GDPR – AN OVERVIEW

Disclaimer

- This presentation is my personal opinion it is not legal advice and specific legal advice should be sought

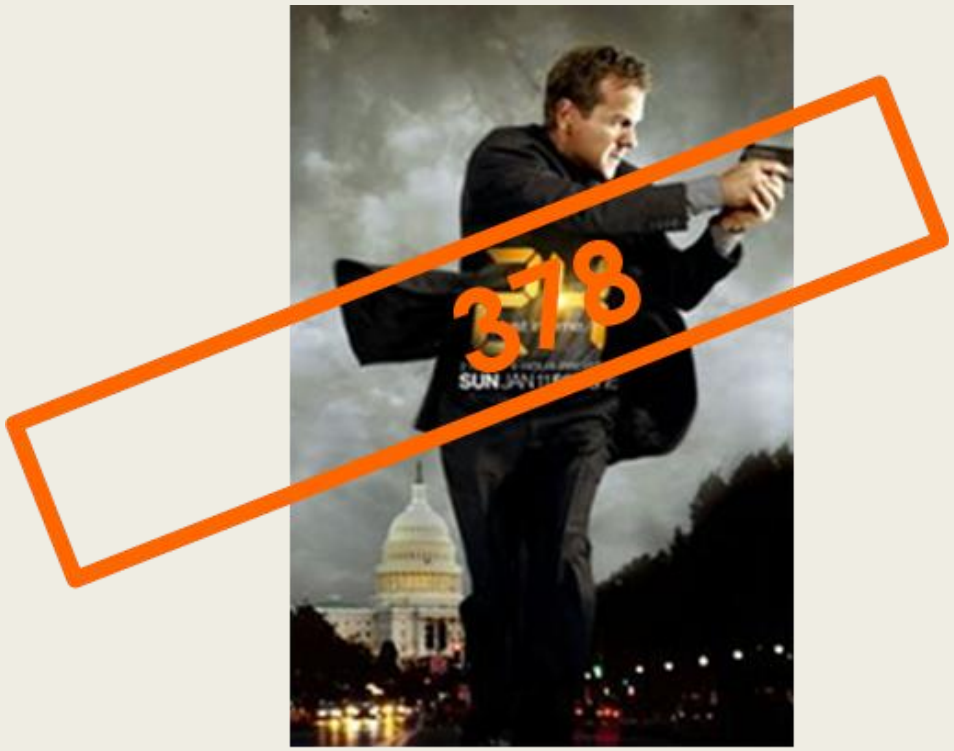
Overview

- What is GDPR
- How will GDPR affect your organisation
- How can you prepare your organisation for GDPR

What's Been Going On?

- Data Breaches
- Hacking
- Spying/ "microwaving"
- Terrorism
- The untrained
- The uncaring
- Big Data
- Information Sharing
- IOT etc
- Blockchain

https://www.tickcounter.com/countdown/1527195600000/europe-helsinki/dhms/F5F5F56B09806B09806B0980/TIME_TO_GDPR



Source: http://www.imdb.com/title/tt0285331/

The Law (well the main Irish ones)

- Data Protection Act 1988
  - *1995 EU Directive on Data Protection*
- Data Protection (Amendment) Act 2003
  - *1988 Act and 2003 Act together called "DPA"*
- The main players
  - *Personal data*
  - *Data subjects (YOU, a customer, your children, your family but not your dead relatives)*
  - *Data controllers ("Control")*
  - *Data processors ("Subject to the controller")*
  - *Sub-processors (Usually helping the processors")*
  - *Data Protection Commissioner (DPC)*
  - *Everyone else – third parties*

WHAT IS GDPR?

- General Data Protection Regulation
- 25th May 2018 - Effective immediately
- Increasing the rights and access to rights for YOU a.k.a. ‘DATA SUBJECTS’ – protects those little data bits of you that organisations hold
- Organisations to whom YOU give or use YOUR data much more accountable to YOU and the law
- Big fines
- Accountability

GDPR – What is it doing?

The BIG ISSUES

- What is personal data?
- Increased liability
  - *Wider audience, more accountability and larger fines*
  - *4% of turnover or €20 million*
- More rights for individuals (data subjects) including consent issues

Key Principles of GDPR

- 1) To enhance internal market dimension of data protection
- 2) Increase effectiveness of the fundamental rights to data protection and to put individuals in control of their data
- 3) Enhance the coherence of EU data protection framework

Source DG JUST

Five Key Purposes of GDPR

- 1) Strengthen Individual Human Rights
- 2)Facilitate business by simplifying rules
- 3) Remove costly fragmented administration (est €2.3 billion per annum)
- 4) Policing - protect personnel data of witnesses, victims and suspects of crime
- 5) Facilitate cross-border cooperation on the fight against crime and terrorism

