GDPR - Are you ready?

Anne-Marie Bohan and Michael Finn – 24 March 2018

Matheson Ranked Ireland's Most Innovative Law Firm
Financial Times 2017

International Firm in the Americas
International Tax Review 2017

European Financial Services Tax Deal of the Year
International Tax Review 2017

UCITS Law Firm of the Year
The Hedge Fund Journal 2017

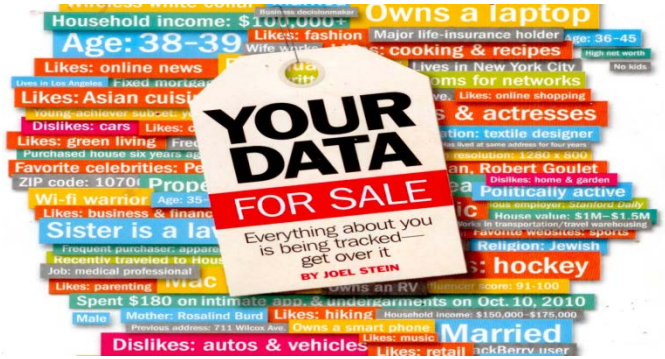
Introduction

- The current regime
- Some common challenges
- Introducing the GDPR
- What the GDPR means for you
- Obligations of Data Controllers
- Data Subjects' Rights
- Dealing with a Data Breach
- Fines and Liabilities
- Getting GDPR Ready

The Current Regime

- Governed by the Data Protection ("DP") Acts 1988 to 2003
- Implemented the DP Directive (95/46/EC)
- Applies to "Data Controllers" and "Data Processors"
- Relevant to:
  - "Personal Data"
  - "Sensitive Personal Data"

'Sensitive personal data' includes data as to "the physical or mental health" of a living individual



Your current obligations

- Registration with the Data Protection Commissioner
- Adhere to data protection principles:
  - Obtain and process information fairly
  - Keep it for one or more specified lawful purposes
  - Process it only in a manner compatible with those purposes
  - Keep it safe and secure
  - Keep it accurate and up to date
  - Ensure that it is adequate, relevant and not excessive
  - Retain it for no longer than is necessary
  - Give a copy to the individual on their request

Common themes and challenges faced by dentists

- ICO Study, June 2014 to June 2015:
  - Confusion around when a dentist should register with DPC
  - Lack of security measures (eg: reception desks)
  - Lack of written contracts with service providers, eg: IT contractors
  - Risk of new technologies, mobile phones and personal devices
  - Data retention policies not always in place

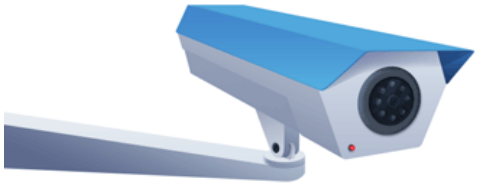
Introducing the General Data Protection Regulation…

- http://gdprandyou.ie/

Introduction to the GDPR

- The General Data Protection Regulation (the "GDPR") is the first new EU-wide DP legislation for over 20 years
- The DP Directive was conceived in early 1990s, when there was:
  - No internet
  - No smartphones
  - No social media
  - No search engines
  - No cybercrime
  - No artificial intelligence

Introduction to the GDPR



Range of data creation sources

(CCTV, biometric, internet use, mobile device use, email, Wi-Fi, travel…)

Sources

Data flows into entities and is processed across a range of services and relationships

Increasing potential for disputes

Third parties may use rights and threats of sanction & penalties tactically

Introduction to the GDPR

- **Objective:** a single, uniform set of data protection rules applying across the EU
- **Basic concepts** – are similar to current legislation
- **Timing:** GDPR applies in all EU Member States from 25 May 2018
- **Get ready:** Need to start now, if not already started
- ICGP Guidance

Basic concepts still the same…

Illustrative Example – Dental Practice

- GDPR applies to all personal data
- Dental Practice: employees, partners, contractors, job applicants, patients (including minors), suppliers & service suppliers, business contacts, experts, advisors, insurers, etc.

