Privacy by Design:

Developing for data protection

Heather Burns // CodeClan // 6 July 2018

What this talk will teach you:

- A little bit about the legal frameworks around privacy which will govern your work as a developer;
- How you can think proactively about developing for privacy and user protection;
- How to adopt privacy-positive workflows and business practices every day.

Who am I?

(I'm having a midlife crisis – hell if I know)

- I have come over from the bright side (Glasgow)
- Designed my first web site in 1997
- Professional web designer from 2007-2015
- Now work exclusively in digital law and tech policy
- Exhaustive/exhausting work on privacy in the two year leadup to GDPR
- Not a lawyer!

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: Spring 2019 (ish)
  - Replaces the ePrivacy Directive of 2002 (UK: PECR 2003)
  - Data in transit: cookies, telemetry, advertising beacons, marketing

Definitions: what we mean by "data"

- **Personal data**

  Any information relating to an identified or identifiable natural person. This can be one piece of information *or multiple data points combined in a record.* New definitions under GDPR include genetic data, biometric data, location data, and online identifiers.

- **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

How is that different from PII?

PII = Americanism

- Full name (if not common)
- Face (sometimes)
- Home address
- Email address (if private from an association/club membership, etc.)
- National identification number (e.g., Social Security number)
- Passport number
- Vehicle registration plate number
- Driver's license number
- Face, fingerprints, or handwriting
- Credit card numbers
- Digital identity
- Date of birth
- Birthplace
- Genetic information
- Telephone number
- Login name, screen name, nickname, or handle

What *might* be PII?

- First or last name, if common
- Country, state, postcode or city of residence
- Age, especially if non-specific
- Gender or race
- Name of the school they attend or workplace
- Grades, salary, or job position
- Criminal record
- Cookies

PII ≠ Personal Data

Definitions: controllers and processors

- **Data controller**
  The data controller is a person or an entity, such as you or your business, which decides what data is processed, how it is processed, and whom it is shared with. ("Processed" simply means "used".)
- **Data processor**
  The data processor is any person other than an employee of the data controller who processes the data on behalf of the data controller.

Who is subject to GDPR and ePD?

- All data collected, processed, and retained about persons within the European Union
- Extraterritorial: applies to non-EU collection and processing
- All capturing and/or processing of personal data: no minimum size or turnover
- All situations: public sector, private sector, academia, startup, side project, or hobby

(A brief and slightly ranty segue into why that matters)

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 - ?)

- Be very afraid of the shape of UK privacy laws outside European human rights protections
- Be very afraid of anti-European spite throwing out the baby with the bathwater
- Be very afraid of moves towards a US-style self-regulatory system to coddle up to US investment

Work to the European privacy system as if Brexit was never happening

Once you are there, do not budge

How to adopt Privacy by Design into your development workflow

Getting it right from the start

How you *work*

- Privacy by Design
- Privacy Impact Assessments
- Training and CPD
- Designing for consent and user rights

