WORDCAMP VIENNA 2019 | PETER PUTZER

PRIVACY CONSIDERATIONS FOR WORDPRESS SITES

WHAT I'M TALKING ABOUT TODAY

- WordPress, the software
- Focus on Core components
  - Only default themes
  - Plugins only as far as they are necessary for effective privacy management
- Technical aspects, not legal ones
- IANAL (this is not legal advice)

POTENTIAL ISSUES

- Differing priorities in Europe and the USA (Data Protection vs. Privacy)
- Legacy code (deeply integrated Automattic services like Gravatar)
- No “Privacy by Design”
- WordPress collects too much data (locally)
- (Unintended) data transmissions to third parties
- Difficult to fulfill legal obligations on data access and erasure

MEANWHILE AT WORDPRESS.ORG

- Only when GDPR was looming on the horizon
- New tools and APIs in WordPress 4.9.6 (May 2018)
- Privacy as a Core Component (https://make.wordpress.org/core/components/privacy/)
- Privacy Roadmap V2 (https://make.wordpress.org/core/roadmap/privacy/)
- Implementation has been delayed severely because of the focus on Gutenberg

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 …)

CHECKLIST – UNINTENDED DATA TRANSMISSIONS

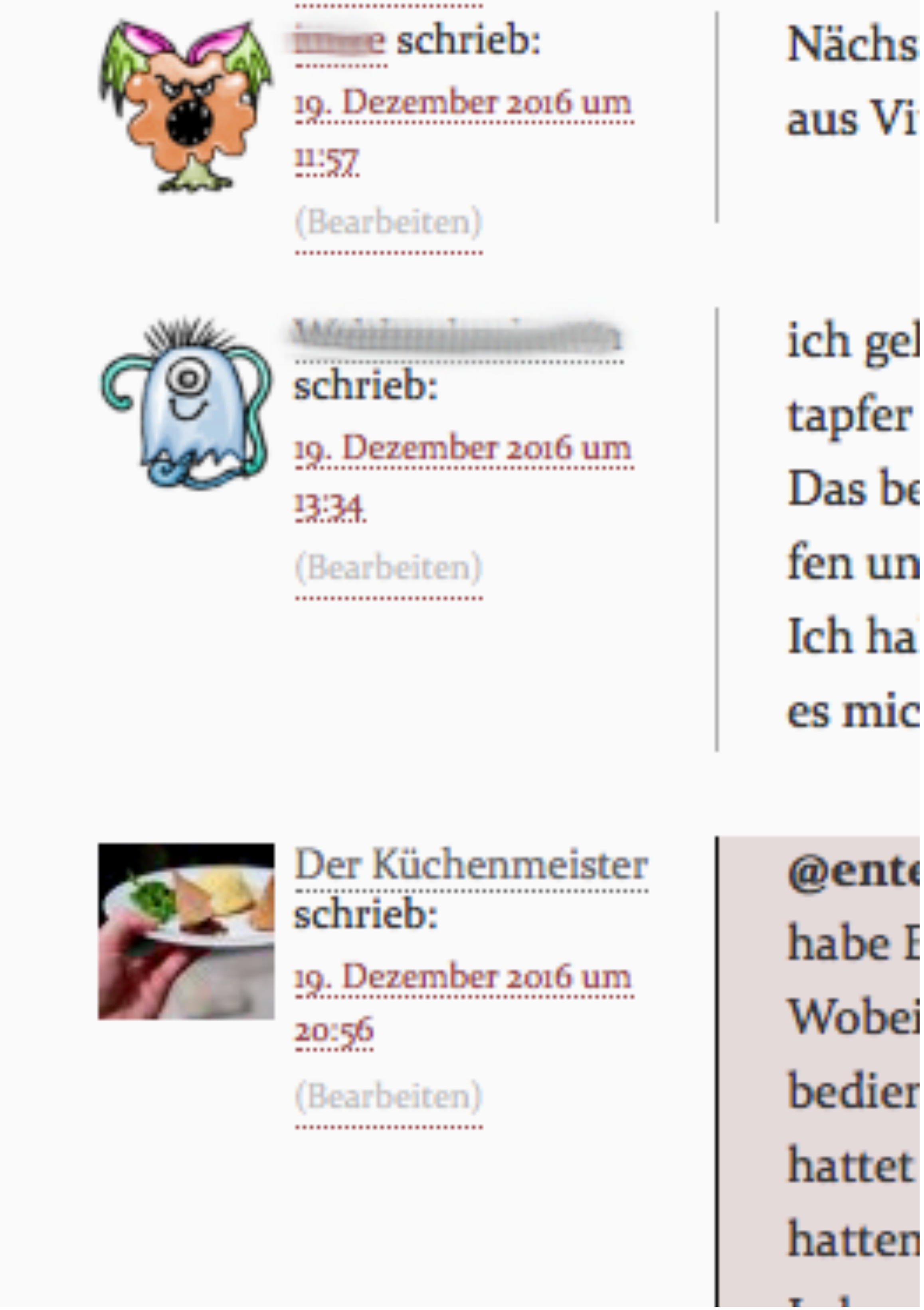
- Core
  - Gravatar (gravatar.com)
  - Embeds (youtube.com, twitter.com …)
  - Emojis (WordPress CDN s.w.org)
- Themes
  - Google Fonts
- Plugins
  - Akismet (akismet.com)
  - JetPack (jetpack.com)

