GDPR and the Construction Industry
9 February 2018

Deirdre Kilroy

Partner

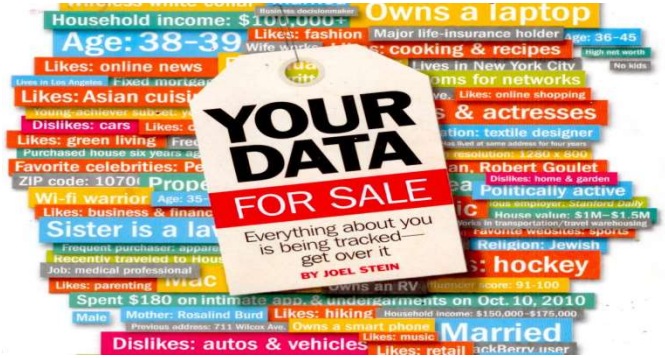
Financial Times 2012-2014
Matheson is the only Irish law firm commended by the Financial Times for innovation in corporate law, finance law, dispute resolution and corporate strategy

Irish Tax Firm of the Year 2013
International Tax Review

Client Choice 2013
International Law Office

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"



'Personal data' means data relating to a living individual who is or can be identified either from the data or from the data in conjunction with other information that is in, or is likely to come into, the possession of the data controller

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 (95/46/EC) was conceived in early 1990s, when there was:
  - No internet
  - No smartphones
  - No social media
  - No search engines
  - No cybercrime
  - No wearable technology

Introduction to the GDPR

- **Objective:** a single, uniform set of data protection rules applying across the EU
  - GDPR draft published on **25 January 2012**
  - GDPR entered into force on **27 April 2016**
  - GDPR applies in all EU Member States from **25 May 2018**

- Years of negotiation and lobbying involved

Overview of the GDPR - EU Level

- GDPR is directly effective but requires some national legislation
- GDPR sets up a "one-stop shop"
  - Common rules
  - Common approach to regulation
  - Common approach to penalties

- There are some **exceptions** to this principle (e.g., specific carve outs for national employment laws) so there will still be a need to consult national laws – really a **hybrid model**

Overview of the GDPR - National Level

- Data Protection Bill 2018 published in January 2018
- Gives further effect to the GDPR
- Deals with MS flexibility options e.g., currently takes public authorities out of the fines regime for some breaches of data protection law

Summary of the GDPR

Basic concepts – similar to current legislation

- For example: the definition of "personal data" in the GDPR in Article 4 is similar to the current definition:

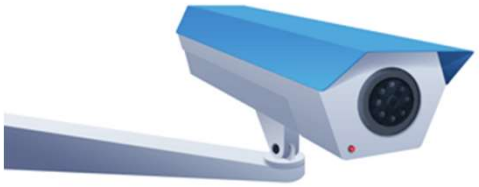
> means **any information** relating to an **identified or identifiable natural person** ('data subject'); an identifiable natural person is **one who can be identified, directly or indirectly**, in particular **by reference to an identifier** such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person

Personal data under the GDPR

Illustrative Example – Construction company

- GDPR applies to all personal data
- Construction company: employees, shareholders, contractors, job applicants, clients, suppliers & service suppliers, business contacts, estate agents, prospective buyers, advisors, insurers

Summary of the GDPR



Range of data creation sources

(CCTV, biometric, internet use, mobile device use, location/GPS data/wearable technology, 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

Summary of the GDPR

Basic concepts – similar to current legislation

- 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

Summary of the GDPR

Basic concepts – similar to current legislation

- 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 (e.g. consent, legitimate interests, necessary for contract performance)

Key Changes – In Brief

- Much higher penalties – higher of €20m or 4% of undertaking's global turnover
- 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
- Wider data subject rights
- Data protection officers

Key Changes – In Brief

- Mandatory DP Impact Assessments
- Extra-territorial effect – applies to data controllers and processors outside EU which process EU resident data subjects' data

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

- Right to rectification, if inaccurate
- Right to erasure (be forgotten) - various conditions but, in general
  - if unlawful
  - processing no longer necessary
  - dispute over "legitimate grounds" basis for processing
- Rights to restrict (freeze) processing
- Additional rights may be useful in disputes

GDPR Data Subject Rights – Automated Decision Making

- Decision having legal effect or significant affect on data subject may not be made based solely on automated processing unless:
  - necessary for performance of contract with data subject;
  - authorised by EU or Member State law; or
  - based on explicit consent

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:
  - Retention period
  - Right to request rectification or to object
  - Safeguards on third country transfer

- Right of controller to refuse (or charge) if manifestly unfounded or excessive; creates a new lever for negotiation over information to be provided?

