Developing for privacy and data protection

Heather Burns

Government track // @webdevlaw // not legal advice
Heather Burns
Tech policy and regulation specialist
@webdevlaw
What you will learn today
What you will learn today

**Theory**
- An overview of the changing data protection and privacy landscape
- The different cultural and legal views of privacy within open source projects
- Why we have a responsibility to overcome these differences

**Practice**
- Defining what privacy means for our work
- Case study: how the WordPress project got a privacy core team
- How you can contribute to privacy in Drupal and in your own work
What you will do with that knowledge
What you will do with that knowledge

- **Shift your thinking** to view privacy as a positive cultural value, not a negative legal obligation;
- **Integrate** best privacy practices into your development workflow;
- **Review** your existing work for privacy improvements;
- **Contribute** to Drupal’s growing privacy work.
CONFERENCE TRAVEL SUPPORTED BY

11th – 13th April 2018
University of York, UK
Workshops – 11th + 12th
Conference – Saturday 13th

CFP opens late September
Early bird tickets available in October

@phpyorkshire https://phpyorkshire.co.uk

Drupal Europe
Darmstadt, Germany
10 - 14 September 2018

17/3/2018
An overview of the changing privacy landscape
Europe’s privacy overhaul

2018 - 2019

GDPR: 25 May 2018
- Replaced the Data Protection Directive of 1995
- Maintains original principles, expands and modernises
- Data at rest: collection, usage, retention

ePrivacy Directive: TBD (winter/spring 2019-ish)
- Replaces the ePrivacy Directive of 2002
- Data in transit: cookies, telemetry, advertising beacons, marketing
- Colloquially and somewhat inaccurately known as the “Cookie Law”
GDPR talks at Drupal Europe

Finally, not me!

- GDPR and Privacy Experience
- Drupal GDPR module
- Drupal GDPR exchange
- GDPR for open technology companies
- GDPR for developers
American privacy legislation is coming

<table>
<thead>
<tr>
<th>“US GDPR” NTIA standards</th>
<th>BROWSER Act of 2017</th>
<th>SPADA of 2017</th>
<th>Internet Bill of Rights of 2018</th>
</tr>
</thead>
<tbody>
<tr>
<td>FTC Privacy Act changes</td>
<td>Social Media Privacy and Consumer Rights Act of 2018</td>
<td>CONSENT Act of 2018</td>
<td>Resolution on applying GDPR protections to U.S. citizens</td>
</tr>
</tbody>
</table>
Differing approaches to privacy within open source projects
Open source software projects are made by the people who show up...

...the problem is, we show up with very different cultural perspectives on privacy.
European cultural approach to privacy

- Privacy is a fundamental human right
- Data belongs to the subject
- Opt-in culture
- Culture of constructive work through regulators, with fines or court action a rare last resort
- People trust governments and fear businesses
Free speech is a fundamental human right
Data belongs to the site/service owner
Opt-out culture
Culture of adversarial courtroom litigation
People fear governments and trust businesses

American cultural approach to privacy
We also show up with very different legal approaches to privacy.
European legal approach to privacy

- Privacy is regulated through hard law
- One overarching law for all member states and sectors
- Data protection regulators
- Not tied to citizenship or nationality
- Privacy is its own law
- Litigation is the last resort
American legal approach to privacy

- Privacy is governed through soft law
- No overarching DP law; piecemeal approach across sectors and states
- No data protection regulator (no law to enforce)
- Tied to citizenship and nationality
- Privacy is a subcategory of contract or consumer law
- Litigation is the first resort
These differing views shape our approach to compliance.
Barely 1.5 weeks into GDPR and it seems to have completely stopped being a source of any discussion in the tech circles I follow. Somehow I doubt that it is because everyone has started complying and moved on.

Mike Richwalsky @mrichwalsky · Jun 5
Replying to @ChrisWiegman
Until the first lawsuits and judgements start coming in. They it will flare back up I think.

Chris Wiegman @ChrisWiegman · Jun 5
Unfortunately I think you're probably right

Jamie Schmid @jamieschmid · Jun 5
Replying to @ChrisWiegman
we're all waiting for a big case ruling to scare us into compliance
“Under the GDPR’s new tools, we’ll be able to use enforcement notices to require companies to delete algorithms or stop processing.

I think orders to stop processing are going to be as powerful, if not more powerful than administrative fines.”

-Elizabeth Denham, the UK Information Commissioner, to the Civil Liberties Committee of the European Union, 4 June 2018
And when it comes to privacy, we don’t always agree to disagree.
Things Europeans say about the American approach to privacy...