CHECKLIST – OTHER TOPICS

- Data collection too extensive:
  - Comments
  - Contact forms
  - Analytics
- Fulfilling GDPR obligations
  - Right to be informed (data protection notice)
  - Right of access
  - Right of rectification
  - Right of erasure

ISSUE: GRAVATAR.COM — 1/2

- Cross-site profile pictures
- Queried via MD5 hash of email
- MD5 hashes are always made public, even if there's no Gravatar account for email
- Possible to reverse engineer email from MD5 hash (via rainbow tables or brute force)
- Danger of involuntary revealing identity



[redacted] schrieb:
19. Dezember 2016 um 11:57
(Bearbeiten)

Nächs
aus Vi

[redacted]
schrieb:
19. Dezember 2016 um 13:34
(Bearbeiten)

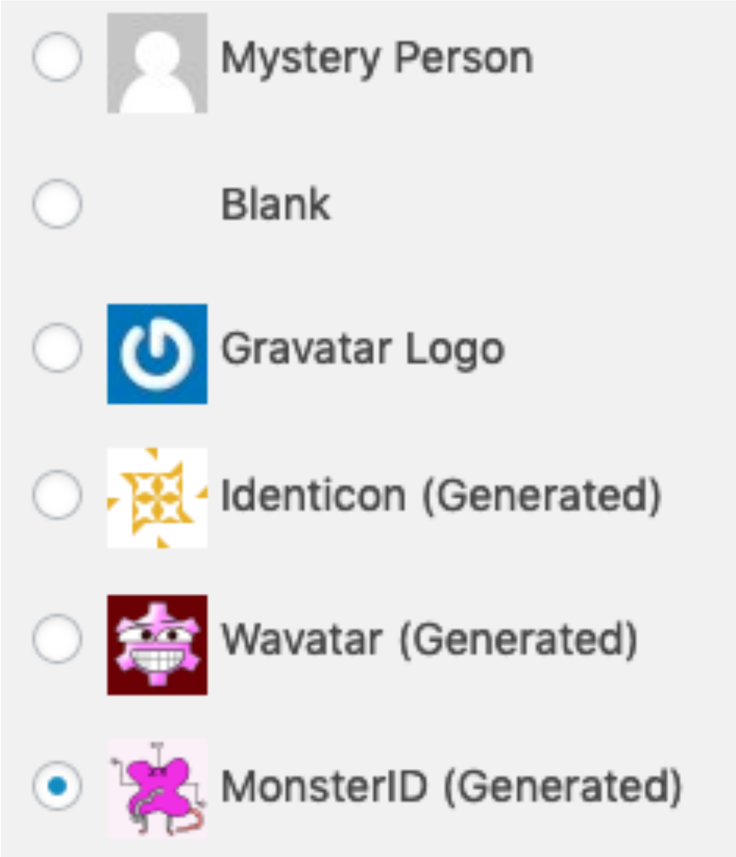
ich ge
tapfer
Das be
fen un
Ich ha
es mic

