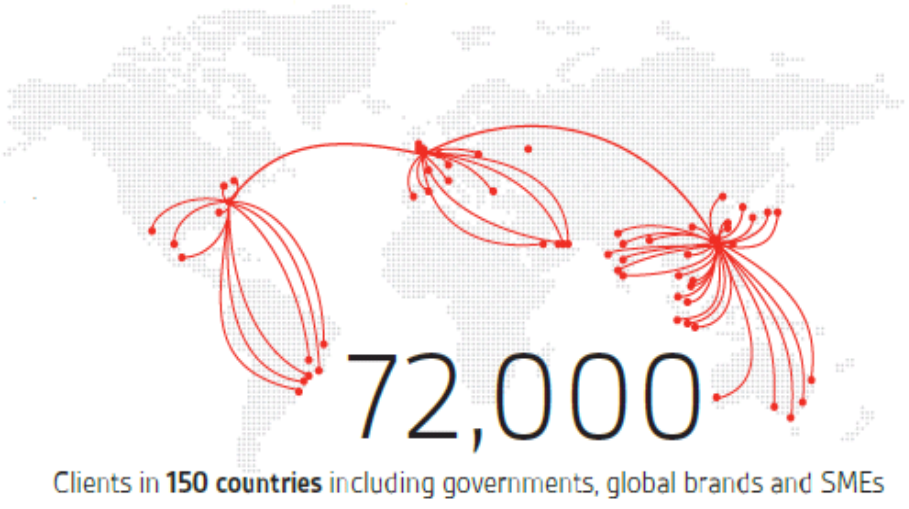
General Data Protection Regulations

Overview of the upcoming regulations and their likely impact on Cloud and Data Centre management.