“Wild West”

“Even before GDPR starts, they are violating the rules”

“Their tone is still far from acknowledging the serious concerns people have”

“A lack of progress may challenge the effectiveness of self-regulation in this area and may increase the pressure to legislate.”

“We thank you for appearing to testify before our committee today”
Things Americans say about the European approach to privacy...

- "Jack-booted thugs"
- "It could significantly interrupt transatlantic commerce and create unnecessary barriers to trade"
- "The European approach runs the risk of being insensitive to context"
- "There should be no government involvement"
- "I don't understand how we've reached a point where we, in the United States, are reliant on a foreign regulation to protect our data"
We all have different perspectives and approaches about privacy as a value.

...but who are we?
We make the CMSs which have 72.7% market share on the web.

https://w3techs.com/technologies/history_overview/content_management
We are people of enormous power and influence over privacy on the internet.
And we’ve never understood our differences, nevermind acknowledged them.
What’s the consequence of that?

- We *structure* our work with different cultural approaches to privacy
- We *write* our code with different legal approaches to privacy
- We *assume* everyone we code with works and thinks like we do
- We *create* the open web with no common standard for privacy
- We *fail* to do everything we could do to protect the people in the data
- We *don’t* learn from our mistakes.
We have to do better.
The actions we take within the project, however small, can protect the people in the data from those who would use that data to hurt them.
So we need to shift our thinking.
We need to stop thinking of privacy as a legal problem to run away from, and instead, think of it as a cultural opportunity to embrace.
Okay, so how do we do that?
Defining what privacy is, and what it means for our work
Let’s talk about the Privacy by Design Framework.
What is Privacy by Design?

- Non-regulatory development framework devised in Canada in the 1990s
- Incorporated into GDPR as a requirement
- Review your existing projects for PbD compliance, and retrofit as required
The seven principles of Privacy by Design

- Pro-active
- Default
- Built into design
- User-centric
- Open
- End-to-end
- + sum
Checking your work for PbD

Questions from the UK’S 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 your work for PbD

Questions from the UK’s 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 within a project
• Document what you are doing and why (consent/legal basis)
• Document the risks
  o To the data subjects
  o To the organisation
  o To technical and systems
• Document your risk mitigation
PBD: Privacy Impact Assessments

- Data collection and retention
- Subject access rights
- Human and technical security
- Risks
- Legal
- People and contributors
PIA Questions: People 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?
PIA Questions: People and contributors

- 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
If you use *nothing* else, use the PBD framework.

...but I’m not going to let you off that easy, you’re going to do this too.
Two kinds of privacy rules

Which do you choose, a hard or soft option?

Hard law and regulation
- GDPR
- CJEU judgements
- COPPA / HIPPA
- ICO / CNIL / FTC / etc

Soft policy and regulation
- Industry codes of conduct
- ISO standards
- International conventions
- Frameworks (Privacy by Design)

Hard laws build their foundations on the standards defined in soft laws. This is certainly the case for online privacy.
Let’s use soft law to define common privacy values.
International privacy frameworks

