The GDPR: what does it mean for controllers?

Denis Kelleher,
Senior Legal Counsel,
Legal Division.
Data protection is not privacy

“Everyone has the right to respect for his or her private and family life, home and communications”

Article 7, EU Charter of Fundamental Rights
What is data protection?

1. Everyone has the right to the protection of personal data concerning him or her.

2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.

3. Compliance with these rules shall be subject to control by an independent authority.

Article 8, EU Charter Fundamental rights
Why do we need the GDPR?

“Cambridge Analytica says it has as many as 3,000 to 5,000 data points on each of us, be it voting histories or full-spectrum demographics — age, income, debt, hobbies, criminal histories, purchase histories, religious leanings, health concerns, gun ownership, car ownership, homeownership — from consumer-data giants....

Because the United States lacks European-style restrictions on second- or third-hand use of our data, and because our freedom-of-information laws give data brokers broad access to the intimate records kept by local and state governments, our lives are open books even without social media or personality quizzes”

Why has the EU enacted the GDPR?

• Existing Directive dates back to 1995:
  • Did not anticipate technologies such as the internet (not to mind social media & smart phones);
  • Or globalisation; and,
  • Lacked effective supervision & enforcement regime.

• New GDPR addresses these defects:
  • Grant EU data protection laws a global jurisdiction;
  • Creates new supervisory structures; and,
  • Provides new enforcement mechanisms

• Enacts rules that determine how personal data is controlled and processed within EU.
  • Directly effective; but with,
  • Some Member State discretions.
Where are we now?

• GDPR enacted in May 2016
• GDPR in force now and will apply from 25 May 2018
  • Most, almost certainly all MS will bring in Implementing legislation;
  • But not required, GDPR is a Regulation.
• Have new Data Protection Directive
  • Will apply to criminal justice.
• Proposal for new ePrivacy Regulation
• More expected under Digital Single Market (DSM)
  • 'Bringing down barriers to unlock online opportunities'.
  • Fintech
One (over-simplified)-slide guide

1. Is it personal data?
   - Does it relate to a living person whom you can identify?

2. Do you have a Legitimate basis for processing it?
   - consent/contract, legal, legitimate interest

3. Do you comply with principles?
   - inform subject of processing, don’t process further than required for legitimate purpose

4. **Do you comply with controller/processor rules?**

5. Do specific rules apply?
   - sensitive, telcos, journalist/artistic, international data transfer

6. You must respect subject rights
   - access, rectification/erasure, objection, automated processing

7. Enforcement – role of national DPAs
There is a lot in the GDPR:

I do not have time to talk about:

1. Consent of children;
2. “Hyper-bureaucratic” European Data Protection Board;
3. Powers and duties of DPC; and
Today’s talk

1. Tweaks to duties & rights
2. The new supervisory regime
3. Global jurisdiction of the GDPR.
4. Other laws.
Updates to lawfulness/criteria

Same as before:
• Contract/consent;
• Legal obligation;
• Public interest/official authority task;
• To protect vital interests of subject;
• Legitimate interests of controller/third party unless overruled by rights of subjects (esp Children).

But:
• Legitimate interest cannot be invoked by public bodies;
• Legal obligations or public tasks have to be laid down by law which must:
  • Meet objective of public interest;
  • Be proportionate to legitimate aim pursued.
• If the Bank wishes to process personal data then it will need to do so pursuant to a specific statutory power.

Also limits on processing of criminal records
Changes to Principles!

1. Lawfulness, fairness and transparency
2. Purpose limitation
3. Data minimisation
4. Accuracy
5. Storage limitation (controller cannot be forced to de-anonymise data – Art 11)
6. Integrity and confidentiality
7. Accountability

‘The controller shall be responsible for, and be able to demonstrate compliance…’
Updating of subject rights

Rights must be considered as whole:

1. Information
2. Access
3. Rectification
4. Erasure (right to be forgotten)
5. Restriction (new!)
6. Portability (new!)
7. Object
8. Not to be subject to automated decision making
9. Not to be subject to profiling (new!)
Changes to “modalities” (Art. 12)

• No fees (unless “manifestly unfounded or excessive”);
• Shorter time periods (one month, though can be extend by further two).

Rights of rectification, restriction and to be forgotten require telling recipients (Art 19):

“The controller shall communicate any rectification or erasure of personal data or restriction of processing... to each recipient to whom the personal data have been disclosed, unless this proves impossible or involves disproportionate effort. The controller shall inform the data subject about those recipients if the data subject requests it”
Profiling

‘... any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements’. 
Automated decision making (Art 22)

‘The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her’.

Does not apply if:

• Authorised by law
• Contract/consent

‘...the data controller shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision’.

Limits on use of sensitive personal data
EU & Member States can restrict subject rights under Article 23

Article 23 sets out two sets of restrictions:

1. “respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society to safeguard...important objectives of general public interest of the Union or of a Member State, in particular an important economic or financial interest of the Union or of a Member State, including monetary, budgetary and taxation a matters...a monitoring, inspection or regulatory function connected, even occasionally, to the exercise of official authority ”

2. Restrictions must specify: purpose of processing, categories of data, types of controllers, safeguards, retention periods, etc.
Why care about the GDPR?

New supervisory mechanisms
New supervisory procedures

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)
Co-operation with DPA (Art 31)

'The controller and the processor... shall cooperate, on request, with the supervisory authority in the performance of its tasks.'
Joint controllers (Art 26)

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’.
Processors

Article 28:
• '...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...'

