WhatPrivacy?

~~

What Privacy ? Memo

v0

~~

save a tree, do not print!

INTRODUCTION
============

This memo IS NOT a roadmap.
It is just a draft to formalize what i have observed while testing wp privacy processes, coding exporters and erasers for a plugin as well as coding privacy requests posting with a dedicated mailbox.

COMMUNICATION
=============

Privacy is not to be considered as some boring legal stuff.
So let’s share the fun !

* Logo

I designed a logo (see cover) to summarize WP approach about privacy. As far as i understand, WP do not want to stick to GDPR – even if it can provide guidelines - but to offer tools to help websites to reach their compliance with their local laws.

* Dashicons

There are no dashicons related to privacy as listed in (github).
I propose three new dashicons for privacy :

privacy.svg

privacy-alt.svg

privacy-alt2.svg

* Mails

As the privacy processes relies on mails [is_email(), wp_mail()], it is important to know that :

- All mails are plaintext.
- wp_mail is referenced 29 times to generate 34 different mails (wp 5.1).

Mails have been developped at different periods of WordPress life. They are not all built with the same code approach. Not all of them can be customized.

- Pluggable : 7 (easy customization).
- In between : from apply_filters included in sprintf (wpmu legacy), message content and/sometimes mail subject filtered with some data, to an array with (to, subject, message, headers).
- No filters : 6 (no customization).

Privacy mails are in the «in between» zone.

see also annex I and CONCERNS topic

Annex I is just an extract of a next-to-come memo adressing mails in WP.

PROCESSES

* Settings

see ticket #43713 (use of Help panel)
hooks in privacy setting page ?

* Exporting (annex IIa)

a) Data export request posted (with an email or a name if registered).
b) mail sent to requester : «Confirm Action: Export Personal Data».
c) link confirmed.
d) mail sent to admin : «Action Confirmed: Export Personal Data».
e) admin goes to export_personal_data page and clicks on «Send Export Link» button :
  e.1) several ajax calls to generate the file locally
  e.2) zip file is copied to uploads/wp-personal-data-exports
  e.3) mail sent to requester : «Personal Data Export»
f) requester click on link to download zipfile (direct access).

g) admin can click on «Download Personal Data Again»
  g.1) same as e.1
  g.2) zip file available for download (exactly same name as e.2/e.3)

h) admin can click on «Remove request»
  g.1) request removed from list
  g.2) zip file still available (security issue ?)

* Erasing (annex IIb)

a) Data erase request posted (with an email or a name if registered).
b) mail sent to requester : «Confirm Action: Erase Personal Data».
c) link confirmed.
d) mail sent to admin : «Action Confirmed: Erase Personal Data».
e) admin goes to erase_personal_data page and clicks on «Erase Personal Data» button :
  e.1) several ajax calls to delete data
  e.2) several messages are displayed
  e.3) mail sent to requester : «Erasure Request Fulfilled»

If an export has been previously done, the zip file is still available ?

CONCERNS
========

* Mail content

You know how legal staff likes to put plenty of disclosures with an almost unreadable tiny font in the email footers (not possible with plaintext) … and to put a link to the data protection policy pages (privacy page in WP). Of course, «the Howdy» and «All at» are not really professional.
Those mails sent to requesters are also part of the communication policy of the website.

* Security

Apparently, when the admin (or dpo) ask to resend email or to Download Personnal Data, the zip file is not regenerated, and the old file is not suppressed (see export g.2).

* Collision

When an erase and export requests are posted at the same time …
   - erase request paused ? (the answer is no)
   - export request deleted if erase completed ? (the answer is no)

* Batch processing

When there is one or two requests a day, one mail per requester is manageable. What about ten’s of requests posted each day when a data breach has been detected ? (see *communication of a personal data breach to the data subject*)

* Accountability/Auditability

If i were a dpo, i would ask the system to have its specific log in order to prove in front of a court law, that a request as been posted at this time, processed at this time, etc … and who did what.

How can i have a trace if the objectives is to anonymize the email of the requester ?
To develop that kind of trace or log, it would require :
    - to set up hooks in core for all privacy related events (no more links to directly download a zip file)
    - to store all the privacy events and actions into a mysql table with a hashed email (using md5() for example), event_id, status of event, timestamp of event, useragent, ip address, any other information such as WP error message if any ...
So that when the dpo requests all actions for a specific email, the research is done with the hashed email (like a basic password verification).
    - from WP to insert in core code:

```
do_action( ‘wp_privacy_event’, $name_of_event, $status_of_event, $email …  );
```

whenever this is possible.

* Records of processing activities (GDPR prerequisite)

As WP somewhere «Records of processing activities» listed ?
see also Extensions/Documentation

* Communication of a personal data breach to the data subject (GDPR prerequisite)

I think 80% to 90% of security issues are coming from the inside. The more people have access to sensitive functionalities and/or data, the more your site is at risk.

- Prevent

Rely on trusted people first!
Apparently, Site health new Tools menu option [currently in trunk 5.2] can be used to fullfill part of that task.