- Council of Europe Convention for the Protection of Individuals with Regard to the Processing of Personal Data (1980/two weeks ago 2018)
- APEC Privacy Framework (2005)
- FTC Fair Information Practice Principles (2000)
<table>
<thead>
<tr>
<th>OECD</th>
<th>COE</th>
<th>ISO</th>
<th>APEC</th>
<th>FIPP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Collection Limitation Principle</td>
<td>Legitimacy of data processing and quality of data</td>
<td>Consent and choice</td>
<td>Preventing harm</td>
<td>Notice/Awareness</td>
</tr>
<tr>
<td>Data Quality Principle</td>
<td>Special categories of data</td>
<td>Purpose legitimacy and specification</td>
<td>Notice</td>
<td>Choice/Consent</td>
</tr>
<tr>
<td>Purpose Specification Principle</td>
<td>Data security</td>
<td>Collection limitation</td>
<td>Collection limitation</td>
<td>Problems with Choice/Consent</td>
</tr>
<tr>
<td>Use Limitation Principle</td>
<td>Transparency of processing</td>
<td>Data minimization</td>
<td>Uses of personal information</td>
<td>Access/Participation</td>
</tr>
<tr>
<td>Security Safeguards Principle</td>
<td>Rights of the data subject</td>
<td>Use, retention and disclosure limitation</td>
<td>Choice</td>
<td>Integrity/Security</td>
</tr>
<tr>
<td>Openness Principle</td>
<td></td>
<td>Accuracy and quality</td>
<td>Integrity of personal information</td>
<td>Enforcement/Redress</td>
</tr>
<tr>
<td>Individual Participation Principle</td>
<td></td>
<td>Openness, transparency and notice</td>
<td>Security safeguards</td>
<td></td>
</tr>
<tr>
<td>Accountability Principle</td>
<td>Individual participation and access</td>
<td>Access and correction</td>
<td>Accountability</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Accountability</td>
<td>Information security</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Privacy compliance</td>
<td></td>
<td></td>
</tr>
<tr>
<td>OECD</td>
<td>COE</td>
<td>ISO</td>
<td>APEC</td>
<td>FIPP</td>
</tr>
<tr>
<td>------------------------------------</td>
<td>------------------------------------------</td>
<td>------------------------------------------</td>
<td>--------------------------------------------</td>
<td>-------------------------------------------</td>
</tr>
<tr>
<td>Collection Limitation Principle</td>
<td>Legitimacy of data processing and quality of data</td>
<td>Consent and choice</td>
<td>Preventing harm</td>
<td>Notice/Awareness</td>
</tr>
<tr>
<td>Data Quality Principle</td>
<td>Special categories of data</td>
<td>Purpose legitimacy and specification</td>
<td>Notice</td>
<td>Choice/Consent</td>
</tr>
<tr>
<td>Purpose Specification Principle</td>
<td>Data security</td>
<td>Collection limitation</td>
<td>Collection limitation</td>
<td>Problems with Choice/Consent</td>
</tr>
<tr>
<td>Use Limitation Principle</td>
<td>Transparency of processing</td>
<td>Data minimization</td>
<td>Uses of personal information</td>
<td>Access/Participation</td>
</tr>
<tr>
<td>Security Safeguards Principle</td>
<td>Rights of the data subject</td>
<td>Use, retention and disclosure limitation</td>
<td>Choice</td>
<td>Integrity/Security</td>
</tr>
<tr>
<td>Openness Principle</td>
<td></td>
<td>Accuracy and quality</td>
<td>Integrity of personal information</td>
<td>Enforcement/Redress</td>
</tr>
<tr>
<td>Individual Participation Principle</td>
<td></td>
<td>Openness, transparency and notice</td>
<td>Security safeguards</td>
<td></td>
</tr>
<tr>
<td>Accountability Principle</td>
<td></td>
<td>Individual participation and access</td>
<td>Access and correction</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Accountability</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Information security</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Privacy compliance</td>
<td></td>
</tr>
</tbody>
</table>
From there, we can identify and define common privacy values and what they mean.
Collect only the data you need and no more
Data integrity

Ensure that the data is true, authentic, and up to date
Purpose minimisation

Use the data only for the purpose you collected it for and nothing else
Do not use the data for other purposes, keep it longer than you need, or share it with others without reason
Human and technical security

Take adequate technical and human measures to protect the data from misuse and its subjects from harm.
Transparency and notice

Make public what data you hold, why you hold it, and what you do with it.
Give people rights to access their data, correct mistakes, and the ability to ask you to stop using their data.
Fix problems when things go wrong, make it right when people are hurt, and face the consequences for misuse.

Accountability, enforcement, and redress
Give people choices, options, and rights over how you use their data at any time
Special categories of data

Take care with sensitive data which could result in the people it is about being hurt.
Legal compliance

Work cooperatively and productively with regulations, laws, and supervisory bodies
11 universal privacy principles for development

- Data minimisation
- Purpose minimisation
- Data integrity
- Lifecycle limitation
- Human and technical security
- Transparency and notice
- User participation and rights
- Choice, control, and consent
- Accountability, enforcement, and redress
- Legal compliance
- Special categories of data
https://github.com/webdevlaw/open-source-privacy-standards
Creating and following “soft regulation” principles for user privacy lessens the chances of “hard regulation” being imposed onto your project.
BSA’s privacy framework for US policymakers

Released yesterday

1. Transparency and notice
2. Purpose minimisation
3. Choice and consent
4. Data integrity
5. Consumer control
6. Technical security
7. Facilitating data use for legitimate interests
8. Accountability
9. Legal compliance
10. International interoperability
So how do we integrate those principles into the project?
Example: Transparency and Notice

Here’s how we did it in WordPress.org

• What is the status of transparency and notice in core?
• Does it need to change?
• What do the development guidelines say about project design and transparency and notice?
• What do the development guidelines say about code and transparency and notice?
• What do we want to achieve?
• When do we want to ship that?
• How do we build in the functionality for transparency and notice?
• What about plugins and themes?
• Who else needs to be involved?
Example: Transparency and Notice

