FRONTIER privacy

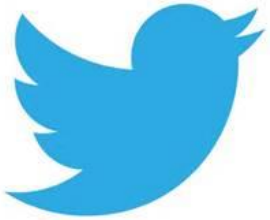
The General Data Protection Regulation:

Aoife Sexton

20 September 2017

Why the need for a new law?

- No update to the principal EU data protection legislation since 1995
- (Mark Zuckerberg was 11)
- Many new technological developments and increasing digitilisaton
- Arrival of social media
- Law outdated


It’s all got out of hand…

Data brokers collect more than 50 trillion unique data transactions per year

82% of Android apps track your other online activities

If you read all of the terms of service for all of your apps it would take 76 days

PayPal’s Terms of Service is 36,275 words long: that’s longer than Hamlet

‘Free’ online services are ‘paid for’ using personal data which have been valued in total at over EUR 300 billion

Sources: IDC, European Data Protection Supervisor, Marc Goodman: *Future Crimes*, Carnegie Mellon University

Why the need for a new law?

THE GDPR IS A GOOD THING..

- Law designed to result in single, uniform set of data protection rules across the EU
- Principles based legislation - Technology neutral – Although not much detail on the “How”

- Implementation date: 25 May 2018

The GDPR is not simply an IT or security issue..
….BUT there is a role for technology in the GDPR

Information Governance

What personal data do I have, where is it, how sensitive is it,
why do I have it, do I have consent to use it, can I delete it, etc.

Meeting Specific Requirements

RTBF, Consent, Encryption, Data Portability,
Record keeping, incident response, etc.

Review State of the Art

“appropriate technical and organisational measures”
Encryption, backup & restore, testing, access control, etc.

The role of technology in GDPR

Meeting Specific Requirements

RTBF, Consent, Encryption, Data Portability,
Record keeping, incident response, etc.

Article 30 requires (unless less than 250 employees and no Special Category of personal data processed)

- Name and contact details of the controller, joint controller , controller's representation and DPO
- Purposes of Processing
- Description of the categories of data subjects and the categories of personal data
- Categories of recipients to whom the personal data is or will be disclosed including recipient in third countries
- Details of transfer to third countries
- Where possible the envisaged time limits for destruction of different categories of data (retention schedule)
- Where possible, a general description of the technical and organisational measures used to secure the ongoing confidentiality , integrity availability and resilience of the systems.

Main Changes: New & enhanced rights for individuals

- Today: Individuals have certain rights under the DP Acts.
- Change : Individuals have new and enhanced rights under the GDPR. Rights below will apply in certain circumstances.
  - Maintained: Right to rectification
  - Enhanced: Right to Erasure/Right to be forgotten
  - New: Right to restrict processing
  - Enhanced: Right to object to processing
  - New: Restrictions on individuals being subject to decisions based solely on automated processing
  - New: Data portability of personal data provided to the controller

Requests by data subject to be actioned by controller without undue delay or at least within 1 month

- Subject Access Rights – Increased obligations on Controllers
  - Individuals have right to request access to a copy of their personal data which request may be refused only under GDPR where the request is "**manifestly unfounded or excessive**" (Today- it is "**disproportionate effort**")
  - Change in time period to deal with request reduced from Today @ 40 days to GDPR 1 month
  - Change in fees charged : Today it is €6.35 but under GDPR no charge

The brave new world of outsourcing

Controllers v Processors

- Today: 90/10

- Change: 60/40

Impact on Outsourcing: New Obligations (and legal exposure) for Processors

- Today: Processors compliance obligations are principally with the terms of the Controller-Processor agreement rather than statutory obligations under the DP Acts. Controllers are legally responsible for breaches of the Data Protection Acts caused by their processors.
- Change: GDPR imposes **direct** statutory obligations on processors. GDPR makes controller and processors jointly and severally liable for ensuing damage caused by the breach of their respective obligations.

- Today: DP Act only has limited detail on the terms of a controller-processor contract. These include the need for the following;
  - a written contract,
  - for processor to follow the instructions of the controller; and
  - for processor to take appropriate technical and organisational measures to ensure data is kept secure.
- Change: Article 28(3) GDPR is more prescriptive on the mandatory terms to be inserted in a controller-processor contract

Main Changes: Direct statutory obligations on Processors

- The controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of the GDPR and ensure the protection of the rights of the data subject.

- Change: Article 28- Direct statutory obligations on a processor including
  - To not engage a sub-processor without controller's prior written authorisation
  - Only process data on instructions of the controller
  - To implement appropriate technical and organisational measures
  - To notify controller of data breaches without undue delay of becoming aware of the breach
  - To maintain records of processing
  - Cooperate with Supervisory Authority
  - To appoint a DPO, as required
  - To ensure that transfers to third countries are lawful
  - Red flag to the controller any controller instruction in the processor opinion that breaches the GDPR

Main Changes: Contractual Clauses

- Article 28(3) Contract must set out the
  - subject matter and duration of processing,
  - nature and purpose of the processing,
  - type of personal data and categories of data subject; and
  - obligations and rights of the controller.

- Article 28(3) GDPR: Processor must contractually
  - only process data on documented instructions from controller including transfers to third countries
  - ensure that staff have committed themselves to confidentiality
  - implement appropriate security and organisational measures
  - only subcontract with prior written authorisation of controller
  - assist controller with responding to requests of data subjects
  - assist controller with data breach notifications to SA, data subjects as well as conducting DPIA's.
  - delete or return data etc. at the choice of the controller at the end of the contract
  - provide information to demonstrate compliance and permits audits and inspections conducted by controller and auditors.

Main Changes: Contractual Clauses

- Processor must cascade the same GDPR contractual data protection obligations down to its subprocessors, in particular ensuring sufficient guarantees on the implementation of requisite security measures.
- Processors will be fully liable for subprocessors breach of DP obligations
- No grandfathering of existing contracts that run past 25th May, 2018

GDPR IS A GAME CHANGER FOR PROCESSORS

- Change: This means that for processors, they now face 3 possible actions arising from breach of their GDPR processor obligations
  - action by the controller for breach of the controller processor agreement
  - direct action by a data subject or by consumers through a group privacy claim
  - direct fines by supervising authority for breach of the GDPR e.g. ODPC.

The bad news for Processors…..

The good news for Processors….

Frontier Privacy- What we do

Innovative data protection consultancy firm delivering a complete range of data protection services in Ireland and internationally.

- The first essential step- A Privacy Assessment + Report (with action plan to achieve compliance)

Range of Services

- Bespoke Training
- Drafting of Policies & protocols
- Data Protection Impact Assessments (DPIA)
- Advice on Employer-related issues
- Advice on Marketing & databases
- Advice on Outsourcing and Cloud computing
- Advice on Controller –Processor Contracts
- Advice on International Data Transfers
- Outsourced Data Protection Officer (DPO)

FRONTIER
privacy

Aoife Sexton

Co-Founder & Director

asexton@frontierprivacy.com

T: +353 1 639 2935

www.frontierprivacy.com

*

This presentation contains general information. This presentation is not intended to constitute legal advice and therefore should not be relied on as such