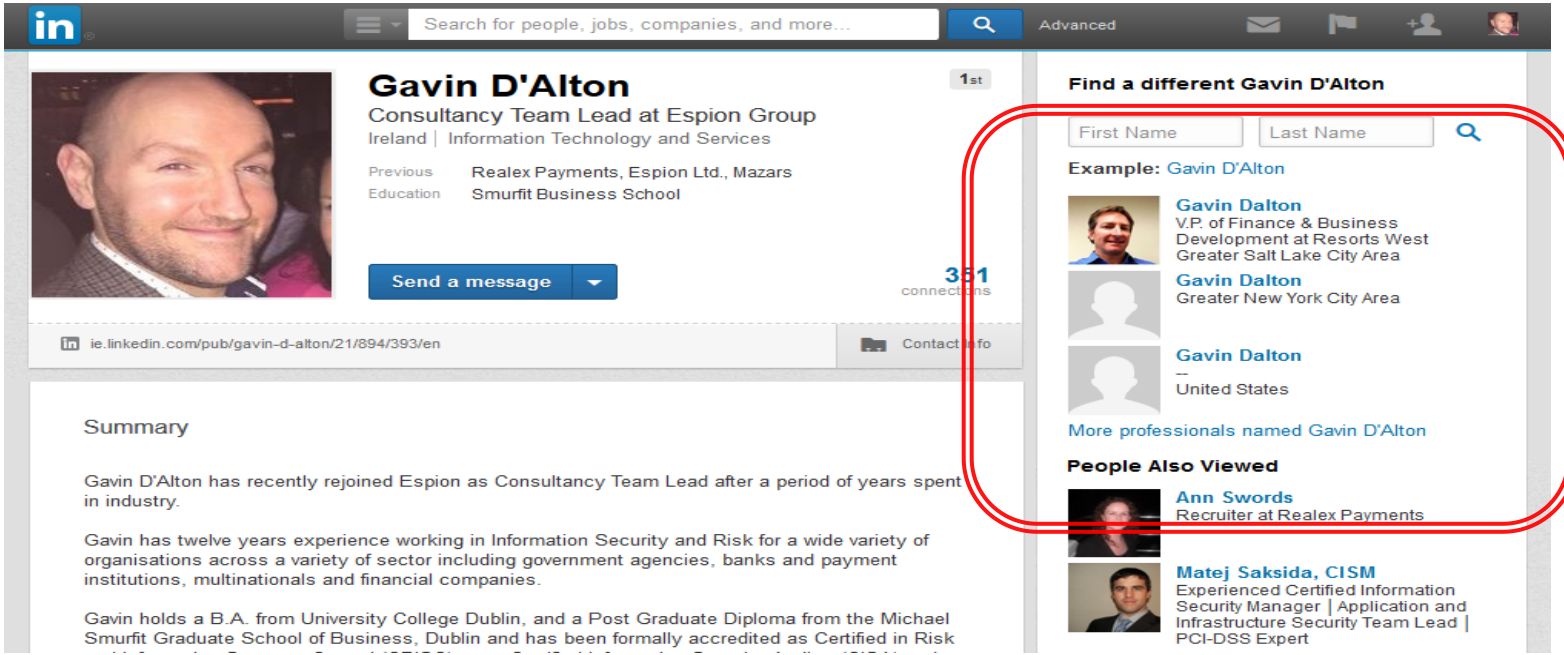
Company Overview - BSI

- World's first National Standards Body
- Been around since 1901
- 72,000 clients in over 150 countries worldwide
- Offices in over 67 locations around the world
- Working with 54%+ of FTSE500
- Royal Charter status, profits reinvested



Me!

*ie.linkedin.com/pub/dir/**Gavin/D'Alton***



Lots of Noise…

Very Brief) Overview of the Data Protection Act

European Data Protection Directive

- 1) Data Protection is about the management of the processing of personal data and the creation of a framework for the lawful processing and protection of personal data.
- 2) The Data Protection Directive (officially Directive 95/46/EC)is a European Union directive adopted in 1995 which regulates the processing of personal data within the European Union.
- 3) The legislation provides a balance between individual rights and organisational necessity by providing a framework within which to process data fairly and lawfully.

Fundamental Rules

The 8 requirements:

- 1) Obtain and process the information fairly.
- 2) Keep it only for one or more specified and lawful purposes.
- 3) Process it only in ways compatible with the purposes for which it was given to you initially.
- 4) Keep it safe and secure.
- 5) Keep it accurate and up-to-date.
- 6) Ensure that it is adequate, relevant and not excessive.
- 7) Retain it no longer than is necessary for the specified purpose or purposes.
- 8) Give a copy of his/her personal data to any individual, on request.

Definitions & Concepts

- **Personal Data**: Any data that identifies a living person
- **Countries**: 28 countries of the EU +3 of EEA
- **Global Applicability**: You do not need a legal presence in the EU
- **Sensitive Personal Data**: ethnicity, religious belief, sex life, philosophical beliefs, trade union membership.
- **Data Subject**: User or Person
- **Data Controller**: Defines the data collected and reasons
- **Data Processor**: Processes data on behalf of the data controller
- **Supervisory Authority**: Data regulator

Background to the GDPR

- What are the key factors driving this?
- Who are the key players in the reform?
- Why now?
- What took so long?

Timelines

Timeline: Directive (EU) 2016/80 and Regulation (EU) 2016/679

- EU Data Protection Regulation **published** 2016
- The **Directive** enters **into force** on 5 May 2016
- EU Member States have to **transpose** it into their national law by 6 May 2018.
- The **Regulation** enters **into force** on 24 May 2016
- It shall **apply from** May 25th 2018

Radical Overhaul?

Not really…

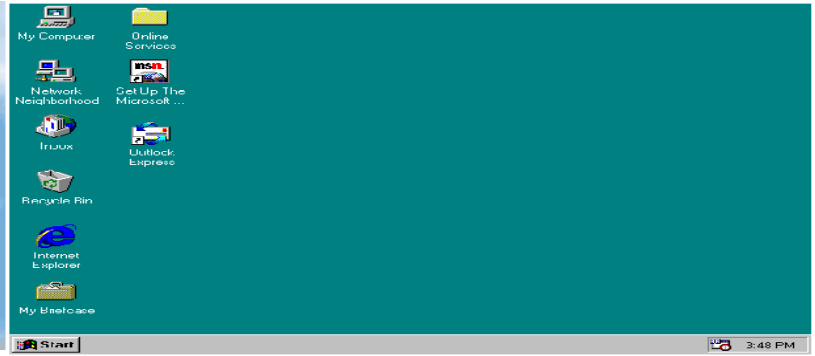
- The proposed changes do not represent a radical overhaul of DP law, rather an enhancement of the existing law.
- Some clarifications.
- And a few new requirements.

But…

- Fundamentally the same intent.

Why now?

- When the 1995 law came about, the internet was in its infancy (Our Digital DNA is now everywhere we go)
- And every country has interpreted things a bit differently…



Goals?

What does the Commission hope to achieve?

- Consistency of interpretation and enforcement.
- Ensure a high level of DP across all industries.
- Reinforce individuals' rights – privacy by design and by default.
- Strengthen the EU internal market through new, clear and robust rules for the free movement of data.
- Set global data protection standards

Impacts!