Planning and documentation

- https://developer.wordpress.org/plugins/privacy/
- How does your plugin handle personal data? Use `wp_add_privacy_policy_content` to disclose to your users any of the following:
- Does the plugin share personal data with third parties (e.g. to outside APIs/servers). If so, what data does it share with which third parties and do they have a published privacy policy you can provide a link to?
- Does the plugin collect personal data? If so, what data and where is it stored? Think about places like user data/meta, options, post meta, custom tables, files, etc.
Example: Transparency and Notice

Planning and documentation

- Does the plugin use personal data collected by others? If so, what data?
- Does the plugin pass personal data to a SDK? What does that SDK do with the data?
- Does the plugin collect telemetry data, directly or indirectly? Loading an image from a third-party source on every install, for example, could indirectly log and track the usage data of all of your plugin installs.
- Does the plugin enqueue Javascript, tracking pixels or embed iframes from a third party (third party JS, tracking pixels and iframes can collect visitor’s data/actions, leave cookies, etc.)?
- Does the plugin store things in the browser? If so, where and what? Think about things like cookies, local storage, etc.
Example: Transparency and Notice

Development guidelines and code

Code Example

```php
function my_example_plugin_add_privacy_policy_content() {
    if (!function_exists( 'wp_add_privacy_policy_content' )) {
        return;
    }

    $content = sprintf(
        'When you leave a comment on this site, we send your name, email address, IP address and comment text to example.com. Example.com does not retain your personal data.

        The example.com privacy policy is <a href="%s" target="_blank">here</a>;,
        'my_plugin_textdomain'),
        'https://example.com/privacy-policy'
    );

    wp_add_privacy_policy_content( 'Example Plugin',
        'Example Plugin',
        wp_kses_post( $content, false )
    );
}
add_action( 'admin_init', 'my_example_plugin_add_privacy_policy_content' );
```
Integrating privacy principles

- Define how each privacy principle needs to be adopted
- Amend project guidelines on how work is *structured*
- Amend development guidelines on how work is *coded*
- Provide resources for developers to understand how to use any new functionality
- Provide resources for site administrators to understand why these things matter and what they need to do
Case study: the WP core privacy team
Phase 1:
GDPR compliance
GDPR core-compliance V1 roadmap

- Enhancing privacy standards in core
- Examining the plugin developer guidelines with privacy in mind
- Creating documentation focused on best practices in online privacy
- Adding tools which will allow site administrators to create user-friendly privacy notices
Project constraints

- We cannot make WordPress sites compliant
- No tool achieves compliance in and of itself
- No tool removes the user’s responsibility for compliance
- There is no such thing as “compliance”, only a journey
- The WordPress project is allergic to anything “legal” – and privacy was seen as a legal (and European) thing
So here’s what we did do:

1. Add tools to core to allow users to create a privacy notice, export data, and erase data
2. Create plugin functionality and hooks to feed data into those tools
3. Add documentation/help for admins, users, and devs
4. Remove “legal compliance” from plugin guidelines
5. Identify areas for future work outside GDPR
Project constraints

- We cannot make WordPress sites compliant
- No tool achieves compliance in and of itself
- No tool removes the user’s responsibility for compliance
- There is no such thing as “compliance”, only a journey
- The WordPress project is allergic to anything “legal” – and privacy was seen as a legal (and European) thing
GDPR tools shipped in WordPress 4.9.6
# Export Personal Data

## Add Data Export Request

An email will be sent to the user at this email address asking them to verify the request.

**Username or email address**

![Send Request button](button.png)

---

### All (0) | Pending (0) | Confirmed (0) | Failed (0) | Completed (0)

<table>
<thead>
<tr>
<th>Requester</th>
<th>Status</th>
<th>Requested</th>
<th>Next Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>No items found.</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Requester</th>
<th>Status</th>
<th>Requested</th>
<th>Next Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>Requester</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Erase Personal Data

Add Data Erasure Request

An email will be sent to the user at this email address asking them to verify the request.

Username or email address

[Enter email] Send Request

All (0) | Pending (0) | Confirmed (0) | Failed (0) | Completed (0)

<table>
<thead>
<tr>
<th>Requester</th>
<th>Status</th>
<th>Requested</th>
<th>Next Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

No items found.

