber monitoring
- Behavioural monitoring
- Incident response planning
- Investigative & forensic support

Retail

PA example: Helped a major online retailer respond quickly and effectively to a significant security breach

Please get in touch if we can help you with your GDPR requirements

Mark Pearce

Mobile: +44 7767 670 519

Mark.Pearce@paconsulting.com

Michael Shuff

Mobile: +44 1763 267 639

Michael.Shuff@paconsulting.com

Elliot Rose

Mobile: +44 121 450 4444

Elliot.Rose@paconsulting.com

The PA Promise

UNCONSTRAINED THINKING EXCEPTIONAL RESULTS

Clients choose us because we are committed to bringing them the right expertise – unconstrained by conventional thinking we deliver exceptional results with lasting impact.

The right team

We focus our expertise where you need it most. Committed to a common goal, we are free to pull together experts from across our whole firm to ensure you get the right team.

Unconstrained thinking

You get team players driven to understanding individual needs and finding new ways of unlocking your business' potential – challenging assumptions, unconstrained by conventional thinking.

Exceptional results

Our experience and commitment to doing things right mean we will overcome every obstacle and together deliver exceptional results for you and your company.

Lasting impact

Our work goes beyond getting the job done – we share our knowledge to create a lasting impact and a brighter future for your organization, your people, your customers and you.