GDPR for WP Developers

Heather Burns // WordPress North East // 8 March 2018

What GDPR is not about

- Lawyers telling you how to code
- The EU telling you how to code
- Throwing your projects away
- FinesfinesfinesfinesfinesfinesfinesOMGfinesfinesfines

What GDPR is about:

- Thinking proactively about developing for privacy and user protection
- Adopting protective workflows and business practices
- Understanding that privacy and user protection are everyone's responsibility;
- Feeling empowered to challenge development practices which can endanger the people in the data

The changing privacy landscape

What is Europe's privacy overhaul?

- GDPR: 25 May 2018
  - Replaces the Data Protection Directive of 1995 (UK: DPA 1998)
  - Maintains original principles, expands and modernises
  - Data at rest: collection, usage, retention
- ePrivacy Directive: TBD (autumn/winter?)
  - Replaces the ePrivacy Directive of 2002 (UK: PECR 2003)
  - Data in transit: cookies, telemetry, advertising beacons, marketing

What data falls under data protection?

- **Personal data:** any information relating to an identified or identifiable natural person
- One piece of information or multiple data points combined in a record
- **Sensitive personal data**: information about racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health data, sex life or sexual orientation, past or spent criminal convictions
- New definitions: genetic data, biometric data, and **online identifiers**

Who does it apply to?

- All data collected, processed, and retained about persons within the European Union
- Extraterritorial: applies to non-EU businesses
- All businesses: no minimum size or turnover
- All situations: public sector, private sector, academia, startup, or corporate

Why does that matter?

UK and Europe

- Privacy is a fundamental human right
- Data belongs to the subject
- One overarching law for all member states and sectors
- Not tied to citizenship or nationality
- Privacy is its own law
- Culture of constructive cooperation before litigation

US

- Free speech is a fundamental human right
- Data belongs to the owner
- No overarching DP law; piecemeal approach across sectors and states
- Tied to citizenship and nationality
- Privacy is a subcategory of contract or property law
- See you in court

But what about…you know what…

Privacy compliance after Brexit

GDPR 2018 – 2020 (at least)

- European privacy law is extraterritorial
- The UK is going into GDPR **regardless of Brexit**
- Data Protection Bill

After the divorce (2020ish - ?)

- What happens down the road?
- Will anti-European spite overrule common sense?
- Will the UK move towards a US-style, market-driven (e.g. write your own rules) regulatory system?

Prepare for the European privacy overhaul as if Brexit was never happening

Once you are there, do not budge

How does your development workflow need to change?

Your changing development workflow

How you *work*

- Privacy by Design
- Privacy Impact Assessments
- Consent mechanisms
- Training and CPD