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 (e.g. new CRM system) and processes
  - minimise data collected
- Data controller must:
  - comply with data protection
  - be able to demonstrate compliance (i.e., reverses burden of proof)

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)
  - transfers of data outside the EU
- Information (privacy notice) must be:
  - concise, intelligible and easily accessible
  - transparent

Data Protection Officers ("DPO") under the GDPR

- Required if:
  - core activities involve systematic monitoring
  - large scale processing of special categories of data
  - a public body (except courts)
  - specified by national laws
- Main obligations under the GDPR:
  - inform and advise controller / processor and employees about GDPR obligations
  - monitor compliance
  - training and raising awareness
  - point of contact for regulator

Data Breaches under the GDPR (1)

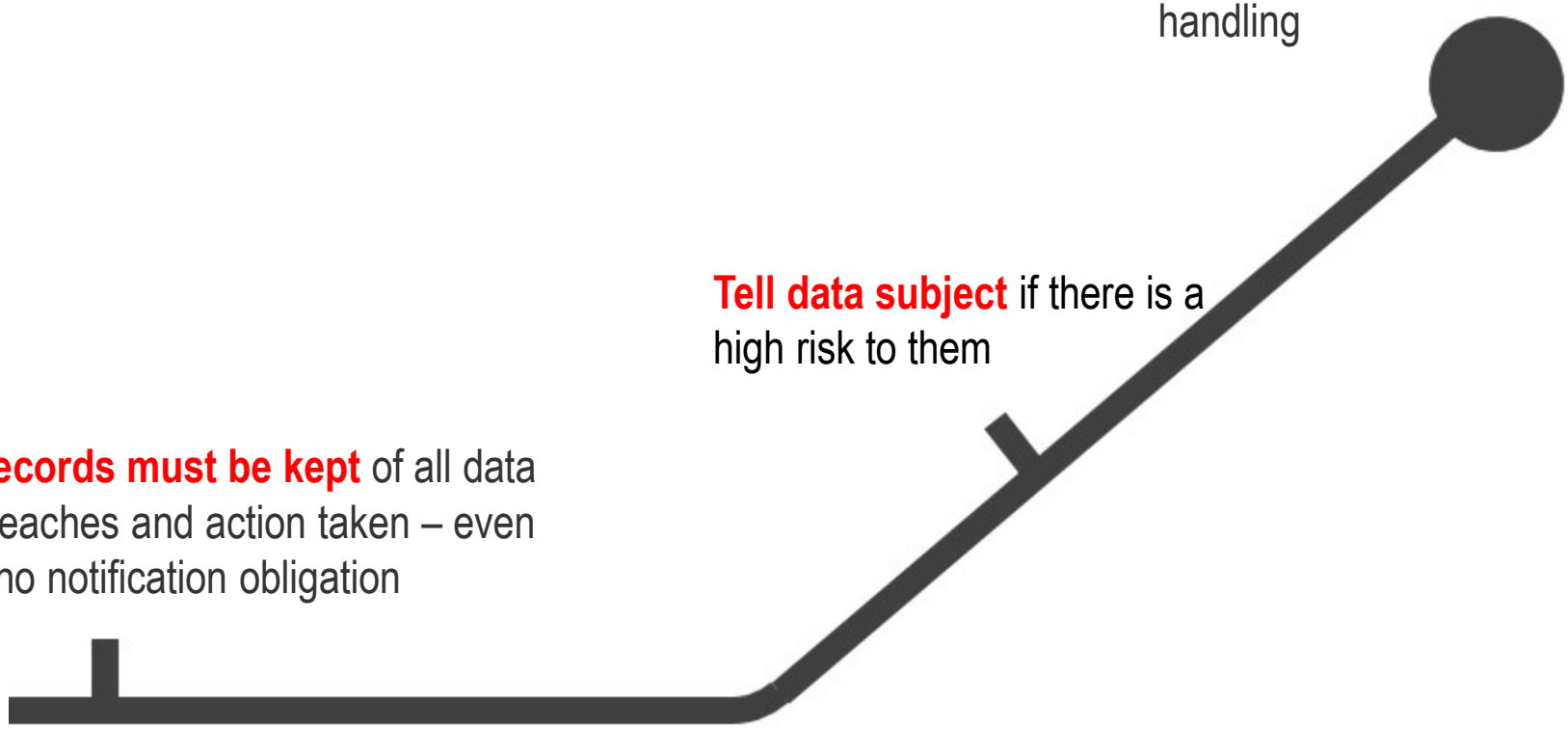
- Breach of security leading to accidental or unlawful data destruction, loss, alteration or unauthorised disclosure
- Notify lead authority promptly and within 72 hours unless breach unlikely to result in a risk (e.g., all data encrypted)
- If late notification - provide a "reasoned justification" explaining the delay
- In notifying a breach, describe:
  - what happened
  - approximate numbers of individuals affected
  - likely consequences
  - measures taken or proposed