Basic concepts still the same…

- GDPR applies to data processed by automated means, as well as manual data forming part of a filing system
- Processing must be fair and transparent; information required is more onerous under GDPR
- Personal data must only be collected for specified, explicit and legitimate purposes
- Personal data must be adequate, relevant and limited to what is necessary for the purpose for which they are processed

Basic concepts still the same…

- More onerous obligations for "*special categories of personal data*" – similar to existing provisions on "*sensitive personal data*"
- Retain personal data for no longer than necessary (then anonymise or delete)
- Put in place appropriate security measures
- Ensure that processing is legitimate by falling within one of the permitted processing grounds (eg, consent, preventative medicine, medical diagnosis, provision of health treatments etc)

Key Changes – In Brief

- Much higher penalties – up to €20m or 4% of undertaking's global turnover if more
- Liability for material and non-material breach
- Broader scope – wider data subject rights
- Accountability and transparency
- More granularity and procedures
  - More information for data subjects
  - More compliance documentation – policies and processes, records of processing
  - Identify and record legal basis for processing

Controllers' Additional Duties under the GDPR

- Maintain detailed record of processing activities and security measures
- Data protection by design – and default
  - Must build data protection into system design (eg, new CRM system) and processes
  - Minimise data collected
  - Third party contracts
- Data controller must:
  - comply with data protection principles (as currently) **and** demonstrate compliance

Information (Privacy Notice) for Data Subjects

- Information to be provided includes:
  - legal basis for processing
  - retention periods
  - data subject rights (including right to withdraw consent and to object to processing)
  - complaint procedure
- Information (privacy notice) must be:
  - Concise, intelligible and easily accessible
  - Transparent

GDPR Data Subject Rights – Delete it, Freeze It, Correct It!

- Right to access data
- Right to rectification, if inaccurate
- Right to erasure (be forgotten) - various conditions but, in general
  - if unlawful (eg: consent withdrawn)
  - processing no longer necessary
  - dispute over "legitimate grounds" basis for processing
- Rights to restrict (freeze) processing
- Right to object (eg: direct marketing, research, etc.)

GDPR Data Subject Rights – New Right to Portability

- Right to receive data which data subject provided to a controller in a *"structured, commonly used and machine readable format"* and to have it transmitted to another data controller.
  - Dental Council Code of Practice – Art 9.3
  - What implications does this have for transferring electronic dental records?

GDPR Data Subject Rights – Subject Access Requests

- 30 day response time, with extension right of up to 2 further months where requests are complex or numerous
- Similar to current arrangements but more information to be given re:
  - Storage period
  - Right to request rectification or to object
  - The recipients of the data, etc.