What the GDPR will mean for regulatory compliance

- National data protection authorities for the EU28 countries (as per the Article 29 Working Party section)
- Local regulation will be subject to a higher scrutiny
- Newly defined independent European Data Protection Board (EDPB) is to replace the article 29 Working Party (key element in the One Stop Shop mechanism).
- The GDPR will replace the current Directive and will be directly applicable in all Member States without the need for implementing national legislation. Member States may still provide more specific rules.

The Main Implications

- More than just a “Top 10”

Top 10 Provisions of GDPR

- **Increased fines** – 4% of global turnover or €20,000,000
- **Privacy by Design** – Privacy to be 'baked in' via Privacy Impact Assessment
- **Opt-in consent** – Clear, no opt-out, use data only as agreed
- **Breach notification** – 72 hours to regulators, users "without delay"
- **Territorial Scope** – All organizations with data on EU individuals
- **Joint Liability** – Data Controllers & Processors
- **Right to Erasure** – The users are in charge
- **Mandatory DPO**?
- **Common enforcement** – Authorities will be strict
- **Collective & individual redress** – Class action & individual lawsuits from individuals

More Provisions of GDPR

- “One Stop shop”
- New European data protection board (EDPB replacer Art 29 Working Party)
- Removes ambiguity – 28 laws become one
- Data portability
- Personal liability?

Summary of Provisions

What it means: The user is in charge. Data Subjects may demand:

- Ask how data was initially sourced
- Ask for the data storage policy
- Access to all their data
- That the data be updated or deleted.
- Right to object to direct marketing
- Compensation for damage if data lost
- That the regulator investigates a concern

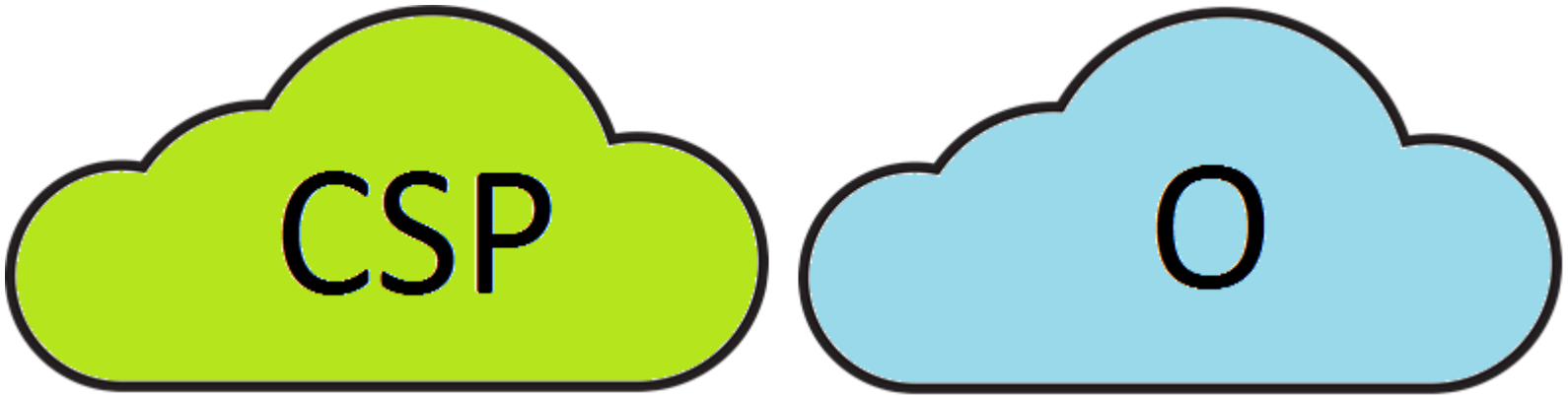
Interesting Clarifications:

- For Cloud Service Providers

  and

- For Organizations hosting personal data in the Cloud

Impact – Service Providers & Organizations



Clarity: Cross Border Impact

The GDPR will have extra-territorial effect

- If the data processed belongs to a data subject in the EU. the law will apply, even to a controller or processor not established in the EU
- Legal terms used: "*Offering goods or services*" or where "*Monitoring of behaviour*" will occur. i.e. Targeting EU consumers.
- Many will need to appoint a representative in the EU.

However… (Please note!)