Der Küchenmeister
schrieb:
19. Dezember 2016 um 20:56
(Bearbeiten)

@ent
habe I
Wobei
bedien
hattet
hatten

ISSUE: GRAVATAR.COM — 2/2

- WordPress loads all profile pictures from gravatar.com, even static ones (e.g. "Mystery Person")
- Example URL: https://secure.gravatar.com/avatar/e43af6a00f69cc44461f6330aa7dc7a6?s=32&d=mm&r=g
- Identical images are loaded multiple times
- Equivalent to "tracking pixels"
- Possible solutions:
  - Settings/Discussion: Disable "Show Avatars"
  - Install the "Avatar Privacy" plugin:
    Consent, caching, self-hosted avatar and default images (https://wordpress.org/plugins/avatar-privacy/)



○ Mystery Person

○ Blank

○ Gravatar Logo

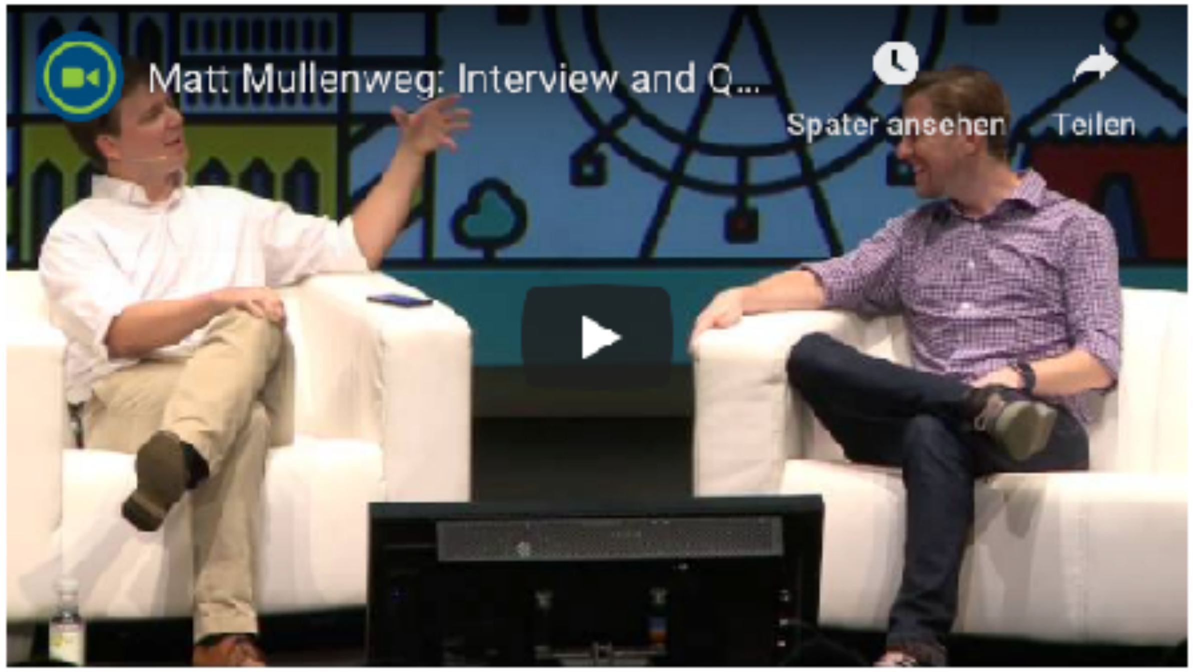
○ Identicon (Generated)

