WORDCAMP VIENNA 2020 | PETER PUTZER

PRIVACY BY DESIGN: WRITING PRIVACY-CONSCIOUS WORDPRESS PLUGINS

PRIVACY BY DESIGN

- First developed in 1995
  - Canadian and Dutch data protection authorities
  - Ann Cavoukian (Information and Privacy Commissioner of Ontario 1997–2014)
- International adoption since 2010
  - International Assembly of Privacy Commissioners and Data Protection Authorities
  - ISO standard under development
- Incorporated into GDPR
  - “data protection by design”
  - “data protection by default”

PRIVACY BY DESIGN – PRINCIPLES

1. Proactive not reactive; preventive not remedial
2. Privacy as the default setting
3. Privacy embedded into design
4. Full functionality - positive-sum, not zero-sum
5. End-to-end security - full lifecycle protection
6. Visibility and transparency - keep it open
7. Respect for user privacy - keep it user-centric

WHAT YOU SHOULD DO (AS A PLUGIN DEVELOPER)

1. Think!
2. Think again
3. Write things down
4. Code

WHAT YOU SHOULD THINK ABOUT – PART I

- What data will the plugin collecting/processing?
- How will the plugin handle and store the data?
- How can users access their data? Grant and revoke consent?
- Data export and erasure
- Security measures
- Disclosure (privacy notice, README, etc.)
- Legal compliance

WHAT YOU SHOULD THINK ABOUT – PART II

- That’s a lot of questions
- Answers will often be domain-specific
- Some best practices apply regardless of domain

WHAT DATA?

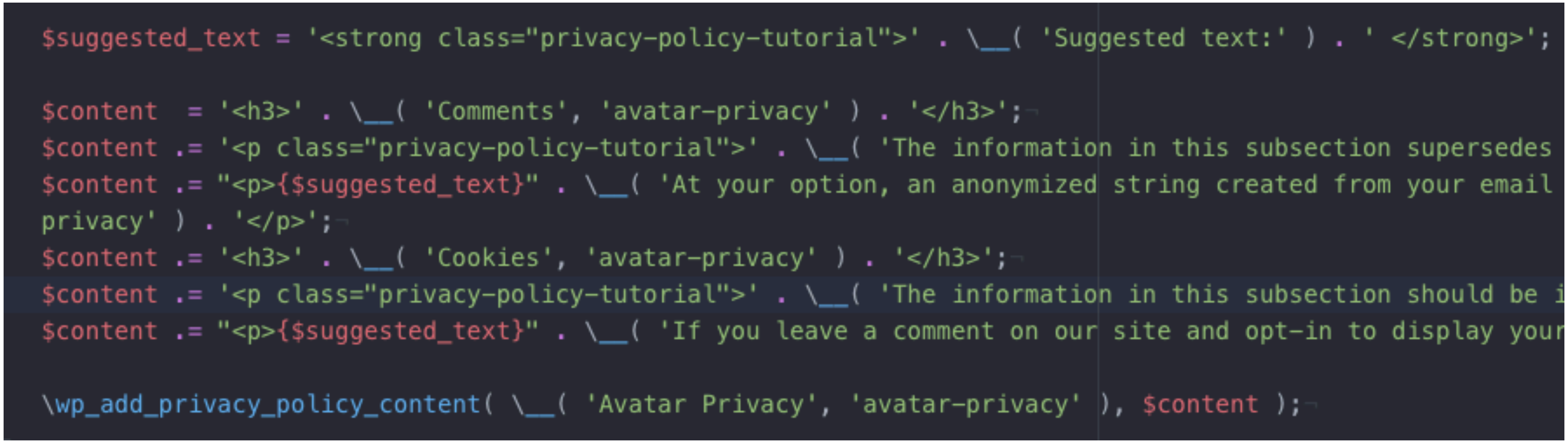
- Whose?
  - Visitor data
  - Admin/author data
  - Data about the server
- Different kinds
  - Technical data (IP address, browser, operating system …)
  - Content data (email, comments, posts …)
  - Special categories (sensitive personal data – e.g. health, biometrics)

FULL DISCLOSURE – PART I

- Document the plugin’s data handling
  - README
  - Privacy Notice
  - comments in your code
- Things to include
  - cookies (name, lifespan, purpose)
  - data sent to external services/APIs
  - data that is stored locally (user meta, custom tables, etc.)
  - retention periods
- Don't promise legal compliance (you can’t, and it’s not allowed in the WP.org plugin repository)