- Right of controller to refuse (or charge) if manifestly unfounded or excessive

Data Breaches under the GDPR

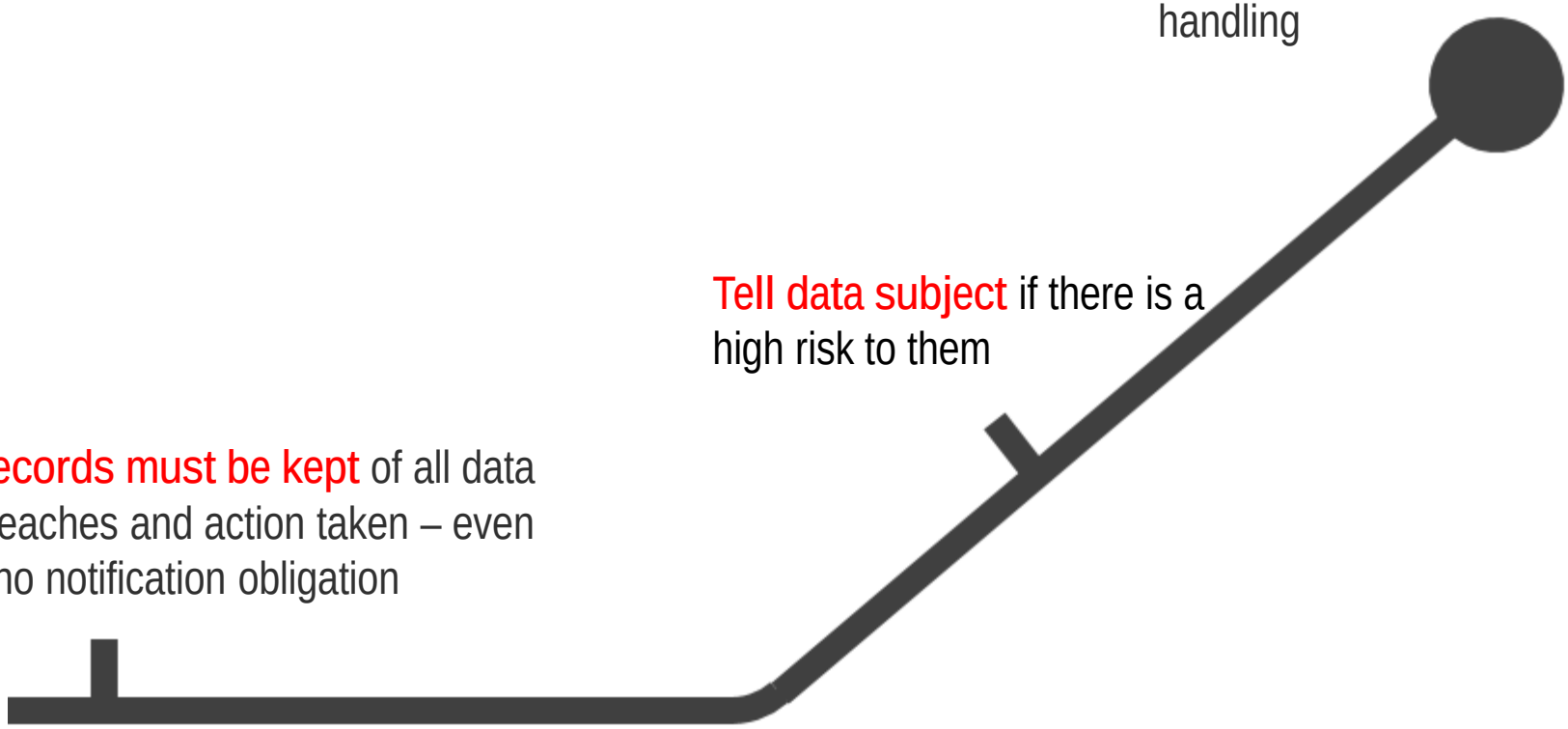
- Breach of security leading to accidental or unlawful data destruction, loss, alteration or unauthorised disclosure
- Notify DPC promptly and within 72 hours
- If late notification - provide a *"reasoned justification"* explaining the delay
- In notifying a breach, describe:
  - what happened
  - approximate numbers of individuals affected
  - likely consequences
  - measures taken or proposed
- Must inform data subject if breach = “high risk” to their rights

Data Breaches under the GDPR

Data breaches not uncommon – short time frame…need clear policies on handling

Tell data subject if there is a high risk to them

Records must be kept of all data breaches and action taken – even if no notification obligation



