Get ready for GDPR!

Rob Humphries

microserve
THE DRUPAL EXPERTS

What are we talking about today?

GDPR

- First a bit about me
- Whys
- Whats
- Whens
- Hows
- Any questions

A bit about me

- Background in digital PM
- Mainly large scale database and analysis tool implementations
- Now Drupal websites as Head of Production at Microserve
- How did I find out about GDPR?

Whys

Why is it being introduced?

- The key idea is to give the people more control over their data
- People are extremely trusting online
- The regulation doesn't want to stop that, but it does want to give them the option to change their mind

Why does it impact me/my clients?

- External
  - Sites with users
  - Sites with newsletters
  - Sites with form submissions
  - Preference centres (especially!)
- Internal
  - Client information (Sales, Finance)
  - Employee information (Finance, HR)

Why should I be bothered?

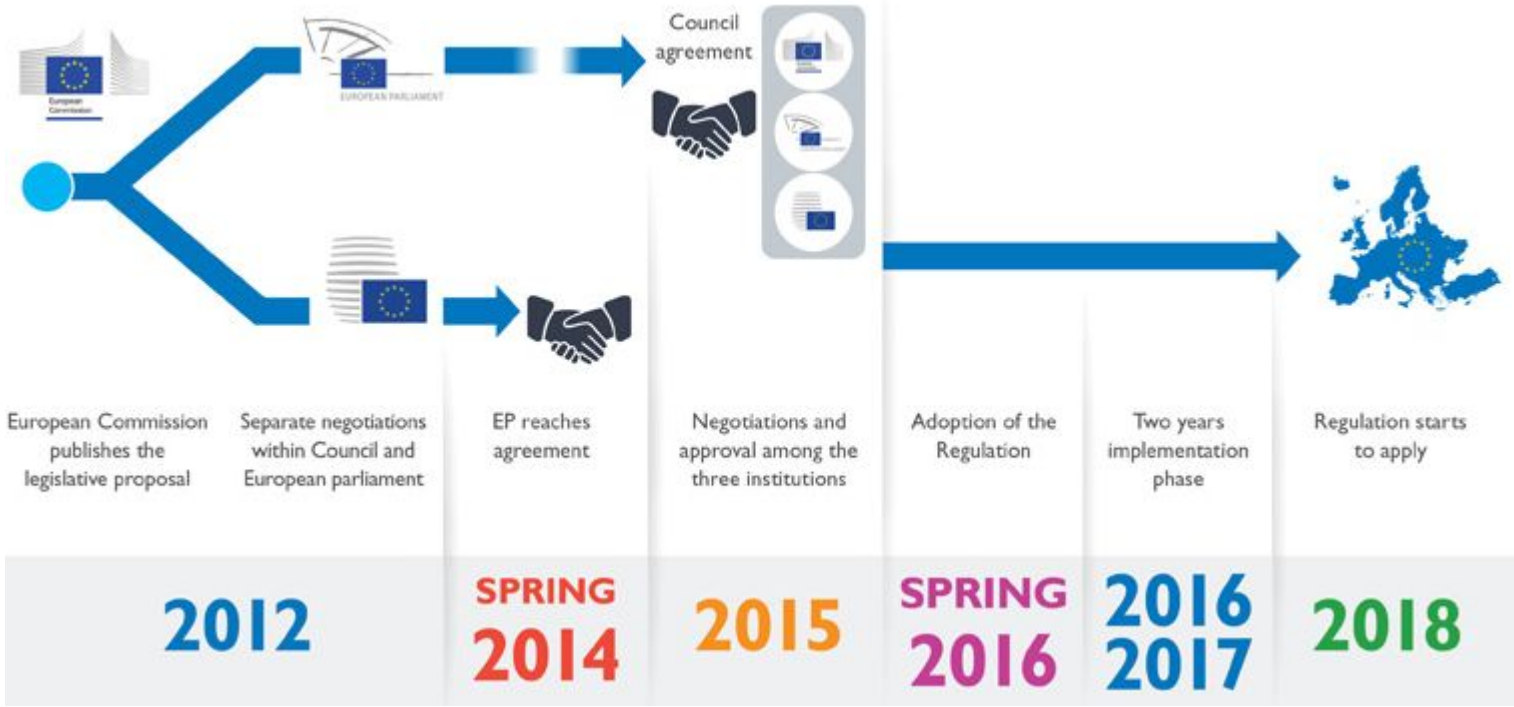
First offence: Maximum fine of €10million or 2% of worldwide turnover, whichever is higher

Second offence: Maximum fine of €20million or 4% of worldwide turnover, whichever is higher

ICO will be funded only by fines

Whats

What's the history?