Article 29:
• '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...‘.
Record keeping (Art 30)

• 'Each controller... shall maintain a record of processing activities under its responsibility...'
  • Purposes of processes
  • Description of categories of subjects and data
  • Description of categories of recipients
  • Retention periods
  • International transfers
  • Security measures – 'where possible'

• Provide to DPC on request

• Obligation does not apply to SME (<250):
  'unless the processing... is likely to result in a risk to the rights and freedoms of data subjects... processing is not occasional, or the processing includes special categories of data'.
Data protection by design (Art 25.1)

• Controller must:
  • at the time of the determination of the means for processing
  • and at the time of the processing itself

• Take the following into account:
  • state of the art
  • cost of implementation
  • nature, scope, context and purposes of processing
  • risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing

• And then ‘...implement appropriate technical and organisational measures‘:
  • such as pseudonymisation

• ‘...which are designed to implement data-protection principles...‘:
  • 'such as data minimisation'

• This must be 'effective' and '... integrate the necessary safeguards into the processing'. This must be done:
  ‘...in order to meet the requirements of this Regulation and protect the rights of data subjects’.
Data protection by default (Art 25.2)

Obligation of minimisation:

• 'The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed'.

Obligation applies to:

• amount of personal data collected
• extent of processing
• period of storage
• accessibility

One specific obligation, controllers must:

'...ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons'.
DPIA

• Take into account:
  • the nature
  • scope
  • context
  • purposes

• Of the processing and in particular whether it’s a type of processing using new technologies and decided whether it:
  ‘...is likely to result in a high risk to the rights and freedoms of natural persons...’.

• Then 'prior to the processing' the controller must:
  ‘...carry out an assessment of the impact of the envisaged processing operations on the protection of personal data’.
DPIA is required

Where processing is:

(a) a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;

(b) processing on a large scale of special categories of data or of personal data relating to criminal convictions and offences; or

(c) a systematic monitoring of a publicly accessible area on a large scale.

DPC must publish list of the kind of processing operations which are subject to the requirement for a DPIA
DPIA is in two parts

Analysis:

1. A systematic description of the envisaged processing operations including:
   • the purposes of the processing
   • where applicable, the legitimate interest pursued by the controller
2. an assessment of the necessity and proportionality of the processing operations in relation to the purposes, and
3. an assessment of risks to the rights and freedoms of data subjects.

Response: measures envisaged to address the risks, including:
   • safeguards
   • security measures
   • other mechanisms

Which should:

'...ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned'.
Prior consultation

Article 36: If DPIA indicates '...processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk' then controller must contact national DPA.

• If DPA thinks processing ...would infringe this Regulation

• Particularly where '...insufficiently identified or mitigated the risk

The DPA shall (w/in 8 weeks):

• Provide written 'advice' to controller/processor

• May extend by 6 weeks

• Time will stop if DPA waiting for information.
Why care about the GDPR?

New enforcement mechanisms
Responsibility & Accountability

Article 24 – Responsibility of data controller

1. '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’

2. Controllers may need to implement their own policies and

3. comply with codes of conduct.

Article 5(2)

Accountability is now a principle of data protection
Article 82

• '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’.

• Any controller involved in processing shall be liable for the damage caused by processing which infringes this Regulation. Processors liable:
  1. only where it has not complied with obligations of this Regulation specifically directed to processors, or
  2. where it has acted outside or contrary to lawful instructions of the controller.

• Neither liable if can prove '... not in any way responsible for the event giving rise to the damage’.

• Joint liability for controller and processors.
Class actions (Art 80)

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.
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’.
Breach notification to DPC

• 'personal data breach' means:
  '... a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed'.

• If a controller suffers one of these:
  'controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it'.

• Notify DPC (explain delay if one has occurred)
Notification to subject

• If breach '... likely to result in a high risk to the rights and freedoms of natural persons...'
• Must communicate to subject 'without undue delay'.
• Notification should 'describe in clear and plain language' the consequences of breach, controller’s response and details of DPO.
• Do not have to notify if:
  1. used encryption or similar
  2. controller’s response has ensured risks to data 'no longer likely to materialise'
  3. 'would involve disproportionate effort’
• DPC may require that notification be given to subjects.
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?

Set at 2% - breach of DPO, DPIA, child, ineffective anonymisation
Or 4% - breach of basic principles, subject rights, trans-border etc.,
Trans-border data flows
Privacy Shield

• Safe Harbor struck down by CJEU a year ago
  • Furious negotiations followed
  • Agreed this summer

• Many DPAs want to challenge Privacy Shield
  • Art 29 Committee has given it a year
  • Evidence US firms waiting to see what happens
Three judgments

• One given:
  • *Watson/Davis C-698/15*
    Challenge to national data retention laws

• New *Schrems*
  • Challenge to approved contractual clauses
  • Still before Irish High Court
  • Won’t be referred to CJEU before next year, if at all

• *Canadian PNR (CJEU Opinion 1/15)*
  • AG opinion negative
The GDPR’s global jurisdiction (Art 3)

1. GDPR '... applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not‘.

2. GDPR '... applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:
   - the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or
   - the monitoring of their behaviour as far as their behaviour takes place within the Union.
What happens to: MoU?
Conclusion

What else is there?
What other laws are there?

Legislation:
1. Data Protection Directive – criminal justice (AML)
2. ePrivacy Directive/proposed Regulation- ECN/OTT
3. Regulation 45/2001 covers EU Institutions
4. Article 39 TEU Decision (?) – Foreign & Security policy

The Court of Justice of the EU (CJEU); developing own case-law:
• *Mac Fadden*;
• *Breyer*.

European Court of Human Rights.
Thank you