○ Wavatar (Generated)

● MonsterID (Generated)

ISSUE: EMBEDDING OF THIRD-PARTY SERVICES – 1/2

- Convenience feature with severe privacy implications: oEmbed
- Instead of displaying a “raw” URL in a post, the linked third-party service is embedded
- Embeds an IFRAME of the service (which could set/track cookies)
- https://www.youtube.com/watch?v=b1rTZJxEnAQ



ISSUE: EMBEDDING OF THIRD-PARTY SERVICES – 2/2

- No way to deactivate behavior from the backend
- Workaround: Don’t paste stand-alone URLs into your posts
- Technical solution: Put this code snippet into your functions.php

```
remove_filter( 'the_content',
array( $GLOBALS['wp_embed'], 'autoembed' ), 8 );
```

- Alternatively, install “Embed videos and respect privacy” (current version only available via GitHub https://github.com/michaelzangl/wp-video-embed-privacy)

ISSUE: EMOJIS 😳🦑🔮

- Since WordPress 4.2, a script is checking if the browsers supports emojis
- If not, fallback images are loaded from the WordPress.org CDN domain s.w.org
- Tor browser detects this as canvas fingerprinting
- Possible solutions:
  - Install “Disable Emojis” plugin (https://wordpress.org/plugins/disable-emojis)
  - Install “Local Emojis” plugin (https://wordpress.org/plugins/local-emoji/)

ISSUE: GOOGLE FONTS

- Many themes make use of Google Fonts, including many WordPress default themes (like Twenty Seventeen, Twenty Eighteen, Twenty Nineteen)
- Cannot be disabled (in most cases)
- Possible solutions:
  - Change theme
  - Install "Self-Hosted Google Fonts" plugin (https://wordpress.org/plugins/selfhost-google-fonts/)

