UWE Bristol | University of the West of England

Presentation by

John Rugg

Engineer.net

An Introduction to the General Data Protection Regulation (GDPR)

24 January 2017

1. What's happening?

- It's a new EU Regulation
- It applies from 25 May 2018 across the EU
- It causes the EU Data Protection Directive to be repealed, and thereby also the UK Data Protection Act (1998) derived from it
- The 'Article 29 Working Party' which currently provides EU data protection advice, will be replaced with the European Data Protection Board (EDPB)
- The Information Commissioners Office will be our supervisory authority
- It will affect the way we process personal data.
- The maximum level of fines will be eye watering

We will need to get busy.

2. Can we get out of it?

No

3. Just one regulation…

- Containing **99 articles**
- Underpinned by **173 recitals** (the reasoning behind the articles)
- Totaling 88 pages

Sometimes the recitals can conflict with the articles. Clarification and guidance is expected from the European Data Protection Board.

However, there is much that is in common with the existing Data Protection Regulation.

4. Article 1 GDPR

‘This Regulation protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data.’

5. Fines

- Now under DPA : **Max £500,000** (TalkTalk fine)

- 2018 under GDPR: **Max €20,000,000** or 4% of total annual worldwide turnover, whichever is higher. (Article 83)

- Member states free to enact additional 'dissuasive' fines where the regulation does not already.

6. Data protection principles

Broadly unchanged, but

- Now 6 data principles (Article 5), and not 8 in the DPA
- 'Personal data shall be processed in accordance with the rights of the data subject' is no longer a principle but covered under 'Rights of the data subject', Articles 12 – 23
- Adequate protection on transfers out of the European Economic Area is no longer a principle but covered under ' Transfers of personal data to third countries or international organisations' Articles 45 – 50

a) Processed lawfully, fairly and **transparently**
b) Purpose limitation - now has default inclusions of **archiving, research and statistical purposes**.
c) Data minimisation - adequate, relevant and limited to purposes
d) Accuracy - take reasonable steps to correct errors
e) Storage limitation - kept in a form which **permits identification of data subjects** for no longer than is necessary for the purposes
f) Integrity and confidentiality - using appropriate technical or organisational measures

7. Privacy Statements

Transparent information (Article 12):

"The controller shall take appropriate measures to provide any information referred to in Articles 13 and 14 and any communication under Articles 15 to 22 and 34 relating to processing to the data subject in a **concise, transparent, intelligible and easily accessible form, using clear and plain language**, in particular for any information addressed specifically to a child. The information shall be provided in writing, or by other means, including, where appropriate, by electronic means."

8. Privacy Statements

New requirements for information (Article 13):

- Contact details of the Data Protection Officer (new GDPR role)
- The legal basis for processing
- The legitimate interests pursued by the controller or a 3rd party
- The recipients or categories of the recipients of the personal data
- Intended transfers of personal data to a 3rd country or international organisation.
- The existence of automated decision making, including profiling.
- The reason(s) personal data needs to be supplied (statute, contract), and the possible consequences of not providing it
- Subject rights to :
  - restrict or object to processing
  - withdraw consent at any time
  - data portability
  - lodge a complaint with the supervisory authority (eg ICO)

9. Consent

- Ground frequently used for processing by UWE
- Data subject has the right to withdraw consent at any time
- It shall be as easy to withdraw as to give consent.
- "'consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her; ." [Article 4]
- "explicit consent" for special categories of personal data (Article 9 - =sensitive personal data)
- implicit/explicit consent (DPA) → unambiguous/explicit (GDPR), implicit consent no longer an option (?) . Explicit consent cannot be obtained through a course of conduct, but unambiguous consent can.
- Silence, pre-ticked boxes or inactivity does not constitute consent.