FULL DISCLOSURE – PART II

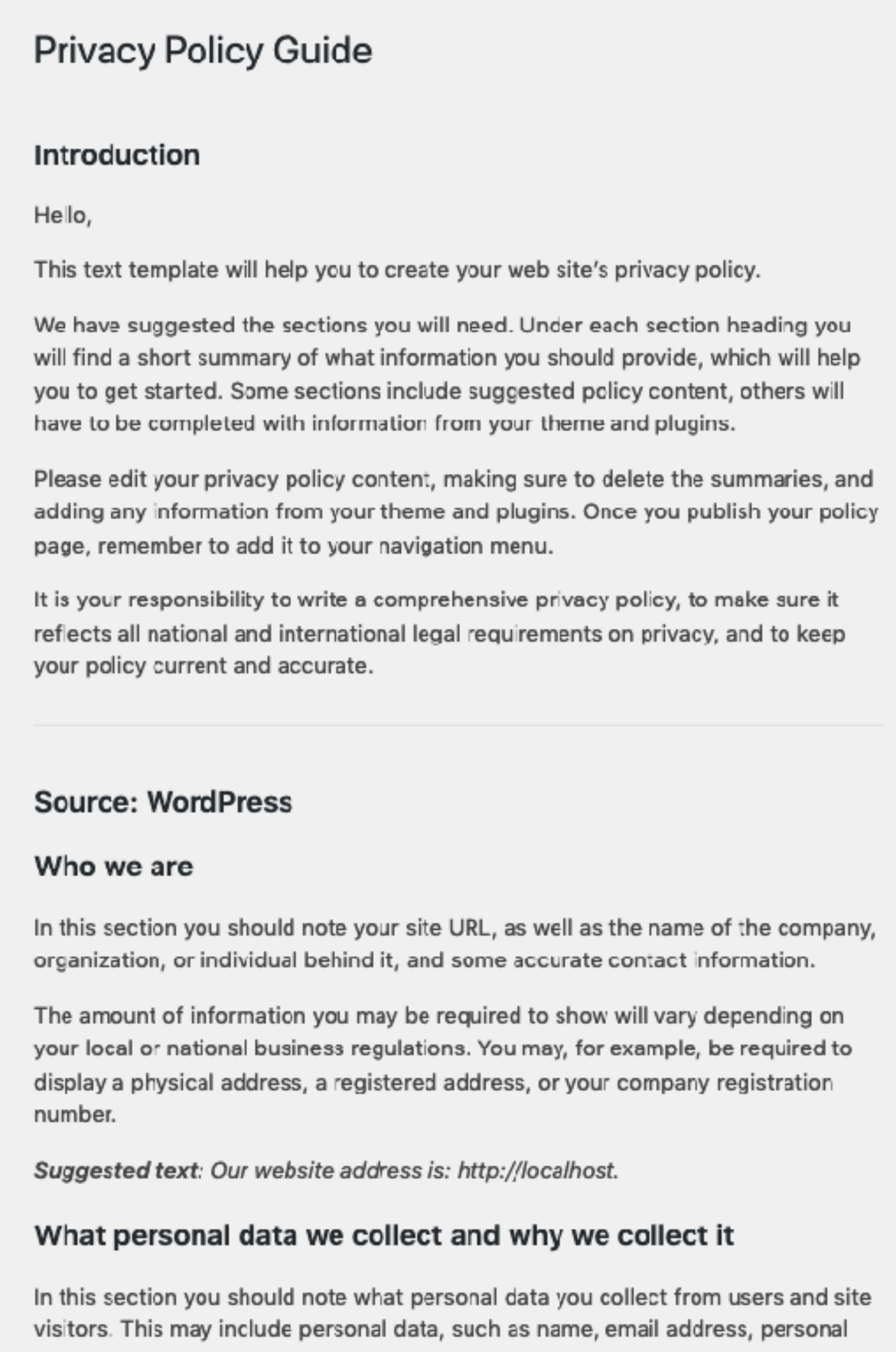
- There's a Privacy Notice API
  - Suggest content blocks for the Privacy Notice using `wp_add_privacy_policy_content()`
  - Link to the Privacy Notice in any data collecting forms using `get_the_privacy_policy_link()`
- Privacy policy content is just a block of HTML markup
- Use `<p class="privacy-policy-tutorial">` to mark text not intended for verbatim inclusion



```
$suggested_text = '<strong class="privacy-policy-tutorial">' . \__( 'Suggested text:' ) . ' </strong>';

$content  = '<h3>' . \__( 'Comments', 'avatar-privacy' ) . '</h3>';
$content .= '<p class="privacy-policy-tutorial">' . \__( 'The information in this subsection supersedes
$content .= "<p>{$suggested_text}" . \__( 'At your option, an anonymized string created from your email
privacy' ) . '</p>';
$content .= '<h3>' . \__( 'Cookies', 'avatar-privacy' ) . '</h3>';
$content .= '<p class="privacy-policy-tutorial">' . \__( 'The information in this subsection should be i
$content .= "<p>{$suggested_text}" . \__( 'If you leave a comment on our site and opt-in to display your

\wp_add_privacy_policy_content( \__( 'Avatar Privacy', 'avatar-privacy' ), $content );
```