ISSUE: AKISMET

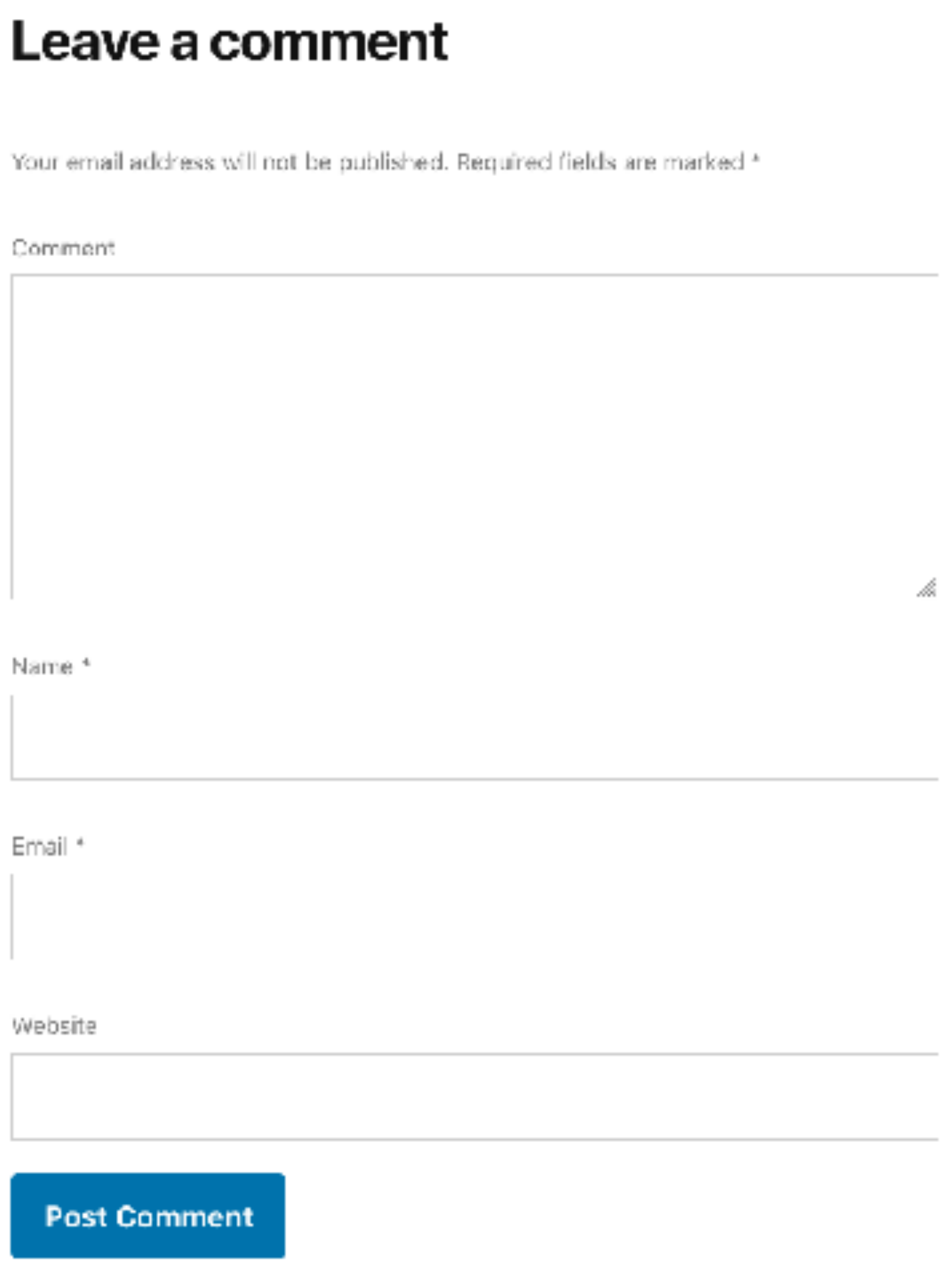
- Akismet Anti-Spam (spam filtering for comments) distributed with WordPress
- Problematic when used in Europe (comments are transmitted to Automattic servers in the USA)
- Alternative: Antispam Bee (https://wordpress.org/plugins/antispam-bee/)

ISSUE: JETPACK

- Many themes strongly urge you to use JetPack (especially those made by Automattic)
- "WordPress.com for self-hosted installations"
- Some modules are problematic (e.g. Statistics)
- Possible solutions:
  - Install "Statify" plugin (https://wordpress.org/plugins/statify/)
  - Install "Slimstat Analytics" plugin (https://wordpress.org/plugins/wp-slimstat/)

ISSUE: THE COMMENT FORM – 1/2

- WordPress comment form standard fields: comment, name, email, website URL
- Only name and comment are really needed
- Also stored:
  - IP address
    141.244.150.15
  - user-agent string
    Mozilla/5.0 (Windows NT 6.1; rv:12.0) Gecko/20100101 Firefox/12.0