- The GDPR also makes clear that it is not lawful to transfer personal data out of the EU in response to a legal requirement from a third country.
- It also imposes hefty monetary fines for transfers in violation of the Regulation. (this is already happening)

Clarity: Liability for Data Processors

Controllers and processors will be jointly liable for data protection breaches.

- Data processors now have direct obligations, including:
  - implementing technical and organisational measures, notifying the controller without undue delay of data breaches and appointing a DPO (if required).
- This will likely impact how data protection is addressed in contracts / SLAs. More detailed contract terms and flow down terms for sub-processors are required.
- Processors now liable for breaches when acting outside the instructions of controllers.
- Detailed records of processing activities must be kept by processors and controllers and must be made available for inspection by the Supervisory Authority.

Clarity: Liability for Data Processors

Clarifications for Sub-Processors

- Processors are now prohibited from enlisting another processor without prior specific or general written permission of the controller.
- Controllers retain the right to object to the addition or replacement of processors.
- Sub-processors also are subject to the same requirements under the GDPR and they too are bound by any contracts with the controller.

Clarity: Liability for Data Processors

Vendor Management in the New Context.

- Controllers will maintain specific responsibility for:
  - Carrying out data protection impact assessments on vendor engagements
  - Assuring the protection of data subject rights, such as erasure, reporting and notice requirements, and maintaining records of processing activities.
  - Duties to the supervisory authority, such as data breach notification and consultation prior to processing.
- Note: Data controller /processor registration will no longer be required

Clarity: Subject Access Requests

- New timeline: 30 days to respond
- Much less scope to push back and refuse to respond to access requests.
- And now, processors may be directly asked to respond to a subject access requests by a data subject.

Clarity: Right to Erasure

- An individual will have an explicit right to have their personal data removed from a controller/processor's system and/or online content.
- The controller shall be obliged to ensure erasure of the data without undue delay.
- A good example is where they withdraw consent and no other legal ground for processing applies.
- Alongside this obligation is one to take reasonable steps to inform third parties that the data subject has requested the erasure of any links to, or copies of, that data.
  - These third parties must then also comply themselves!

Clarity: Privacy by Design

Privacy by Design: The principle

- Privacy by Design and by Default (Article 23).
- Requires that data protection is designed into the development of business processes for products and services.
- Privacy settings are set at a high level by default.

Privacy by Design: How it will work

- Data Protection Impact Assessments (Article 33) have to be conducted when specific risks occur to the rights and freedoms of data subjects.
- Risk assessment and mitigation is required and a prior approval of the DPA for high risks.
- Responsibility of the Data Protection Officers.

Clarity: Data Portability

Portability of Data

- A right that would enable data subjects to transfer their personal data in a commonly-used electronic format from one data controller to another without hindrance from the original controller.
- Requirement to provide personal data to the data subject in a commonly used format.
- Where feasible, the controller may even be required to transmit the data directly to a competitor.
- Aim: Make the data transfer process from one service provider to another easier.

Clarity: Personal Liability…

Personal Liability? Maybe…

- Interpretation point: GDPR state that Member States may impose criminal sanctions for infringements of the Regulation.
- This broadens scope of potential concerns for Boards / Management / etc.

Clarity: Mandatory DPO appointment

- Organisations which regularly or systemically gather or process data will be required to appoint a Data Protection Officer

What's Next? What Now?

Call to Action and an Action Guide

Call to Action!

- **Prepare now** for the GDPR, don't wait and see, be proactive
- **Comply where possible**, but remember: cultural change is vital
- **Embrace** the GDPR where it doesn't hurt your business and consult where it does
- **Remember** that the GDPR may also serve as an enabler rather than as an obstacle

Action Guide: Review Current Data

Review Current Procedures, Training & Technologies

- Existing Data is covered under the Regulation
- Identify:
  - Where all data is stored
  - Procedures for data transfers
  - All outsourcers (including cloud services, approved & shadow)
  - Security policies
  - Training of employees
  - Technologies deployed to secure, track and report

Action Guide: Collecting New Data

- Inform all new users of the purpose for data collection
- Users must opt-in to that collection
- Information must be clear & not hidden
- No automatic opt-in, no pre-ticked boxes
- Only use data for purpose it was collected
- Do not demand opt-in or restrict users' access to a service
- Keep data only for length of time necessary

Action Guide: Processing Data

Processes, Technologies, Legal & Contractual

- Users can demand data withdrawal at any time, what's your process?
- Reduce risk or be faced with data loss, data destruction and alteration.
- Consider access management to restrict the quantity of data available to each individual.
- Encryption can significantly reduce the risk of data loss.
- Identify all data processors and ensure that they understand joint liability.