<table>
<thead>
<tr>
<th>Requester</th>
<th>Status</th>
<th>Requested</th>
<th>Next Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Privacy notice tool

- Starter for a GDPR-ready privacy notice
- Not a template – headers and prompts are just that
- Functionality to feed info in from plugins and themes
- Admin is responsible for publishing
Privacy Settings

Privacy Policy page

As a website owner, you may need to follow national or international privacy laws. For example, you may need to create and display a privacy policy. If you already have a privacy policy page, please select it below. If not, please create one.

The new page will include help and suggestions for your privacy policy. However, it is your responsibility to use those resources correctly, to provide the information that your privacy policy requires, and to keep that information current and accurate.

After your privacy policy page is set, we suggest that you edit it. We would also suggest reviewing your privacy policy from time to time, especially after installing or updating any themes or plugins. There may be changes or new suggested information for you to consider adding to your policy.

Edit or view your privacy policy page content.

Need help putting together your new Privacy Policy page? Check out our guide for recommendations on what content to include. Along with policies suggested by your plugins and theme.

Change your Privacy Policy page

Select an existing page: Privacy Policy

Or: Create New Page

Use This Page
Introduction

Hello,

This text template will help you to create your website's privacy policy.

We have suggested the sections you will need. Under each section heading you will find a short summary of what information you should provide, which will help you to get started. Some sections include suggested policy content, others will have to be completed with information from your theme and plugins.

Please edit your privacy policy content, making sure to delete the summaries, and adding any information from your theme and plugins. Once you publish your policy page, remember to add it to your navigation menu.

It is your responsibility to write a comprehensive privacy policy, to make sure it reflects all national and international legal requirements on privacy, and to keep your policy current and accurate.

Source: WordPress

Who we are

In this section, you should note your site URL, as well as the name of the company, organisation, or individual behind it, and some accurate contact information.

The amount of information you may be required to show will vary depending on your local or national business regulations.
Hello,

This text template will help you to create your website’s privacy policy.

We have suggested the sections you will need. Under each section heading you will find a short summary of what information you should provide, which will help you to get started.
Functionality and documentation
Developer guidelines

https://developer.wordpress.org/plugins/privacy/

Theory
• What is privacy?
• Privacy by Design
• Food for thought for your plugin

Practice
• Suggesting text for the site privacy policy
• Adding the Personal Data Exporter to Your Plugin
• Adding the Personal Data Eraser to Your Plugin
• Privacy Related Options, Hooks, Filters, and Capabilities
We got “legal compliance” removed from plugin guidelines
...at last
Guideline 9 *(Developers and their plugins must not do anything illegal, dishonest, or morally offensive.)* has been amended to include the following new prohibition:

*implying that a plugin can create, provide, automate, or guarantee legal compliance*
What we didn’t do was as impactful as what we did do.
We didn’t:

- Scaremonger or threaten
- Discuss penalties, fines, or enforcement – at all
- Make a plugin rather than applying the work to core
- Leave the work with legal
- Get the version numbering right
- Get support from the project leadership
So with the test run being over...
We got Privacy established as a permanent core component.

Privacy component

94 open tickets
Open bugs: 31. View list on Trac

Help maintain this component
Component maintainers:

desrosj  allenday  idea15  xkon  postphotos  caslepa
Core privacy V2 roadmap

1. Core features (embeds, Gravatars)
2. Plugin privacy
3. Consent and logging
4. Erasure and export tools
5. Internationalisation
6. Multisite support
7. CLI
Contributing to privacy in Drupal and in your own work
Where to start in your own work?

- Review your data capture, sharing, flows, and retention
- Conduct a Privacy Impact Assessment
- Read up on GDPR, PBD, and the open source standard idea
- Follow the WP core privacy team
- Support Drupal core privacy work
- Become privacy champions in your workplaces
- Demonstrate leadership in privacy within the ecosystem
What have you learned today?

By now I hope you know how to

● **respect** privacy as a positive cultural value, rather than resent it as a negative legal obligation;
● **integrate** best privacy practice into your development workflow;
● make a plan to **review** your existing work for privacy improvements;
● **contribute** to Drupal’s privacy work.
We make the CMSs which have 72.7% market share on the web.

https://w3techs.com/technologies/history_overview/content_management
We are people of enormous power and influence over privacy on the internet.
The actions we take within the project, however small, can protect the people in the data from those who would use that data to hurt them.
Let’s make our open source projects the most privacy-conscious work in the world.
Thank you for coming today. Now show me what you can do.

@webdevlaw

https://webdevlaw.uk/data-protection-gdpr
https://github.com/webdevlaw/open-source-privacy-standards

https://www.smashingmagazine.com/2018/02/gdpr-for-web-developers/