Leave a comment

Your email address will not be published. Required fields are marked *

Comment

Name *

Email *

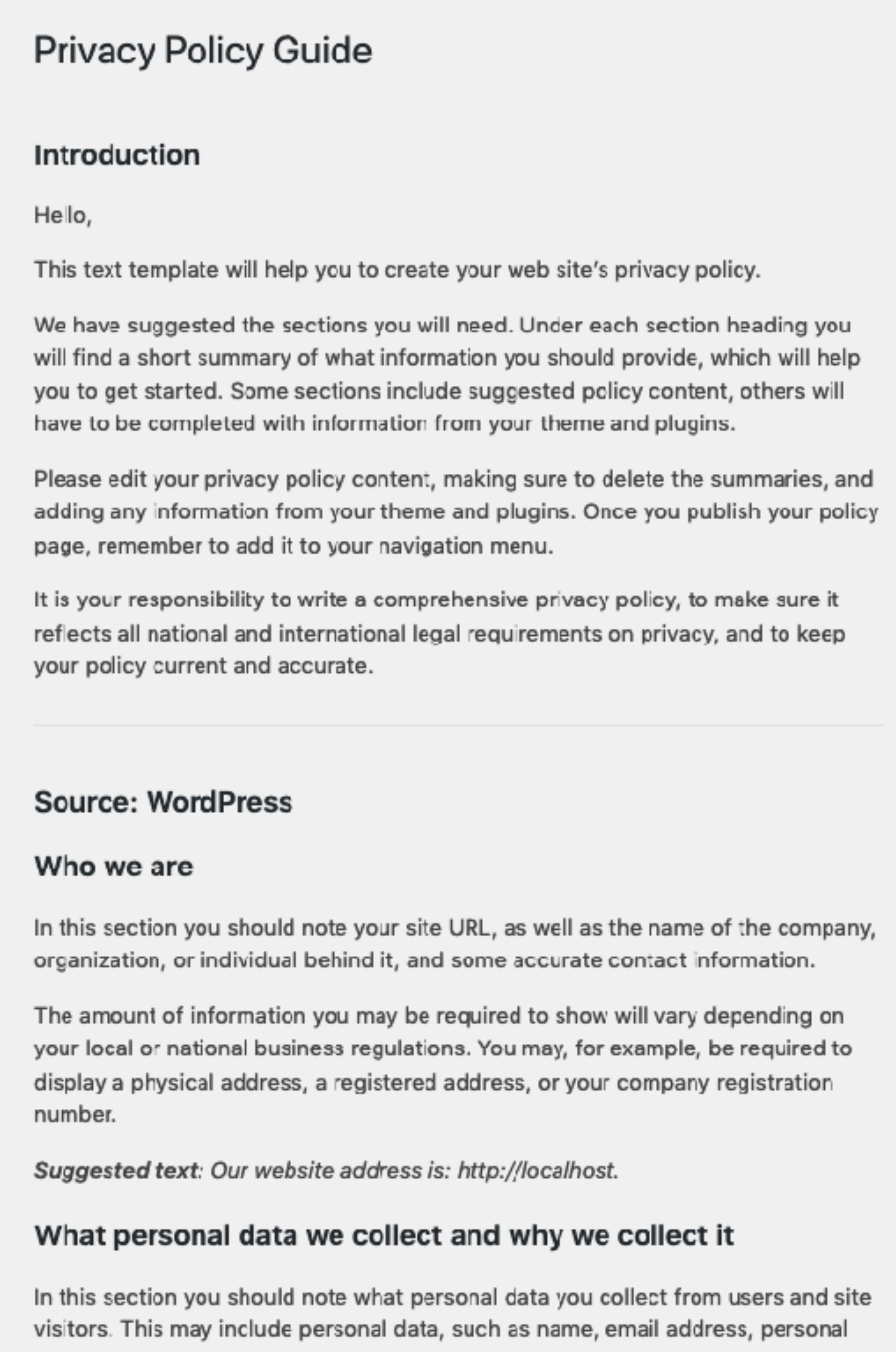
Website

ISSUE: THE COMMENT FORM — 2/2

- IP address can be anonymized via filter hooks
- Sometimes it is better to only delete/anonymize the IP address after a certain amount of time (evidence)
- Possible solution:
  - Install “Remove Comment IPs” plugin (https://wordpress.org/plugins/remove-comment-ips/)
- You should also include a link to the privacy notice

FULFILLING YOUR GDPR OBLIGATIONS

- New tools in WordPress 4.9.6
  - Guide for creating the privacy notice
  - Exporting personal data (right of access)
  - Deleting personal data (right of erasure)
- Plugins can hook into the tools
- Identity is checked via access to email account