Action Guide: Transferring Data

Review Your Data Paths, Privacy Policy

- Transfers should only occur if "necessary"
- Transfer happens as soon as data leaves the EU
- Users should be informed that data may leave the EU & allow opt-out
- EU considers eleven countries have "adequate" privacy laws, OK to transfer data there
- For transfers to other countries, there needs to be a legal contract with the recipient (E.g.. Data Processor)
- Responsibility cascades down, every transfer inherits the privacy clauses

Action Guide: Deleting Data

Procedure for data deletion

- Users can demand data be deleted
- Data should be deleted routinely if it is not needed any longer
- Do you have a process?
- How do you ensure deletion from all data stores?

Action Guide: In event of Data Loss / Breach

Comprehensive Plan Required - Led By Senior Management

- How do you know you may have had a breach?
  - IT needs to be able to investigate data breach
- You have 72 hours to inform the Regulator
  - Users must be informed “without undue delay”
- Communication to users; how, when, who owns?
- Encryption: Removes many of these issues

Action Guide: Maintaining Records

Prove Your Processes

- The Data Controller must keep accurate records; Demonstrate that you understand the regulation
- Where did a record come from? When was it entered into the system? What will it be used for?
- Prove that the user accepted terms
- Which Data Processors are you using?
  - Show that you informed data processors of their responsibilities
  - What technical measures and safeguards are in place?
- Show your internal procedures, what training is in place?

EU GDPR – Crossovers with other standards

Further reading

Other References

Sources of privacy best practice and certification:

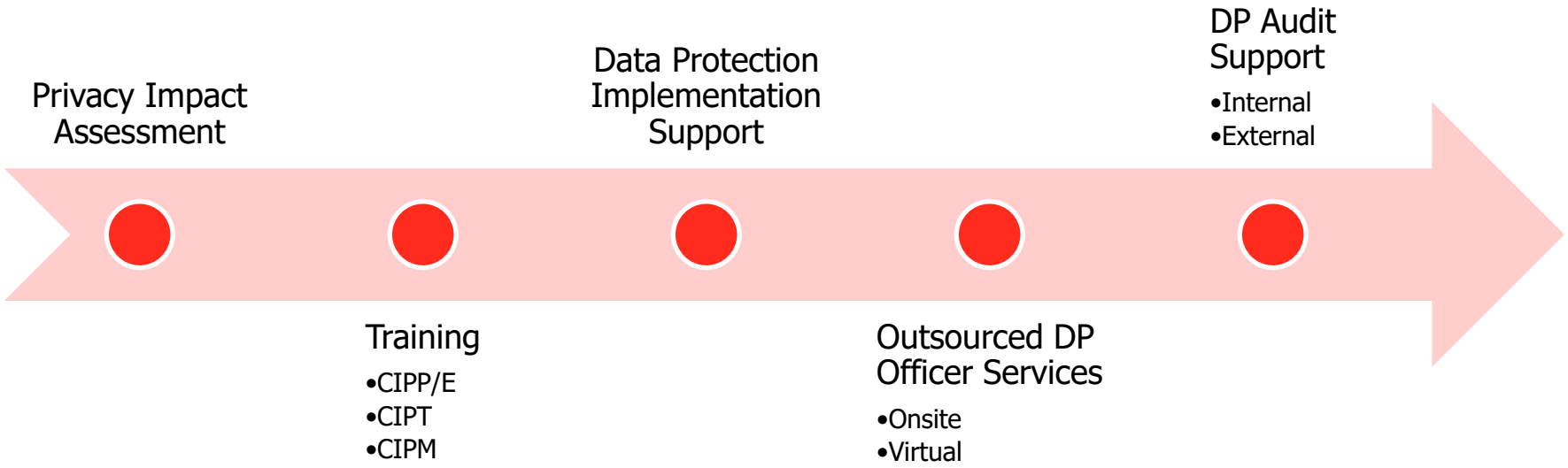
- BSI 10012 - Personal information management system
- ISO 29101 – Privacy Architecture Framework (including 11 global privacy principles which align with EU / Irish data protection rules)
- ISO 22307:2008 - Privacy impact assessment

Other References

EU GDPR White Paper

GDPR

GDPR Services Timeline



bsi.

For more information

W: espiongroup.com

E: info@espiongroup.com

T: IRE +353 1 2101711 / UK +44 845 050 1711