GDPR: what should you be doing now?

Denis Kelleher,
BCL, BL, LLD, Barrister-at-Law.
Disclaimer

Deliver this presentation in a personal capacity and set out my own personal views; not those of any other person.

Not giving legal advice; if you want legal advice then seek it specifically & separately from your own legal advisor.
What I will talk about today:

• Where is the legislation now?
• When should you care about GDPR?
• What should you be doing now?
  – Can you demonstrate compliance?
  – Governance - appointment of DPO;
  – Security – what are your risks/safeguards?
    • Have you procedures in place to notify/admit liability?
• Why should you care about GDPR?
  – Who is going to pay?
Where is the legislation now?

• Have two new EU laws:
  – **General Data Protection Regulation (GDPR)**
    • Will apply from 25\textsuperscript{th} May 2018
  – **Data Protection Directive** (Criminal Justice)
    • Must be implemented by 6\textsuperscript{th} May 2018

• **Heads of Data Protection Bill** have been published.
  – Drafting underway
  – Cabinet approval of Heads still awaited
  – Bill then formally drafted
  – Back to Cabinet
  – Introduced to Dail
When should you care about GDPR?

Now

(this is when we are in transition)
Criminal Justice (Money Laundering and Terrorist Financing) Act 2010

• Implemented Directive 2005/60/EC (should have been enacted before 15 December 2007)
• Enacted on 5th May, 2010
• Commenced on 15 July 2010
• Guidelines issued by the Department of Finance in February 2012
• Substantially amended by Criminal Justice Act 2013
When did the transition period for implementing the *Criminal Justice (AML) Act 2010* end?

Was it:

– 15 July 2010 (when the Act commenced)?
– February 2012 (when the Department of Finance issued its guidance)?
– Between June 2013 & March 2014 when the *Criminal Justice Act 2013* amendments were commenced?
“The Central Bank of Ireland... fined... the Bank of Ireland... €3,150,000 and reprimanded it for twelve breaches of the Criminal Justice (Money Laundering & Terrorist Financing) Act, 2010 (the ‘CJA 2010’). The breaches occurred from the enactment of the CJA 2010 in July 2010 and persisted on average for over three years.”

“The Central Bank of Ireland... fined Allied Irish Banks... €2,275,000 and reprimanded it for six breaches of the CJA 2010... The breaches occurred after the enactment of the CJA 2010... and persisted on average for over three years”.
Controllers are accountable

“The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 (‘accountability’)”

Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary.

Controllers may need to implement their own policies and comply with codes of conduct.

Article 5(2)

Article 24 GDPR
New accountability mechanisms

1. Structural
   - Appoint DPO (Data Protection Officer) (Arts 37-39)
   - Co-operate with DPC (Art 31)
   - Joint controllers (Art 26)/processors (Art 28 & 29)

2. Operational
   - Data protection by design and default (Art 25)
   - DPIA (Art 35)
   - Prior consultation (Art 36)
   - Create records of processing activities (Art 30)
   - Report security breaches to DPC and subjects (Arts 33 & 34)
DPO – who needs one?

Controller and processor designate DPO if:

1. Public authority (other than court);
2. Core activities ‘...require regular and systematic monitoring of data subjects on a large scale...’;
3. Core activities ‘...consist of processing on a large scale of special categories of data... and personal data relating to criminal convictions and offences’.

Can have same one for group of controllers

– employee;
– service provider.

Article 37, GDPR
DPO – What do they do?

1. 'inform and advise' controller;
2. 'monitor compliance... including the assignment of responsibilities, awareness-raising and training of staff... and... audits’;
3. 'provide advice' on DPIA and implementation;
4. 'cooperate with the supervisory authority’;
5. 'act as the contact point for the supervisory authority... consult, where appropriate, with regard to any other matter’.

Must '... have due regard to the risk associated with processing operations, taking into account the nature, scope, context and purposes of processing’.

Article 39, GDPR
DPO – where do they work?

Controller and processor designate DPO if:

1. Public authority (other than court);
2. Core activities ‘...require regular and systematic monitoring of data subjects on a large scale...’;
3. Core activities ‘...consist of processing on a large scale of special categories of data... and personal data relating to criminal convictions and offences’.

Estimate about 36,000 needed in EU
- seems low.

Can have same one for group of companies
- employee;
- service provider.
DPO – who are they?

DPO must be:

1. ‘...involved, properly and in a timely manner, in all issues which relate to the protection of personal data’.

2. Provided with ‘...resources necessary to carry out those tasks and access to personal data and processing operations, and to maintain his or her expert knowledge’.

3. ‘...bound by secrecy or confidentiality concerning the performance of his or her tasks’.

4. Can do other work, but employer must '...ensure that the data protection officer does not receive any instructions regarding the exercise of those tasks‘ and cannot be '...dismissed or penalised...’.

Contact details made public/sent to DPC
DPO – What do they do?