Data Breaches under the GDPR (2)

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



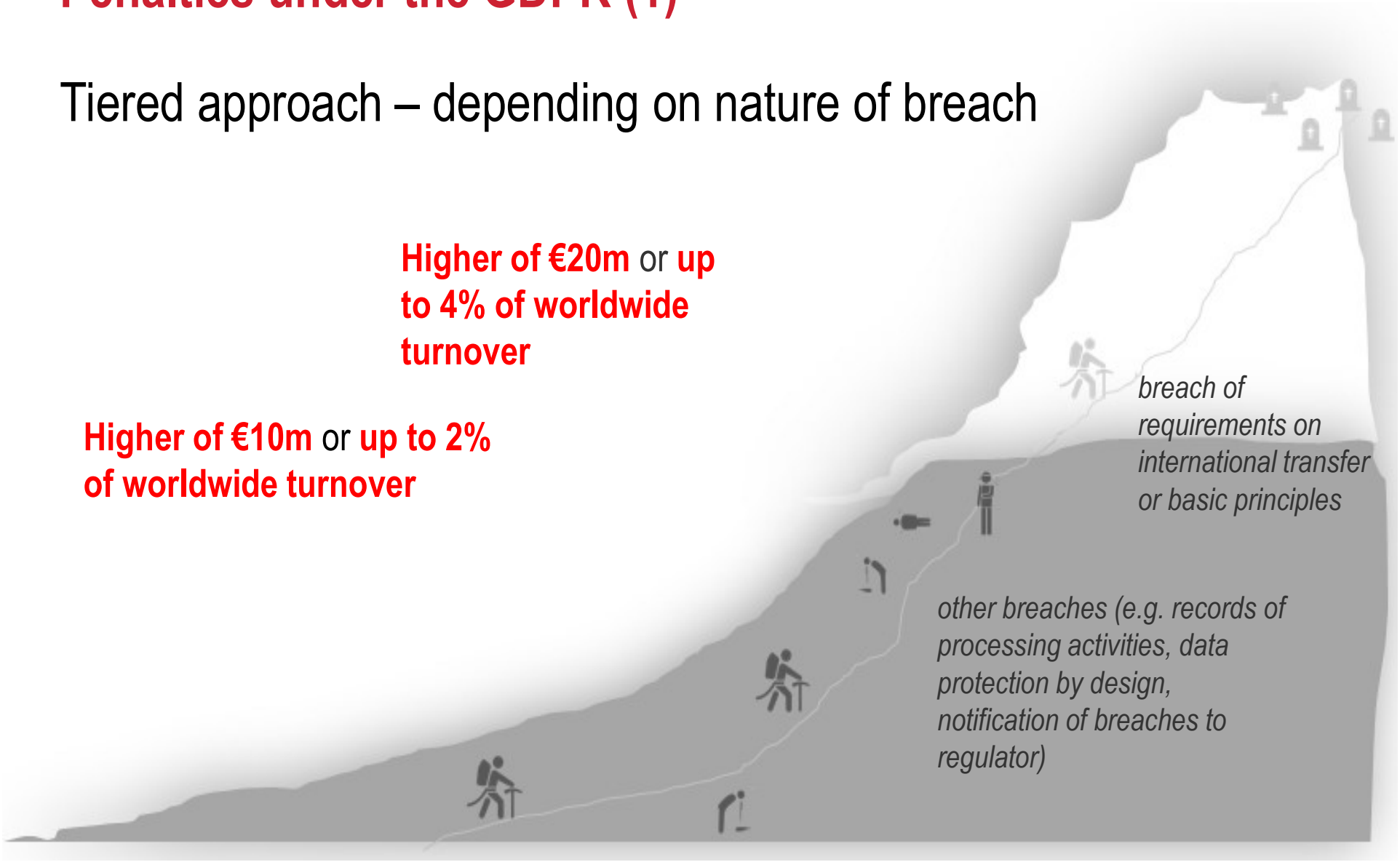
Matheson

Penalties under the GDPR (1)

Tiered approach – depending on nature of breach

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

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



Penalties under the GDPR (2)

- Fines may be levied by Data Protection Authorities
- 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:

Where can I get Further Information?

- Ireland
  - The Data Protection Bill
  - Data Protection Commissioner Guidance – ongoing
- EU
  - Article 29 Working Party Guidance – ongoing
  - EU Commission GDPR webpage – updated regularly
- UK
  - UK Information Commissioner – Brexit updates

Any Questions?

Deirdre Kilroy
Partner
Matheson
70 Sir John Rogerson's Quay
Dublin 2

@DeirdreKilroy
T: +353 1 232 2331
F: +353 1 232 3333
E: deirdre.kilroy@matheson.com
W: www.matheson.com