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

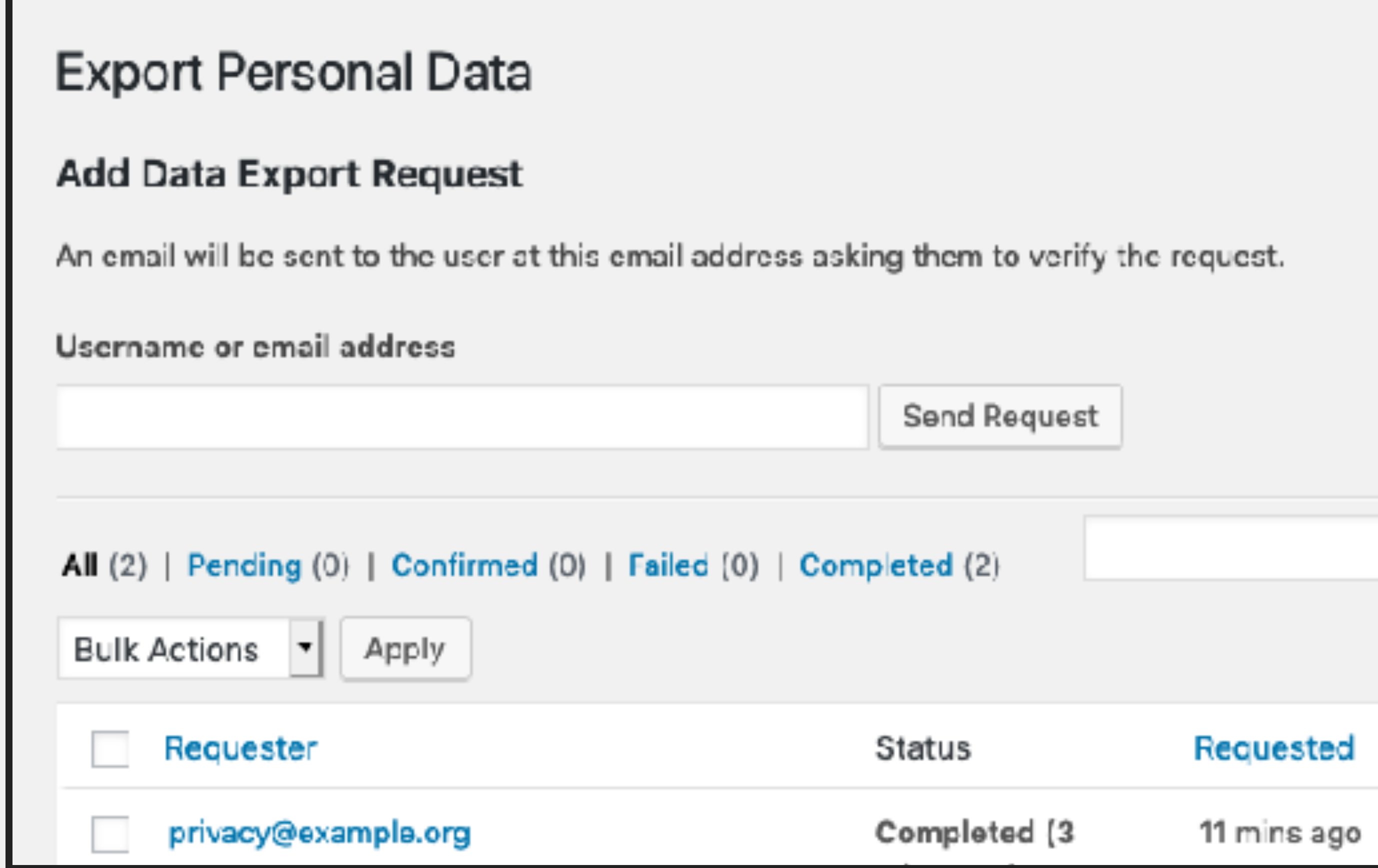
In this section you should note your site URL, as well as the name of the company, organization, or individual behind it, and some accurate contact information.