Privacy Policy Guide

Introduction

Hello,

This text template will help you to create your web site'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

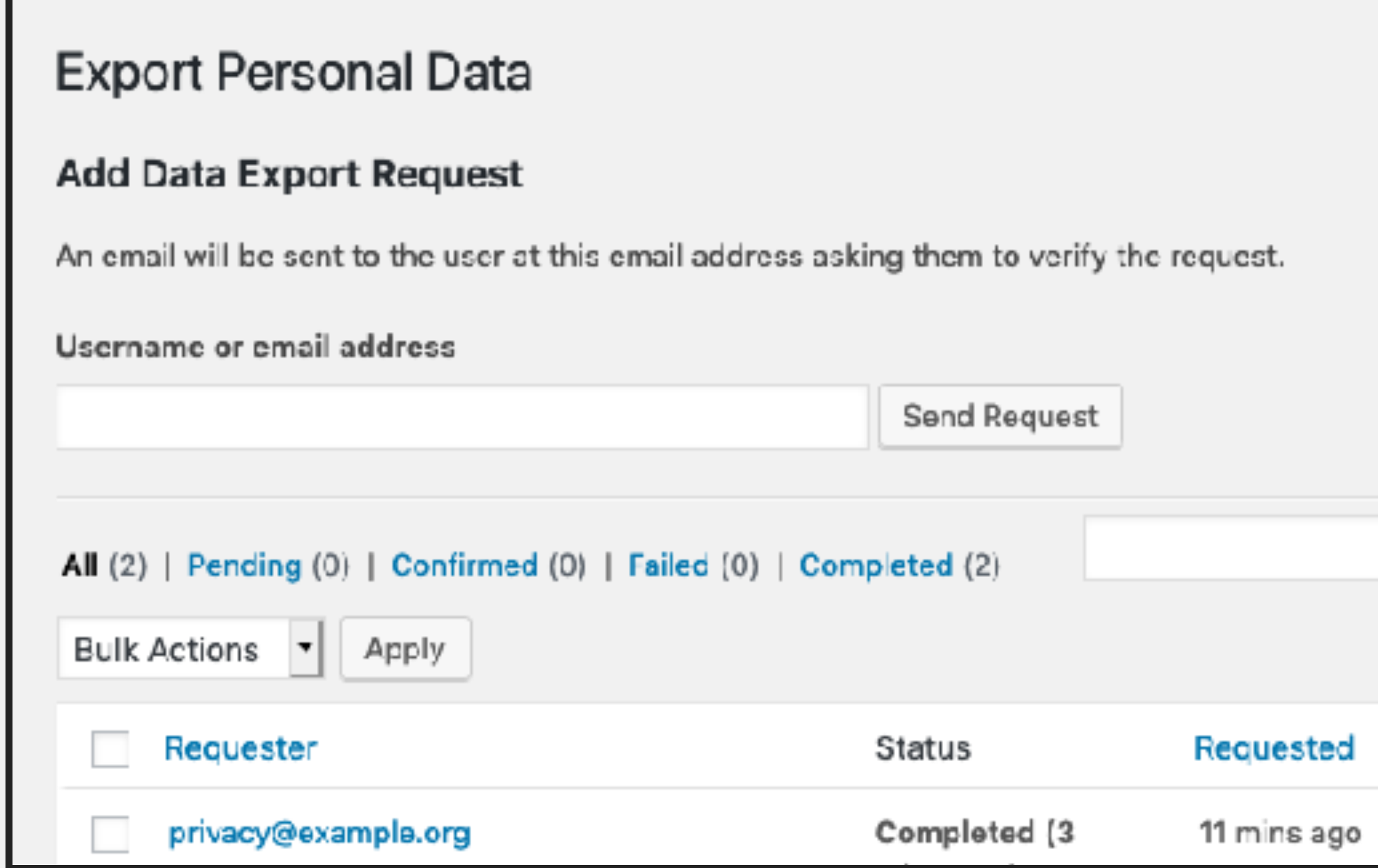
In this section you should note your site URL, as well as the name of the company, organization, or individual behind it, and some accurate contact information.