Source DG JUST

Four High Levels Area of Impact

- Economic – stop fragmentation of the market due to data protection rules
- Policing – closes gaps and inconsistences in the use of personal data in the field of policing and judiciary
  - *Make cross cooperation easier*
  - *Protect victims, witnesses and suspects of crime*
- Administrative Burden – remove 27 different set of rules to be understood and applied (estimate to cost €2.3 billion per annum)
- Individual - build trust in consumer for on line activity
  - *current divergent rules makes it difficult for consumer to know, understand and exercise their rights and this is seen as an inhibitor to growth*
  - *Individuals have lost control over their data due to the sheer volume of data being shared and that individuals are not aware data is being collected*

Source DG JUST

Quick Path Through GDPR

Recitals	Rational Overview
Articles 1-4:	General provisions
Articles 5-11:	The Principles of Data Control
Articles 12-23:	The Rights of the Data Subject
Articles 24-43:	The Controller and Processor
Articles 44-50:	Transfers of Personal Data to Third Countries or International Organisations
Articles 51-59:	The Independent Supervisory Bodies
Articles 60-76:	Cooperation and Consistency
Articles 77-84:	Remedies Liabilities and Penalties
Articles 85-91:	Provisions relating to Specific Processing Situations
Articles 92-93:	Delegated Acts and Implementing Acts
Articles 94-99:	Final Provisions

Personal data

Issue	The Directive	The GDPR	Impact
Personal data This definition is critical because EU data protection law only applies to personal data. Information that does not fall within the definition of "personal data" is not subject to EU data protection law.	Art.2(a) "Personal data" means any information relating to an identified or identifiable natural person ("data subject"); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.	Art.4(1) "Personal data" means any information relating to an identified or identifiable natural person ("data subject"); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.	**The definition of personal data is, for the most part, unchanged under the GDPR.** For some organisations, the explicit inclusion of location data, online identifiers and genetic data within the definition of "personal data" may result in additional compliance obligations (e.g., for online advertising businesses, many types of cookies become personal data under the GDPR, because those cookies constitute "online identifiers")

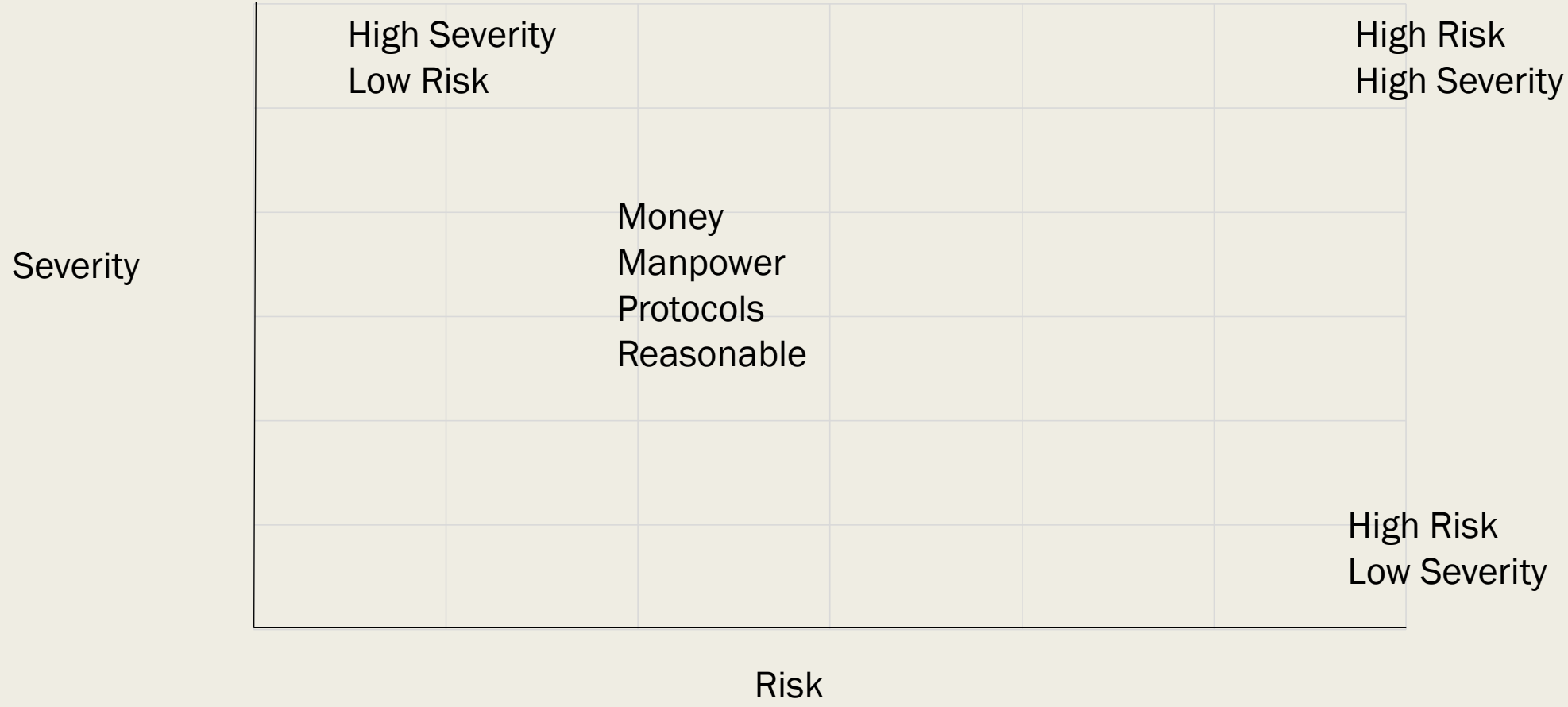
Legal Basis for Processing Personal Data