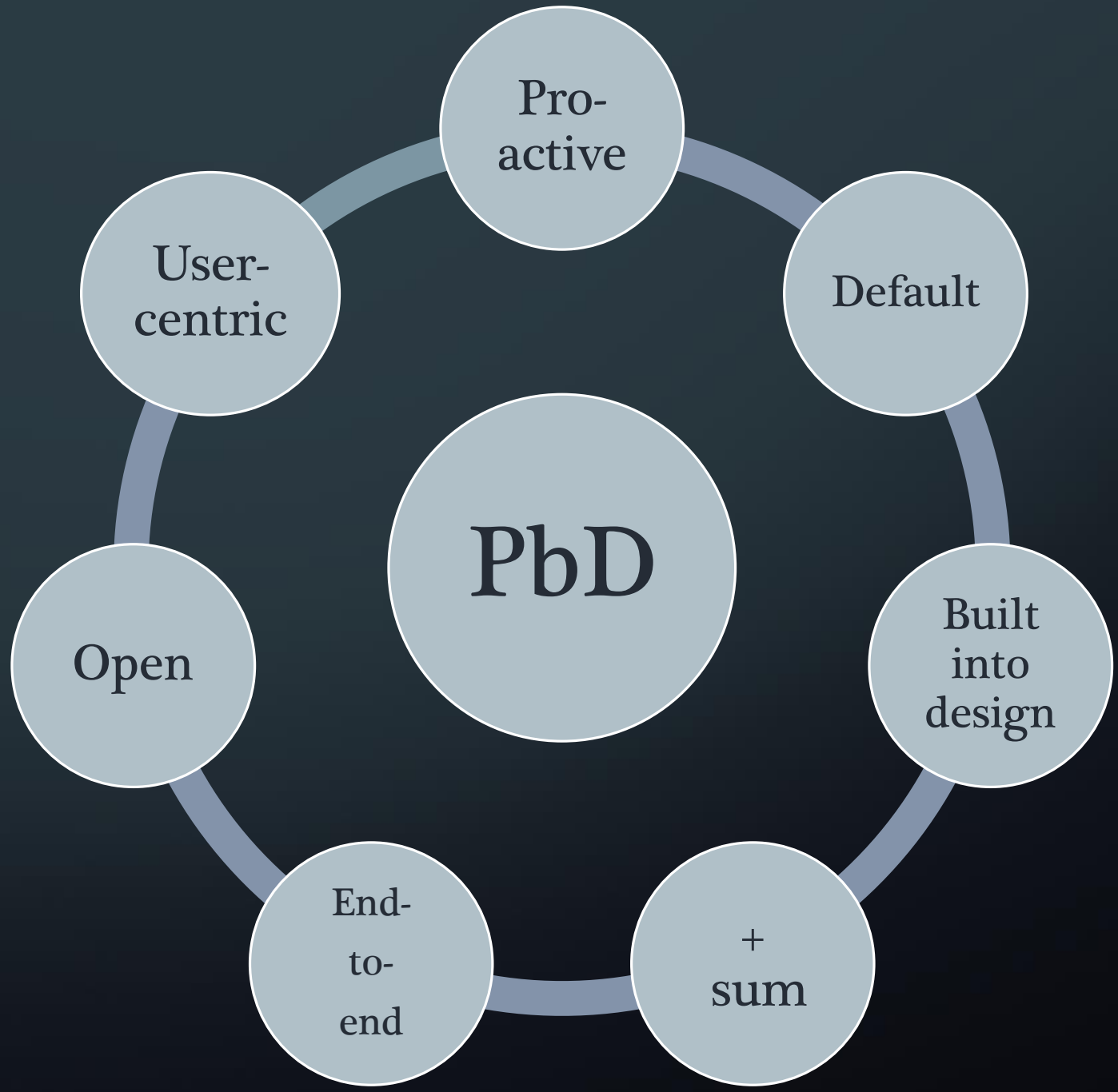
How you *develop*

- Technical and security measures
- Coding standards
- System design
- Testing and maintenance

How you work: Privacy by Design

- Development framework devised in Canada in the 1990s
- Incorporated into GDPR as a requirement
- Review existing projects for PbD compliance, and retrofit as required
- Make PbD your new development religion
- https://catalogue.projectsbyif.com

The seven principles of privacy by design



How you work: Privacy Impact Assessments

- A living document which must be accessible to all
- Document what you are doing and why (consent/legal basis)
- Document the risks
  - To the data subjects
  - To the organisation
  - To technical and systems
- Document your risk mitigation

How you work: Consent mechanisms

- Inform users of the data flows, and their rights over them
- Allow user control of consent settings through control panels, user dashboards, granular privacy options
- Enforce user consent, highest privacy by default, minor consent
- Ensure timestamped documentation of user consent

How you work: Training and CPD

- European data protection and privacy framework
- Industry or sector regulations (health, finance, etc)
- Development frameworks and methodologies
- Documentation of training in HR records
- Inductions and refreshers

How you develop: Technical and security measures

- Documentation of methodology, standards, and testing
- Secure legal international data transfers
- Evaluate physical access to data
- Evaluate user access to information
- Remember: staff training is a security measure

How you develop: Coding standards

- Create a list of approved code libraries, tools, and frameworks
  - Programming languages, version control systems
  - Testing tools, infrastructure, monitoring tools, logging servers
  - Third party frameworks and APIs
- Disable unsafe/unnecessary modules
- Disable unnecessary data retention
- Code reviews should include data maps

How you work: System design

- Data minimisation, limitation, and deletion
- Encryption in transit and at rest
- Data sandboxing, separation, and aggregation
- Pseudonymisation, anonymisation
- Design reviews should view data flows through the eyes of an attacker

How you develop: Testing and maintenance

- Dynamic testing for edge cases in the data
- Fuzz testing by intentionally triggering errors
- Penetration testing for data protection by design
- Security vulnerabilities and upgrades
- Incident logging and data breach preparation

What's WordPress doing about GDPR?

#GDPR-compliance

- Team on Making WordPress Slack
- Office hours are 16:00 UK time on Wednesdays
- https://github.com/gdpr-compliance
- Looking at Core compliance, plugin issues, and information resources

- #1767 - Inform users upon registration, that the account can't be deleted or renamed
- #43175 - GDPR Pseudonymisation
- #43389 - Add a privacy policy page setting to options-reading.php
- #43435 - Add settings screen for creating a privacy policy
- #43436 - Add opt-in for commenter cookies
- #43492 Core telemetry and updates (oh yeah, we went there)
- #43437 - Add way for registered users to request deletion or anonymization of their private data
- #43438 - Export registered user's private data on request
- #43440 - Add tools to show and export the personal data of commenters
- #43442 - Add tools for anonymizing of commenters
- #43443 - Add a method for confirmation of requests for deleting or anonymizing of personal data
- #43481 - Privacy policy tools - Admin page UI

Outside core

- Automattic is improving their products (WordPress.com, WooCommerce, Jetpack, etc)
- Coming soon: a privacy centre for users, admins, and devs
- Also coming soon: a template for privacy notices
- We're looking at the unique challenges of the ecosystem such as plugin guidelines

Thank you. PUB!

Me write good at

- @webdevlaw
- https://webdevlaw.uk/data-protection-gdpr
- https://afterbrexit.tech
- https://www.smashingmagazine.com/2018/02/gdpr-for-web-developers/

See me go blah blah blah at

- CodeMobile, Chester, 2-5 April
- PHP Yorkshire, York, 14 April
- WordCamp London, 15 April
- Frontend United, Utrecht, Netherlands, 1 June
- A large European conference in the middle of June (cough)