The amount of information you may be required to show will vary depending on your local or national business regulations. You may, for example, be required to display a physical address, a registered address, or your company registration number.

***Suggested text**: Our website address is: http://localhost.*

What personal data we collect and why we collect it

In this section you should note what personal data you collect from users and site visitors. This may include personal data, such as name, email address, personal



Export Personal Data

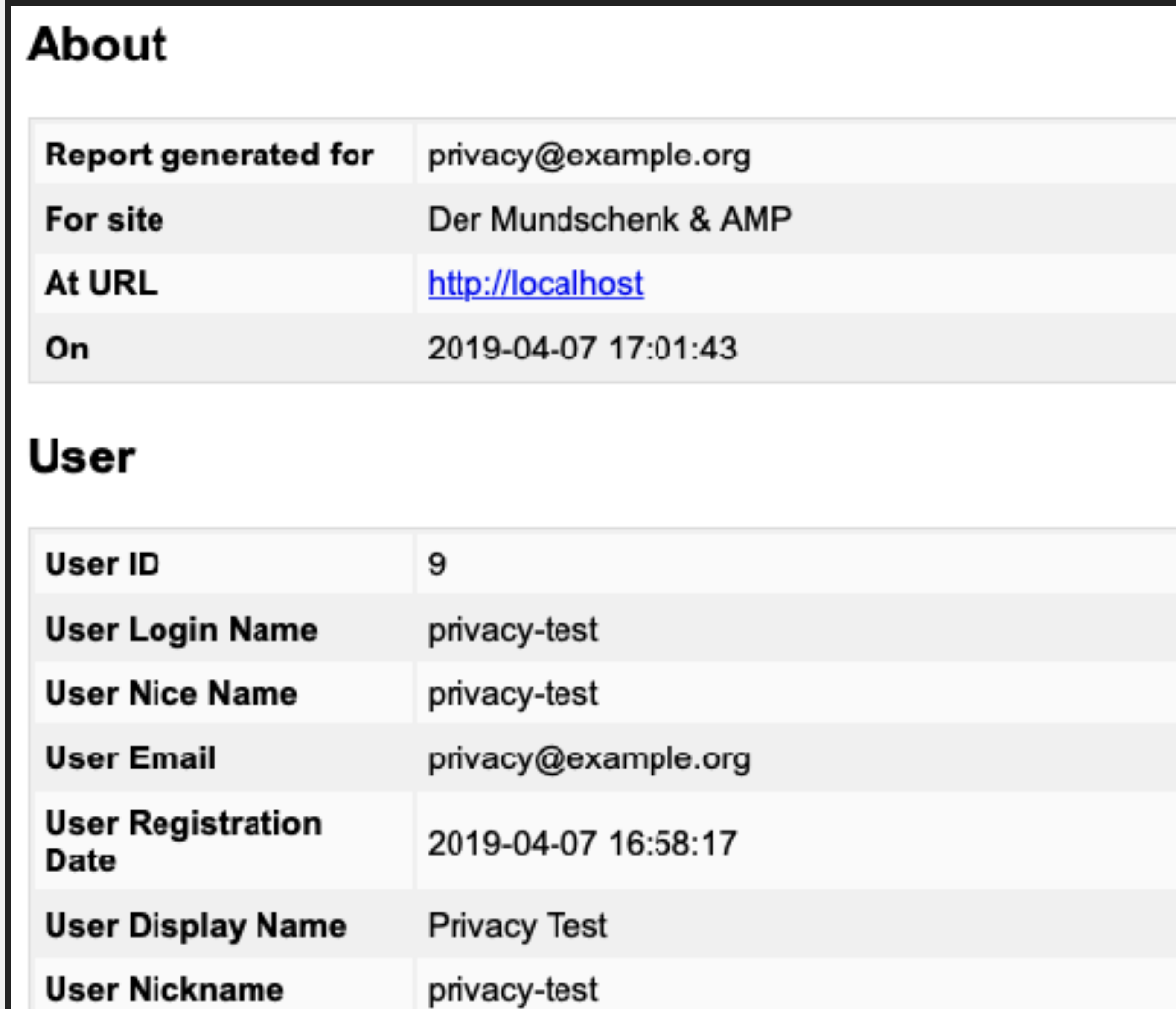
Add Data Export Request

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

Username or email address

All (2) | Pending (0) | Confirmed (0) | Failed (0) | Completed (2)