- Contractual
- Legal Obligations
- Vital Interest of the data subject
- Public Interest
- Consent
- Legitimate Interest of the Data Controller

The 7 Principles of Data Protection

The personal data shall be:

1. Obtained and processed lawfully, fairly and in a transparent manner
2. Collected for a specific, explicit and legitimate purpose
3. Adequate and relevant without being excessive for the purpose for which it was collected and collated
4. Accurate and if necessary altered so as to keep same up to date
5. Must not be kept longer than necessary
6. Processed with appropriate security and
7. The Data Controller must be able to demonstrate accountability with the principles outlined in 1-6



Examples:
Washers - €2; €20; €200
Spray gun
Washing machine
Commercial Aircraft

What are the main Rules to use Personal data

Main Rules for information:

1. Obtain personal data fairly
2. Fairly process data
3. Consent
4. Legitimate interest
5. Retaining and deleting data
6. Are there Legal and contractual obligations

Case Study 1

- Accountancy Practice
  - *Gains new customer for accounts side of the business*
  - *Has signed letter of engagement*
  - *Sends welcome email and advising of contact details and support for service and some advice re upcoming tax dates and changes– no permission sought in letter of engagement*
- GDPR – contract in place but can't be expected to cover every eventuality and has not been updated to include email contact. However, contact of legitimate interest and clearly connected to contracted service.
- Could be made better by
  - *1) Including permission to email in letter of engagement*
  - *2) Providing both an opt in and opt out on the email*

Case Study 2

- Accountancy Practice
  - *Gains new customer for accounts side of the business*
  - *Has signed letter of engagement*
  - *Sends welcome email offering Life Insurance, Investments and/or pensions*

- Under GDPR – this is likely to be a breach
  - *Letter of engagement with company not person*
  - *Email not related to the service contracted for –namely company accounts*
  - *Need persons explicit consent to send emails re these topics*

Smurfit Executive Development

UCD Michael Smurfit Graduate Business School

Dear Dara,

UCD Smurfit Executive Development would like to continue to keep you informed on our range of programmes, courses and events. Under GDPR (General Data Protection Regulation) this requires that we secure your consent by May 25th 2018.

Using the link below, please confirm that you would like to continue receiving this information. You will be able to unsubscribe at any time.

In the form, you also have an opportunity to update your information in our database which we would encourage you to do.

Please click on this link to access the form:
https://docs.google.com/forms/d/e/1FAIpQLSdYbVyC1gO-pnT-SjE27j0QrgY8ua6q8_kxEuEkgcbLhoryhw

How information about you will be used?

We retain your information to personalise our service. We would like to continue to send you information about our programmes, courses and events that may be of interest and expect to contact you no more than twice per month. We keep all academic records on file as a statutory requirement. UCD Smurfit Executive Development does not share your information with any third parties for marketing purposes.

Many thanks for taking the time to complete this and we look forward to keeping in touch with you in the future.

Yours sincerely

Data Protection 2018: We would like to continue sending you occasional marketing messages. If you no longer wish to receive our SMS Freetext OPTOUT to 50123

GDPR – What is it doing?