How you *develop*

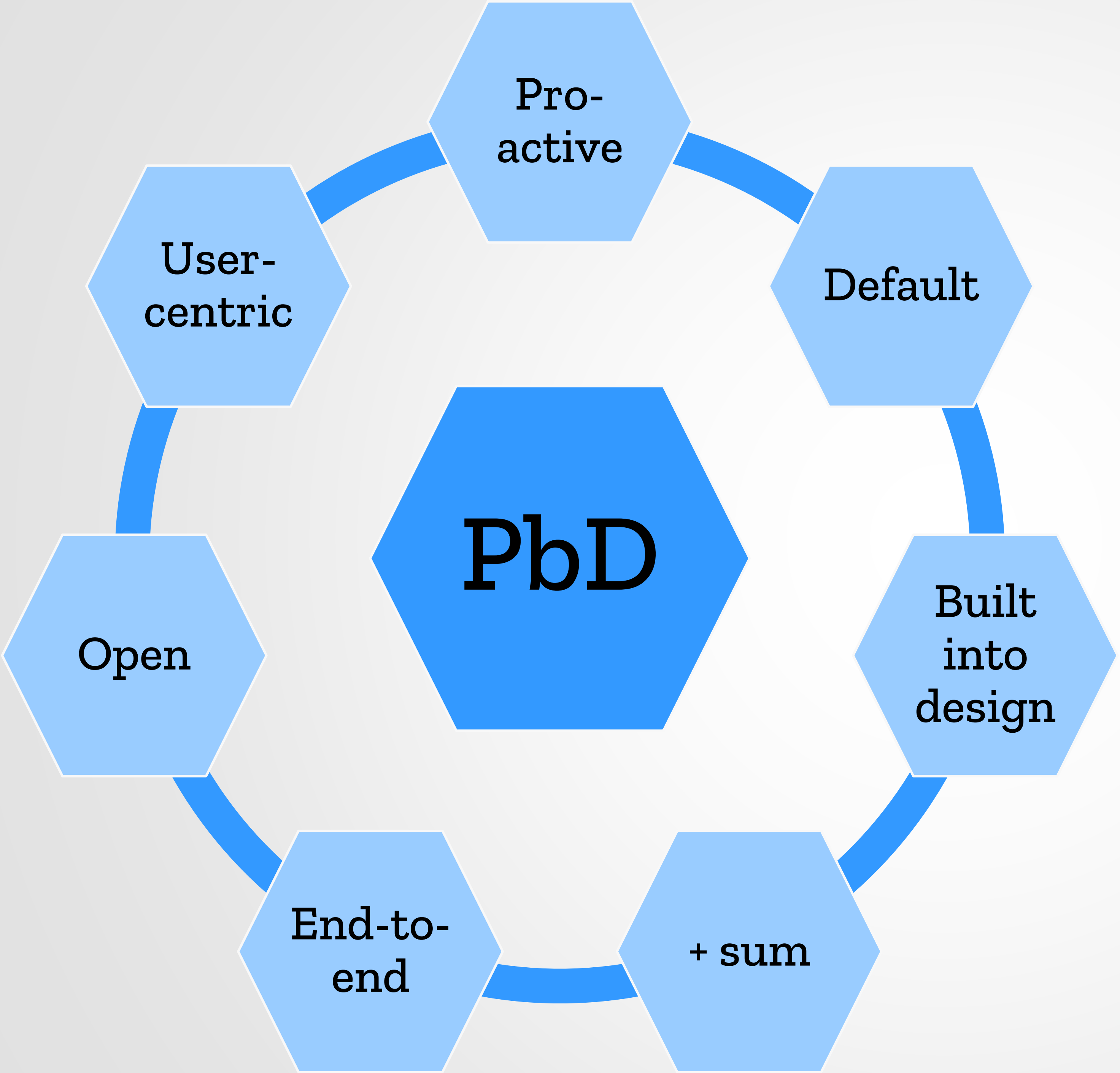
- Technical and security measures
- Coding standards
- System design
- Testing and maintenance

Privacy by Design

How you work

What is Privacy by Design?

- Non-regulatory development framework devised in Canada in the 1990s
- Incorporated into GDPR as a requirement
- A philosophy of identifying and preventing privacy problems *before they happen*
- https://www.smashingmagazine.com/2017/07/privacy-by-design-framework/



The seven principles of Privacy by Design

Checking your work on PBD

Questions from the UK ICO

- ❑ *We consider data protection issues as part of the design and implementation of systems, services, products, and business practices*

- ❑ *We make data protection an essential component of the core functionality of our processing systems and services*

- ❑ *We anticipate risks and privacy-invasive events before they occur, and take steps to prevent harm to individuals*

