Privacy by Design:
Developing for data protection

Heather Burns // PHP Yorkshire // 14 April 2018

What this talk will teach you:

- How to think proactively about developing for privacy and user protection
- How to adopt protective workflows and business practices;
- How to understand that privacy and user protection are everyone's responsibility;
- How to feel empowered to challenge things which may put people at risk.

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 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

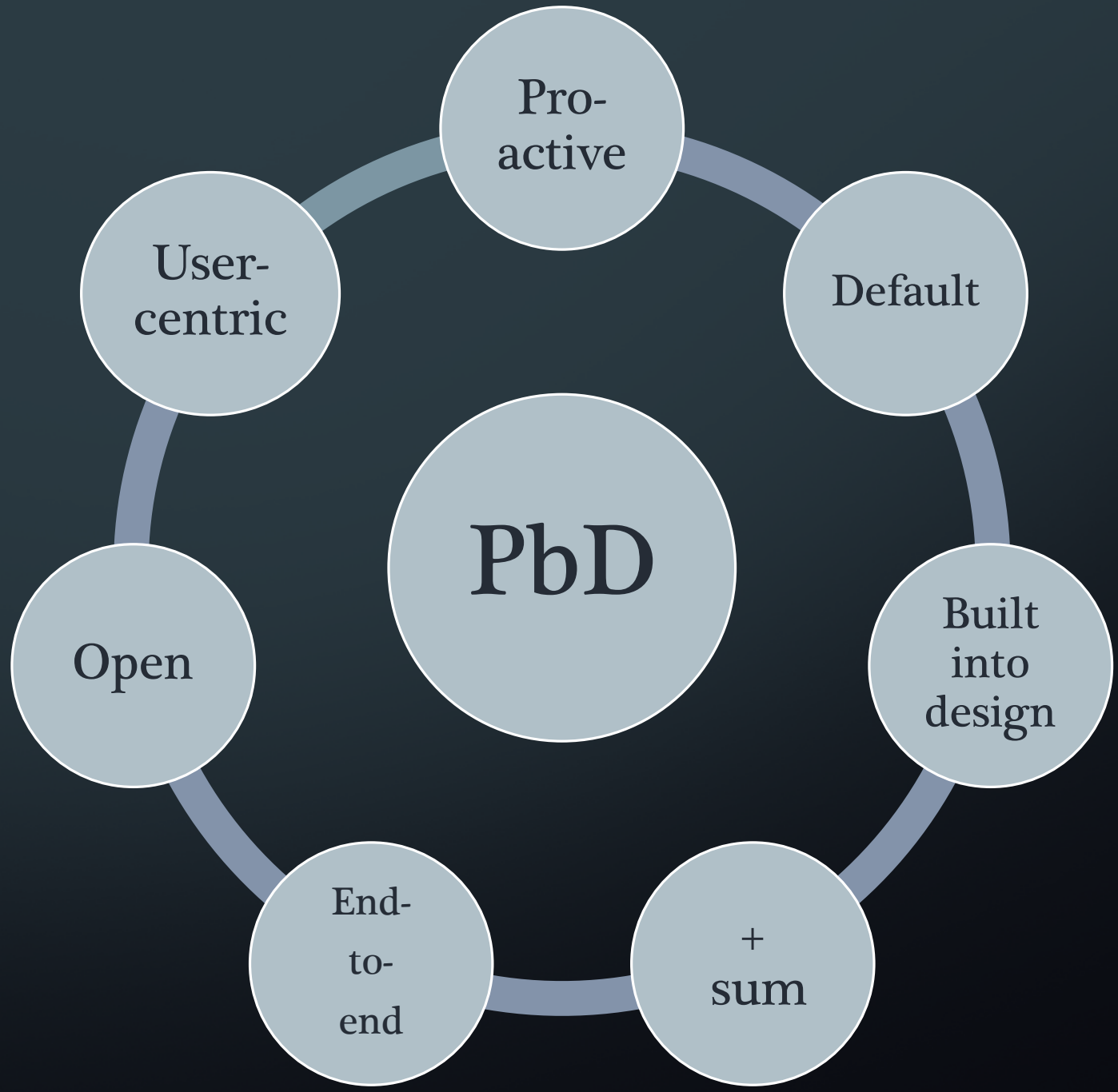
How you *develop*

- 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
- Google “Smashing Magazine Privacy By Design”

The seven principles of privacy by design



*min 6 chars

Terms & Conditions

☐ By proceeding with the registration you are confirming you have read and accepted the terms and conditions and our privacy policy, you agree that we may use the details you give or make accessible to us when you sign up, to display to you targeted advertising in your web browser while you use the service and to contact you subsequently on behalf of our advertisers by email.

I AGREE

CANCEL REGISTRATION

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

Become a privacy champion

Change your mindset

- ~~Privacy is that law we have to comply with~~
- ~~Comply or get a fine~~
- ~~The data we hold is oil~~
- ~~We're probably okay with what we've already got in place~~
- ~~We can't afford the lawyers to do this~~

- Privacy is doing right by your users
- Compliance is an opportunity to get it right and do it better
- The data we hold is toxic waste
- Rip everything up and comply from scratch as a positive business process
- No lawyers required

Become a privacy champion

- Audit your processes, your systems, and your workflows
- Audit your data
- Integrate PbD and DPbD into everything you do
- Train everyone on responsible DP and privacy practice
- Refresh everything regularly
- Document everything regularly
- Check your contracts
- Challenge colleagues and managers who ask you to engage in excessive or illegal DP practices
- Make privacy your selling point, and use it
- Keep up with changing UK, EU, and DP developments
- Use privacy law as the starting point, not the end

Thank you!

Me write good at

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

Upcoming talks

- WordCamp London, 15 April
- WordCamp Belfast, 26 May
- Frontend United, Utrecht, Netherlands, 1 June
- WordCamp Europe, Belgrade, 14-16 June