- Paperwork: Evidencing compliance - training/roll-out etc
- Process & Role (DPO)
- Changing the way we do business with data from May 2018:
  - *Privacy by Design (PbD)*
  - *Data Protection Impact Assessments (DPIA)*
- Getting up to speed with tech and consumer demand
  - *Data portability*
  - *“right to be forgotten”*
  - *Access rights – quicker, better, NOW!*

The Main Areas of Change

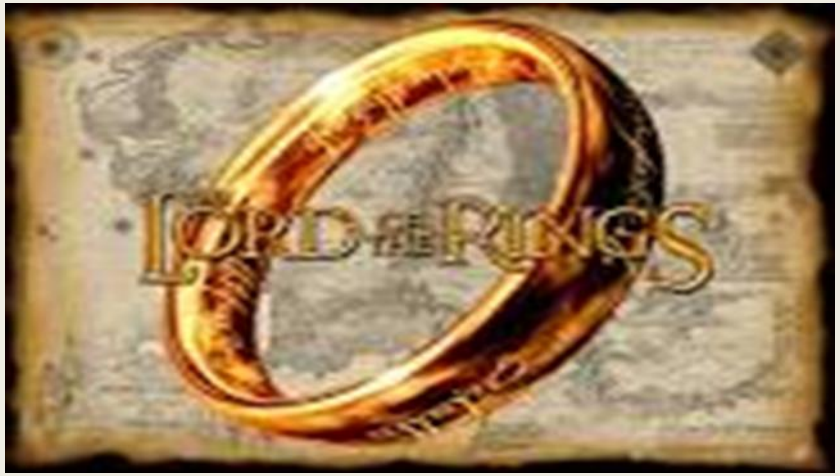
- Increased Territorial Scope
- Data Subject Rights have been extended as follows:
  - *Breach Notification – Within 72 hours to Data Protection Commission*
  - *Right to Access*
  - *Right to be Forgotten (Right to Erasure)*
  - *Data Portability*
  - *Privacy by Design*
  - *Data Protection Officers*
  - *Penalties*
  - *Right of rectification and objection*
  - *30 day compliance and no charge*
  - *Exceptions for receivers appointed under the Companies Acts 2014*
- Consent

Consent Obligations

Issue	The Directive	The GDPR	Impact
The concept of "consent" is foundational to EU data protection law. In general, the validly obtained consent of the data subject will permit almost any type of processing activity, including Cross-Border Data Transfers.	Art.2(h) "The data subject's consent" means any freely given, specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed.	Rec.25; Art.4(11) "The consent of the data subject" means any freely given, specific, informed and unambiguous indication of his or her wishes by which the data subject, either by a statement or by a clear affirmative action, signifies agreement to personal data relating to them being processed.	The GDPR makes it considerably harder for organisations to obtain valid consent from data subjects (see Chapter 8). For organisations that rely on consent for their business activities, the processes by which they obtain consent will need to be reviewed and revised to meet the requirements of the GDPR

One Law, One Rule, One-Stop Shop

SOUNDS FAMILIAR?



Source: everysinnerhasatagline.blogspot.com

One “law” to rule them all and one “law” to find them. One “law” to bring them all and in the darkness bind them

Building Trust with Data Use

- Organisations build trust with their customers by:
  - *1) Being upfront and transparent about how data will be used*
  - *2) Giving customers control over their data*
  - *3) Offering fair value for the use of their data*

- However beware

‘The more people value data the more they expect in return for it’

‘Customer Data Designing for Transparency & Trust’ May 2015 HBR.ORG

Morey & Schoop

What You Can do to Prepare

- Manage Your Data
  - *Can you easily erase data completely – systems, back-ups*
  - *Supply the details of data held on request*
  - *Explain and show how data is being used*
  - *Know individuals right over their data*
- Procedures – detection and reporting of breaches – ‘tell it all, tell it fast, tell the truth’ – ICO UK
- Perform Data Privacy Impact Assessment on High Risk Processing activities
- Data Policy Documents – Privacy, Retention, Access & Consent

What You Can Do to Prepare cont

- Staff Training & Awareness
- Do You Need Data Protection Officer
- Differentiate Your Data
  - *Personal Data – CV's, RFQ's*
  - *Suppliers*
  - *Client Related Data*
    - Current, Lapsed business
    - Marketing
  - *Employee Related Data*
- Audit & Document Your Data
  - *Where it is originated from*
  - *Where and how it is stored*
  - *How it is processed*
  - *Who it is shared with*

Three Things to begin today to get Ready for GDPR

- 1) Create/Identify/Start Policy Documents around Data Retention, Use, Privacy & Access
- 2) Map the data journey – know the source, contact points, storage and when, where and how data changed, updated, deleted – may also include third party data
- 3) Document all of above and decisions reached and ensure all relevant staff/personal up to speed on rules

GDPR in one sentence

- Under GDPR we are moving
  - From asking for Forgiveness not Permission
    - To
      - Asking for Permission not Forgiveness
- You need to be upfront about what of my data you want, why you want it and how you are going to use it

Summary

- GDPR legislation will come in to effect on 25th May 2018
- You need to assess what data you currently have in your organisations
- Put plans in place to prepare for this legislation – it's coming in to play so don't be caught out
- Raises standards of Data Protection and protects all those little bits of me

DARA@DARAKEOGHCONSULTING.EU