Checking the project on PBD

Questions from the UK ICO

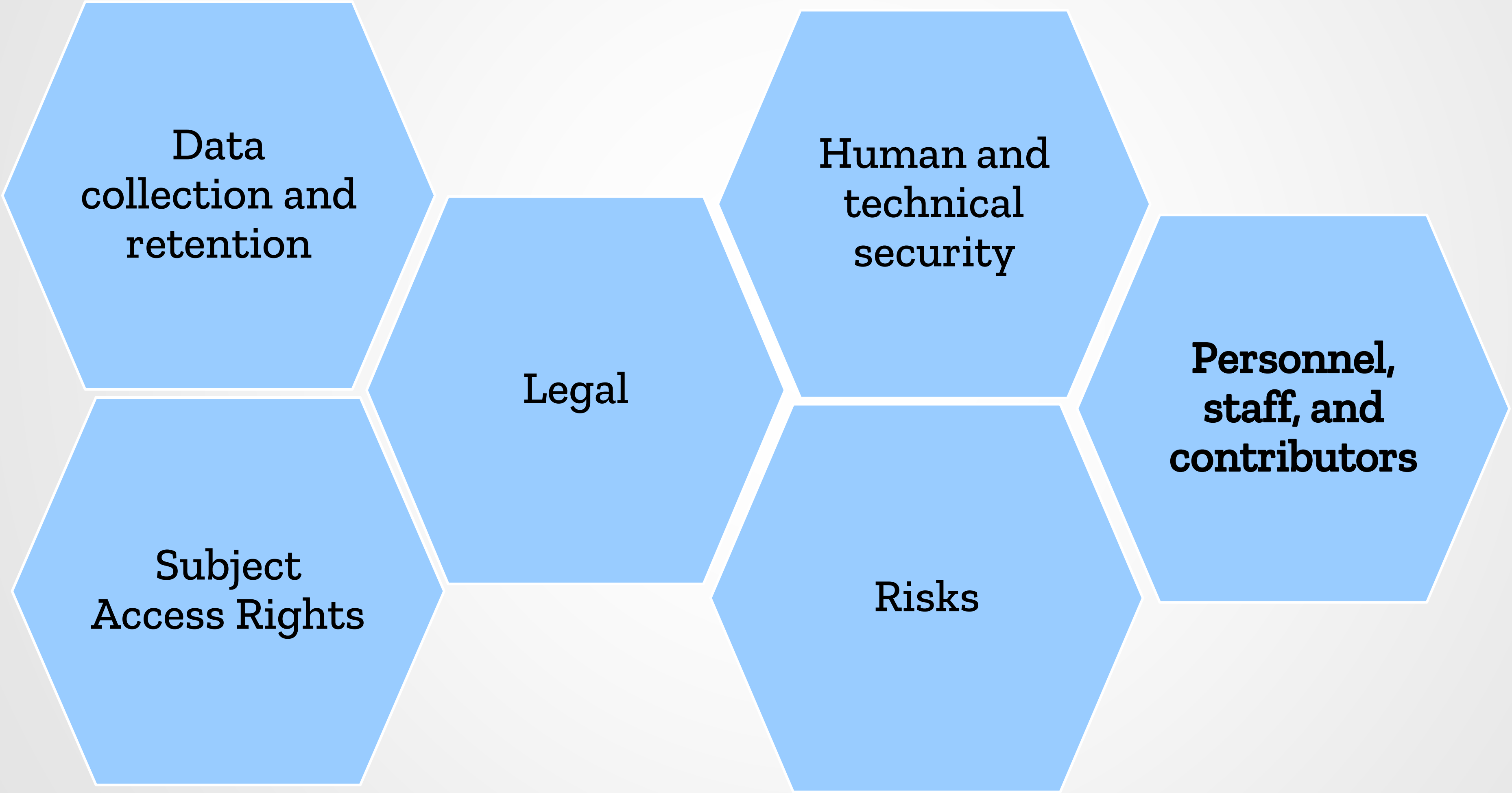
- ❑ *We ensure that personal data is automatically protected in any system, service, product, and/or business practice, so that individuals should not have to take any specific action to protect their privacy*

- ❑ *When we use other systems, services, or products in our processing activities, we make sure that we only use those whose designers and manufacturers take data protection into account.*

PBD: 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

PBD: Privacy Impact Assessments



Data collection and retention

Subject Access Rights

Legal

Human and technical security

Risks

Personnel, staff, and contributors

PIA questions: personnel, staff, and contributors

- Who has access to the data?
- What data protection training have those individuals received?
- What security measures do those individuals work with?
- What data breach notification and alert procedures are in place?
- What procedures are in place for government requests?

Training and CPD

- What data protection training have those individuals received?
  - 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

Designing for consent and user rights

- Inform users what is being done with their data, why, who has it, and what decisions are made based on it
- Inform users of their rights over the data you hold
- 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 develop

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

Making best privacy practice
your everyday development practice

Adopt a healthy mindset

- ~~Privacy is that law we have to comply with because Europe's telling us what to do WTF~~
- ~~Comply or get a fine~~
- ~~The data we hold is oil~~
- ~~We're probably okay with what we've already got~~
- ~~We can't afford the lawyers~~

- Privacy is a commitment to the accountable protection of the people in your data
- Compliance is an opportunity to get it right and do it better
- The data you hold is toxic waste
- Rip it up and start again
- No lawyers required

Adopt healthy workflows

- Audit your processes, your systems, and your workflows
- Audit your data
- Audit your people. Train them up.
- Purge what you don't need
- Refresh everything regularly
- Document everything regularly

Adopt healthy practices

- Check your contracts with your suppliers and partners
- Challenge colleagues and managers
- Call bullshit on all of the above if you need to
- Keep up with changing UK, EU, and DP developments
- Use privacy law as the baseline, not the constraint
- Make privacy your selling point, and use it

Now go forth and be privacy champions

- @webdevlaw
- https://webdevlaw.uk/data-protection-gdpr
- https://afterbrexit.tech
- https://www.smashingmagazine.com/2018/02/gdpr-for-web-developers/
- https://www.smashingmagazine.com/2017/07/privacy-by-design-framework/