□	Requester	Status	Requested
□	privacy@example.org	Completed (3	11 mins ago



About

Report generated for	privacy@example.org
For site	Der Mundschenk & AMP
At URL	http://localhost
On	2019-04-07 17:01:43

User

User ID	9
User Login Name	privacy-test
User Nice Name	privacy-test
User Email	privacy@example.org
User Registration Date	2019-04-07 16:58:17
User Display Name	Privacy Test
User Nickname	privacy-test

DENIABLE ASSETS

- Images, videos, fonts, stylesheets, scripts
- Why you don’t want them to be external
  - external requests on the frontend transfer at least the IP address of the visitor
  - you can’t guarantee what third parties do with the data
  - having the assets on the same domain as the site is faster with modern browsers (HTTP/2)
  - remember: for site owners/visitors, you are a third party as well!
- Include all necessary images, fonts, and stylesheets in your plugin
- Only include JavaScript files if the library is not already shipped with WordPress Core
- Do not embed any videos in your plugin’s admin/settings page (helpful or not)
- Add a link instead (possibly an image link with a screenshot)

LIMITED EXPOSURE

- Only fill necessary fields for external services, not optional ones
- Only call external services/APIs when consent has been given by everyone
  - by the site-owner/admin (for optional features)
  - by the visitor (if call is not technically necessary for using that part of the site)
- When offering data via an API (e.g. the REST API)
  - need-to-know basis
  - limit visibility to admins by default

TO SERVE AND PROTECT – PART I

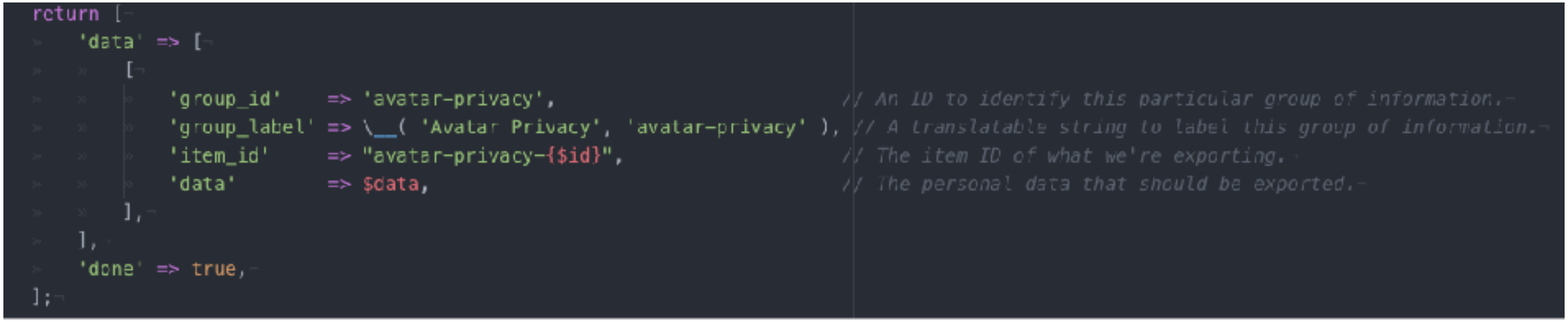
- Protect your users (that includes site-owners who have to comply with local legislation)
- Use TLS (formerly known as SSL, i.e. HTTPS) everywhere
  - Do not set `‘sslverify’=false` in WordPress HTTP API calls (no-one uses self-signed certificates anymore)
- Prepare for breaches – they will happen eventually
  - anonymize
  - pseudonymize
  - hashing
  - encryption

TO SERVE AND PROTECT – PART II

- Protect data integrity (and make breaches harder)
  - check nonces and actions (in forms or inbound API calls)
  - check user permissions
  - validate and sanitize input data
- Be careful to not write personal or sensitive data to log files
- Use PHPCS/WPCS to check for common pitfalls