1. 'inform and advise' controller;
2. 'monitor compliance... including the assignment of responsibilities, awareness-raising and training of staff... and... audits’;
3. 'provide advice' on DPIA and implementation;
4. 'cooperate with the supervisory authority’;
5. 'act as the contact point for the supervisory authority... consult, where appropriate, with regard to any other matter’.

Must '... have due regard to the risk associated with processing operations, taking into account the nature, scope, context and purposes of processing’.
Report '...directly report to the highest management level'
'The data protection officer shall be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfil the tasks…'.
Duty to secure

1. Take into account the following:
   a) state of the art;
   b) costs of implementation;
   c) nature, scope, context and purposes of processing;
   d) risk of varying likelihood and severity for the rights and freedoms of natural persons.

2. Then controller and processor must: ‘implement appropriate technical and organisational measures’

3. To: 'ensure a level of security appropriate to the risk'.

Article 32, GDPR
Appropriate measures

a) the pseudonymisation and encryption of personal data;
b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services
c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.
Risk assessment

• In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

• The controller and processor shall take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller, unless he or she is required to do so by Union or Member State law.
GDPR forces controllers to admit they have failed

“In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority…. unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons”
Why should we care about GDPR?

Three good reasons:

1. Illegality;
2. Fines; and
3. Liability.
Illegality

GDPR requires that data be processed lawfully:
- “Personal data shall be... processed lawfully...” (Article 5(1) GDPR)
- “Processing shall be lawful only if and to the extent that at least one of the following applies...” (Article 6(1) GDPR)
- “Personal data shall be... processed lawfully...” (Head 28(1)(a))

Consequences:
- May not be able to use in court/legal proceedings;
- DPC has power to impose temporary or permanent suspension of processing;
- Fines; and
- Liability.
Administrative fines

'Each supervisory authority shall ensure that the imposition of administrative fines... shall in each individual case be effective, proportionate and dissuasive'.

Imposed in addition to or as alternative to corrective measures such as bans, rectification...

Take various factors into account:
• intentional or negligent character of the infringement;
• efforts to mitigate damage;
• history of controller/processor;
• did controller notify DPC?
Category 1 fines

Up to 2% of global turnover or €10m in respect of the following breaches:

1. Obligations of controllers – DPO, DPIA etc
2. Processing of children’s data
3. Failure to effectively anonymise data
4. Breach of certification rules
Category 2 fines

Up to 4% of global turnover or €20m in respect of the following breaches:

1. Basic principles of processing
2. Subject rights
3. Transfers outside EEA
4. Rules around processing in context of employment, by journalists, or FOI
5. Breach of a ban on processing
Actions for damages

'Any person who has suffered **material or non-material damage** as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered'.

Article 82, GDPR
Class actions?

The data subject shall have the right to mandate a not-for-profit body, organisation or association:

1. properly constituted in accordance with the law of a Member State
2. has statutory objectives which are in the public interest
3. is active in the field of the protection of data subjects' rights and freedoms

To lodge the complaint... and... exercise the right to compensation... on his or her behalf where provided for by Member State law.

But see: Persona Digital Telephony Ltd [2017] IESC 27 (23 May 2017)
Who is going to pay?
Joint controllers:

'... shall in a transparent manner determine their respective responsibilities for compliance with the obligations under this Regulation...’.

'The essence of the arrangement shall be made available to the data subject’.

Article 26, GDPR
Processors

• '...the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures...'

• 'Processing by a processor shall be governed by a contract or other legal act... That contract or other legal act shall stipulate, in particular, that the processor:
  – '...processes the personal data only on documented instructions from the controller...‘

• 'The processor and any person acting under the authority of the controller or of the processor... shall not process those data except on instructions from the controller...‘.
What must be in this contract?

a) Processor will process personal data only on documented instructions from the controller,
b) Confidentiality
c) Takes security measures
d) not engage another processor without prior written authorization
e) assists the controller to respond to requests from subjects
f) assists the controller in ensuring compliance with DPIA etc
g) deletes at the end
h) makes available to the controller all information necessary to demonstrate compliance with GDPR.
2. Any controller involved in processing shall be liable for the damage caused by processing which infringes this Regulation. A processor shall be liable for the damage caused by processing only where it has not complied with obligations of this Regulation specifically directed to processors or where it has acted outside or contrary to lawful instructions of the controller.

3. A controller or processor shall be exempt from liability under paragraph 2 if it proves that it is not in any way responsible for the event giving rise to the damage.
Joint & several liability

4. Where more than one controller or processor, or both a controller and a processor, are involved in the same processing and where they are, under paragraphs 2 and 3, responsible for any damage caused by processing, **each controller or processor shall be held liable for the entire damage** in order to ensure effective compensation of the data subject.

5. Where a controller or processor has...paid full compensation for the damage suffered, that controller or processor shall be entitled to **claim back** from the other controllers or processors involved in the same processing that part of the compensation corresponding to their part of responsibility for the damage...
Thank you