What isn't it?

- It isn't the European Data Protection Directive
- A directive is not a law
- The UK introduced the Data Protection Act 1998
- The design of the directive began with OECD work in the 80's
- Things have moved on a lot

What is it?

- General Data Protection Regulation
- Replaces European Data Protection Directive
- Regulation is law
- A single set of rules for everyone
- Aims to give people more control over their personal data

What's the difference?

Area	DPD	GDPR
Scope	EU companies	Companies controlling or processing EU data subjects
Liability	Data Controllers responsible	Data Controllers and Data Processors responsible
Law	Directive is not law	Regulation is law automatically
Consent	Consent must be given by data subject	"Unambiguous" Consent must be given by data subject
Right to erasure	When inaccurate or incomplete	On data subject objection
Rights	Little mention of rights	Explicit rights on Lodging Complaints, Judicial Remedy and Compensation

What does it mean?

- There are fewer grey areas
- Responsibility is more clearly defined
- Increased rights for individuals
- GDPR is more far reaching and more enforceable than DPD
- It means business!
- So let's take a look at some of the specifics..

What are data controllers and processors?

- Controller - the company who owns the data and makes the decisions about what happens to it
- Processor - contracted by the controller to move, augment, update or even just hold the data

What is a data subject?

- 'Personal data' 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

What is a Subject Access Request?

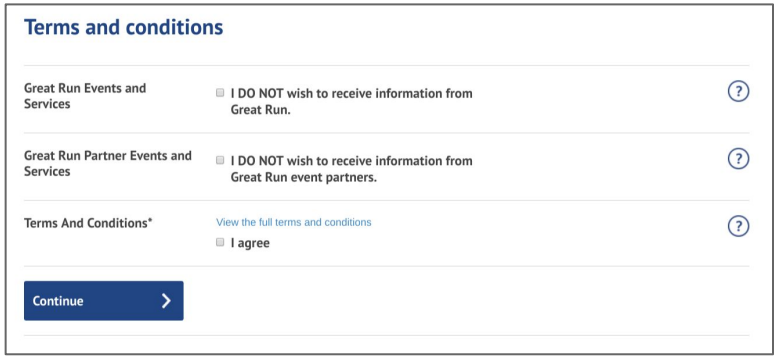
- Under GDPR this is a right of the Data Subject
- Data Subjects can ask a company to confirm if they hold or process their data
- If they do the company must confirm:
  - Which data
  - How it's being processed
  - Where they got it from
  - Where's it going
  - How long is it being retained
  - Any profiling

What can a data subject request?

- The Data Subject then has the right to request:
  - Amends
  - Erasure
  - Transfer

What about preferences?

- No more assumed consent
- Preferences must be:
  - Explicit
  - Appropriate
- Something to think about with clients running shops or newsletters



What constitutes a breach?