EXPORT BUSINESS – PART I

- Users have a right to know what data is being collected about them (right of access)
- WordPress includes a Personal Data Exporter API
- Use `wp_privacy_personal_data_exporters` filter to add exporter function
- It’s best to use a separate function for each type of “data object”
- The function collects the data items and returns a nested array



```
return [
    'data' => [
        [
            'group_id'    => 'avatar-privacy',                                // An ID to identify this particular group of information.
            'group_label' => \__( 'Avatar Privacy', 'avatar-privacy' ), // A translatable string to label this group of information.
            'item_id'     => "avatar-privacy-{$id}",                          // The item ID of what we're exporting.
            'data'        => $data,                                           // The personal data that should be exported.
        ],
    ],
    'done' => true,
];
```

EXPORT BUSINESS – PART II

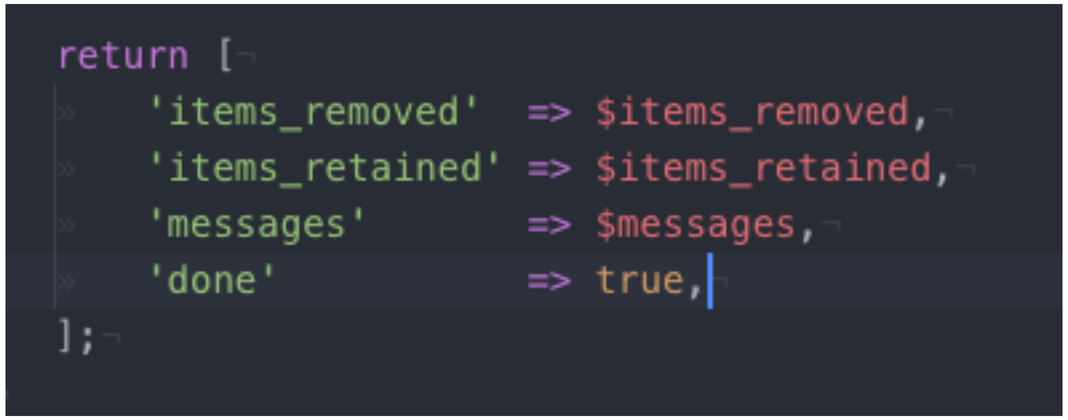
- Use your own groups if conceptually possible
- You can add to existing Core groups (like `comments`, `users`)
  - Omit the `group_label` field in that case
- `done` field can be false if you need paging to prevent timeouts
- Item data consists of `name` and `value` tuples

CLEANING UP – PART I

- Delete data that is not needed anymore (as soon as possible)
- Retention periods should be adjustable using filter hooks
- Delete data linked to an object (like a user account) when that object is deleted
  - This automatically happens when you use meta
  - Don’t forget custom tables!
- Provide a way to remove all data collected by the plugin
  - on plugin deletion (default behavior)
  - if that’s too dangerous, provide a clean-up button in the admin backend (and a corresponding WP-CLI command)
  - Don’t forget about multisite installations (WP-CLI might be the only solution)

CLEANING UP – PART II

- Personal Data Erasure API allows removal of data on email address level
- Similar to Exporter API
- Filter hook `wp_privacy_personal_data_erasers`
- You are responsible for deletion – WordPress only provides the mechanism
- Function returns data about deleted and retained items



```php
return [
    'items_removed'  => $items_removed,
    'items_retained' => $items_retained,
    'messages'       => $messages,
    'done'           => true,
];
```

WHERE DO WE GO FROM HERE?

- Standardization of disclosures in the WP.org plugin repository using README headers: Draft (GitHub)
- WP Consent API feature plugin
- Privacy Audit Workflow for Plugins: Draft (Google Docs)

WOULD YOU LIKE TO HELP?

- Join the Privacy team: https://make.wordpress.org/core/components/privacy/
- Weekly meetings on Slack (#core-privacy):
  - General office hours: Wednesday @ 19:00 UTC
  - Bug scrub: Monday @ 15:00 UTC
- Privacy Roadmap v2: https://make.wordpress.org/core/roadmap/privacy/

DO YOU HAVE ANY

QUESTIONS?

HOW TO CONTACT ME

- Twitter: @mundschenk_at
- Website: https://code.mundschenk.at
- Mail: code@mundschenk.at