Penalties under the GDPR

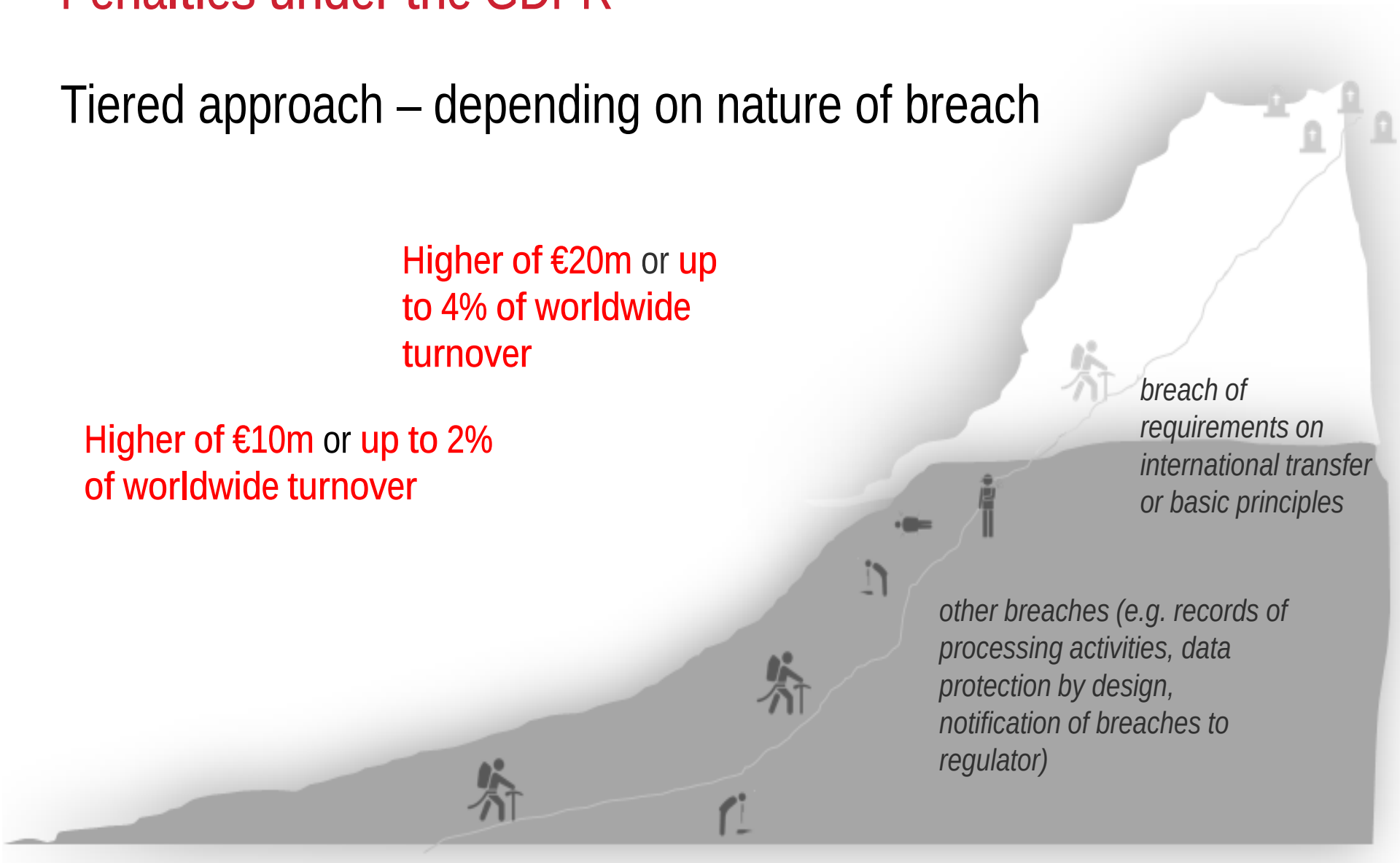
Tiered approach – depending on nature of breach

Higher of €20m or up to 4% of worldwide turnover

breach of requirements on international transfer or basic principles

Higher of €10m or up to 2% of worldwide turnover

other breaches (e.g. records of processing activities, data protection by design, notification of breaches to regulator)



Penalties under the GDPR

- Fines may be levied by Data Protection Commission
- Factors taken into account include:

Nature, gravity and duration of infringement

Number of persons affected

Action taken to mitigate damage

Previous record

Whether notified

Preparation of Data Controllers / Processors

Act now as preparation is necessary to achieve compliance:

Option to develop an IDA Code

- GDPR allows associations prepare Codes for approval, registration and certification with the DPC
- Adherence to Code then demonstrates compliance with GDPR
- Compliance with Code is then monitored by an “accredited body”
- If Code is breached, may be suspended from the Code and reported to the DPC

Some scenarios

Q&A