10. Other grounds for processing

- [The data subject has given consent]
- Performance of a contract to which the data subject is party (eg provision of their education)
- Compliance with a legal obligation to which the controller is subject
- To protect the vital interests of the data subject or another person
- In the public interest
- Legitimate interests of the data controller.

11. Restrictions

Safeguarding:

- National security
- Defence
- Public security
- Prosecution of criminal offences etc

12. Data subject rights

- The controller should … provide means for requests to be made electronically (Recital 59)
- Data subject access response now 1 month (Article 12) not 40 days, free and generally not chargeable (Articles 12, 15)
- Remote access by data subject to their data on a secure system where possible (Recital 63)
- Article 14 – specific info to be supplied to data subject where data about them supplied by others is processed (no secret processing without cause, and risk to anonymity of sources)
- Right to erasure (Article 17)
- Right to restrict processing (Article 18)
- Right to data portability (Article 20)
- Right to object (Article 21)

Data handing arrangements should facilitate the administration of data subject rights.

13. Cookies

- GDPR considers online identifiers like cookies as personal data (Article 4).
- Unambiguous consent must be as easy to withdraw as to give
- Current implied consents to set cookies may be at risk
- May require sites to take note of 'technical settings for information society services ' (GDPR recital 32) (eg Do Not Track)

- Update to the ePrivacy Directive expected, but as a Regulation
- Some argue it is superceded by GDPR
- May require 3rd party cookies to be blocked by default in browsers

14. Privacy Impact Assessments

- Now termed Data Protection Impact Assessment (DPIA)
- Required where there is high risk to the rights and freedoms of persons, including:
  - Extensive evaluation of personal aspects of people including profiling that produces legal effects upon them
  - Processing on a large scale of special categories of data.
- Should include views of data subjects where appropriate
- Lists of processing operations that both do and do not require a DPIA shall be determined by the supervisory authority (ICO), and conveyed to the EDPB.
- Unmitigated high risk processing to be referred to the supervisory authority, prior to processing.

[Article 35]

15. Records

Each controller … shall maintain a record of processing activities under its responsibility, containing

- the name and contact details of the controller and…the data protection officer;
- the purposes of the processing;
- a description of the categories of data subjects and of the categories of personal data
- the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organisations;
- transfers of personal data to a third country or an international organisation and the documentation of suitable safeguards;
- the envisaged time limits for erasure of the different categories of data;
- a general description of the technical and organisational security measures [Article 30]

16. Security

- Controller must assess 'risks of varying likelihood and severity for the rights and freedoms of natural persons' , and implement appropriate technical and organisational measures (Article 24)
- Measures to include (Article 32):
  - Pseudonymisation
  - Ability to promptly restore access to personal data after incidents
  - Regular testing and evaluation of the effectiveness of technical and organisational measures.

17. Breach reporting

- New controller obligation to report data breaches to supervisory authority within 72 hours, unless no risk to rights and freedoms of natural persons (Article 33)

  [Reporting obligation has applied to telecoms providers since 2011 under reg 5A of PECR, but otherwise new requirement]

- Inform data subjects (Article 34) in 'high risk' cases.

18. Europe

- ICO Commissioner Elizabeth Denham on Brexit
- European Commission will hopefully make an adequacy decision against UK as a 3rd party post Brexit, allowing data transfers to/from Europe without further specific authorisation. Reviewed at least every 4 years. This could be suspended at any time if the level of data protection is judged inadequate. (Article 45)
- Other possibility is data transfer subject to appropriate safeguards (Article 46)
- Liaison with other supervisory authorities?
- Resolution of disputes?
- Once outside the EU we would need a representative inside the EU, that would be legally liable for any breaches. Not clear why anyone would want this risky role.

19. Useful links

- General Data Protection Regulation (EU)
- Preparing for the General Data Protection Regulation (GDPR) 12 steps to take now (ICO)
- Privacy Notices under the GDPR (ICO)

- Guide to the GDPR (Linklaters)
- The GDPR at a glance (Linklaters)