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

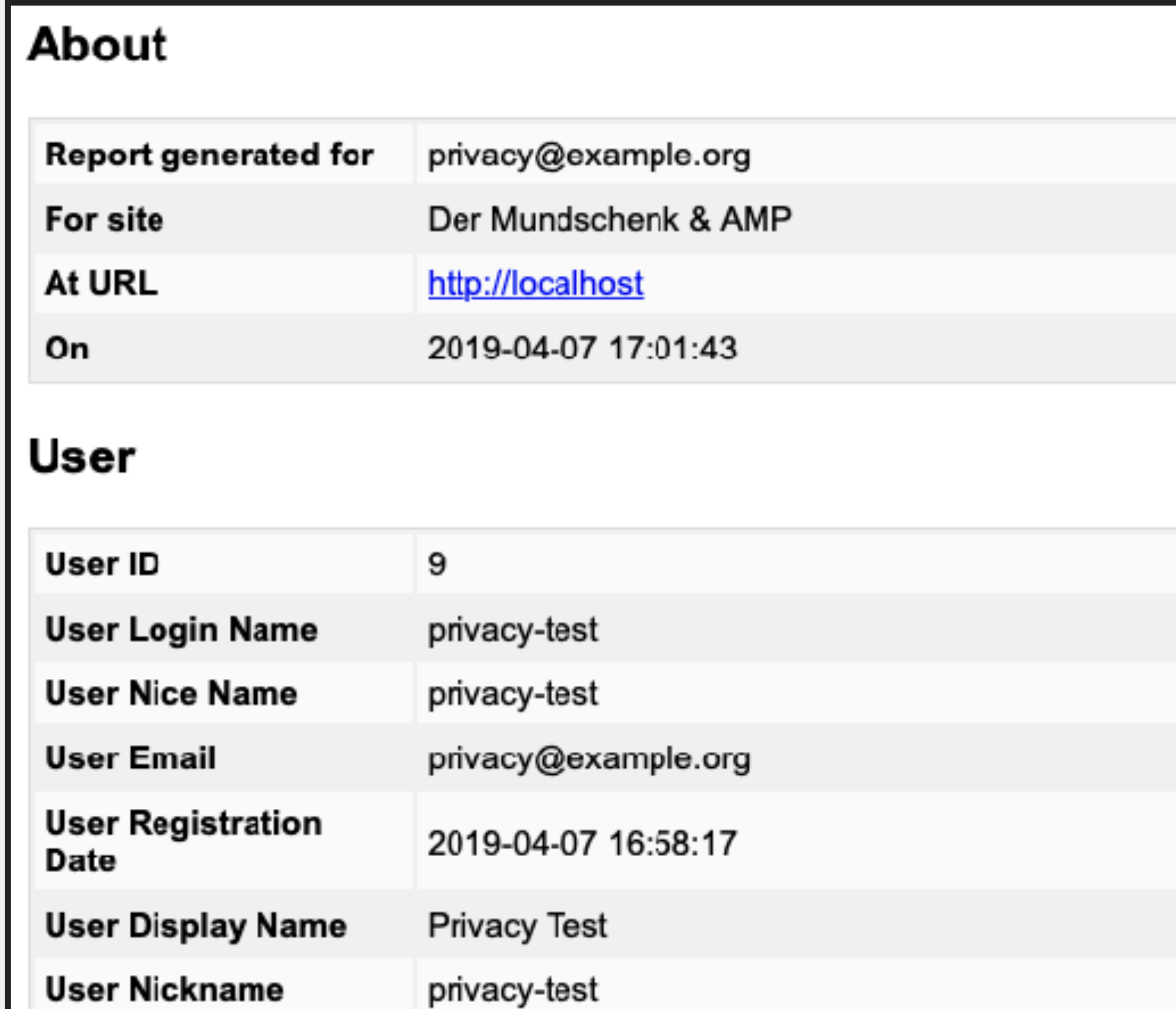
Add Data Export Request

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

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 for 2019: https://make.wordpress.org/core/roadmap/privacy/
- Privacy Audit Workflow for Plugins: Draft (Google Docs)

DO YOU HAVE ANY

QUESTIONS?

HOW TO CONTACT ME

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