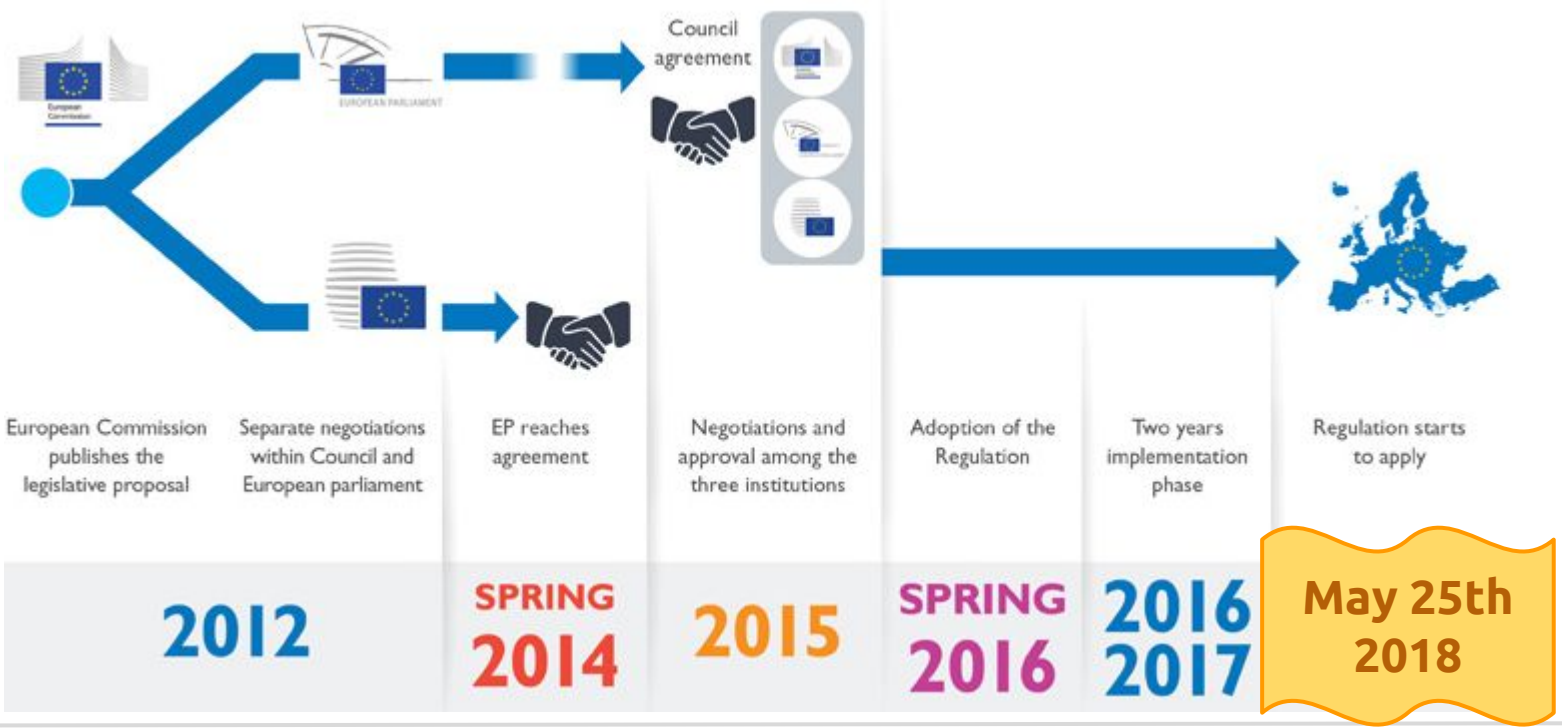
- Data being physically or digitally insecure
- The regulation being broken
- In the event of a breach we must:
  - Report to supervisory authority no later than 72 hours
  - Communicate to the data subject in case the breach is likely to cause high risk to right and freedoms of the person

What about Brexit?

- We're leaving the EU
- It doesn't matter
- GDPR will come into force before we leave
- Great Repeal Bill will probably make it law in the UK
- We shouldn't assume it won't apply
- Also it does account for third countries

Whens

When is it coming into force?



Hows

How can I make sure I am GDPR compliant?

- You can't : (
- The regulation mentions compliance, but offers no checklist
- Spirit of the law not letter of the law
- Cases will be judged on an individual basis
- You will need to be able to show that data protection and information security is a top priority for your company

How can I start to prepare?

- ICO (Information Commissioner's Office) for information
- ISO27001 Information Security compliance
- Add GDPR to the board agenda and/or ISM review agenda
- Discuss it with your clients in account reviews and question their readiness as well
- Discuss it with your suppliers (hosting, third party services (ESPs etc.)
- Plan to handle Data Subject Access Requests

Any Questions?

Summary

- Enforceable from 25th May 2018
- Big fines
- Definition of personal data has been expanded
- More rights for the individual
- No checklist for compliance
- Data Security by design

Thanks!

Rob Humphries
@thedrupalpm
rob.humphries@microserve.io

References:

- Open access to the regulation https://www.privacy-regulation.eu/en
- CIS https://cis-india.org/internet-governance/blog/comparison-of-general-data-protection-regulation-and-data-protection-directive