- Detect

How ? Not easy ! Core ? Extensions ? External services ?

- Solve

Depend of what is at stake. see above …

– Communication

What tools ?
Sticky post (bad publicity), mass mailing (out of core), …

EXTENSIONS
==========

Extensions can be WP themes, WP plugins or any software uploaded by core or an extension or any external service.

* hook

As a plugin dev, i try as much as possible to code in oop (object oriented programming). Inside my plugins, i try to load code only when it is necessary.
I do not know all the hooks related to wp privacy (*to be found*).

There should be a specific do_action hook (**privacy_init**) before the wp_privacy_personal_data_exporters/erasers filters.
Today i load the apply_filters and the related code for exporters and erasers on the **admin_init** hook (not sure everybody does that).
Having a **privacy_init** hook would minimize code load when under admin and will allow the developper to load his code when and only when it is required.

```
do_action( 'privacy_init' );
```

* documentation

WP themes and plugins should have a == Privacy == section in readme.txt file. To show how the developer cares about data privacy (even if it is to say that the extension do not store/share data, do not use any external extension or service (js, font, image, …)).
For my MailPress plugin, i started to write that type of section.
The purpose is to inform the user of the extension as well as giving information to the dpo for his «Records of processing activities» (GDPR prerequisite).
Still under progress but just to give an idea see annex III.

ENHANCEMENTS

* Ergonomics

- Admin bar, admin menu, Help panel ...
(annex IV)

- Export/Erase Personal Data

The two admin pages are too similar. This can be the source of errors. There should be a different color in the background for Erasure Request screen (or maybe both). This could be an option hosted in the screen options panel.
(annex V)

* Roles and capabilities

The standard roles in wp are administrator, editor, author, contributor and subscriber. If for small websites, all theses roles are held by one person, for small or bigger organisations it might be interesting to create a new role : privacy_admin (or dpo), with specific access to privacy settings, privacy pages, privacy admin pages …

* Posting requests

I have seen this topic discussed in #44013: Add Basic Access and Deletion Front-end Request Forms as shortcodes/widgets/blocks.
The major problem with forms is spam, and mail bounces with fake emails.

WordPress allows posting via mail (Writing settings). There is a pop3 class for that. For my favorite plugin, i have coded an access via pop3 to a dedicated mailbox with a specific subject (nothing fancy : export or erase). The dedicated mailbox is scanned via wp_cron hook regularly.
(see annex VI).

But as i wrote in #44013, «*The major problem is that if you receive a mail from an email (the FROM mail header), the email complies with the web standards (RFC) but the request will be rejected due to is_email() that is not compliant with RFC rules*».
Not supporting web standards can become a serious legal issue
(see #46343 and #17491) and a criteria that would discard WP as a potential choice due to inability to reach full compliance

I also tried to bypass is_email() to post a request for **θσερ@εχαμπλε.ψομ** .
The request is inserted, but the data export fails (see annex VII)

CONCLUSION
==========

I could have filled several tickets on track, but I think writing this document is more consistant and the best way to share my view on this topic.
If there are some questions in the document, they are for me, to complete my investigations.
I am not expecting any answer on what I wrote.
I just wanted to share my thoughts on this topic.

Maybe some of my ideas have already been discussed, maybe they will bring other ideas … this work is yours now.

~~

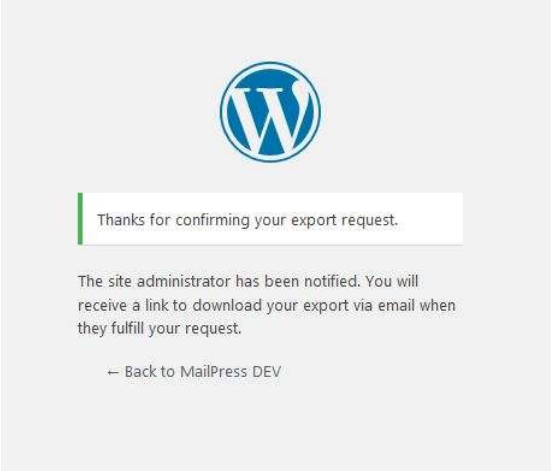
This memo can be downloaded here.

The original .odt and .svg files are available here.

Annexe I – Mails

file	line	function	title
wp-includes/user.php	2011	wp_update_user	'[%s] Notice of Password Change'
wp-includes/user.php	2070	wp_update_user	'[%s] Notice of Email Change'
wp-includes/user.php	2815	send_confirmation_on_profile_email	'[%s] New Email Address'
wp-includes/user.php	3117	_wp_privacy_send_request_confirmation_notification()	'[%1$s] Action Confirmed: %2$s'
wp-includes/user.php	3254	_wp_privacy_send_request_confirmation_notification	'[%s] Erasure Request Fulfilled'
wp-includes/user.php	3509	wp_send_user_request	'[%1$s] Confirm Action: %2$s'
wp-admin/user-new.php	125		'[%s] Joining confirmation'
wp-login.php	422	retrieve_password	'[%s] Password Reset'
wp-admin/ms-delete-site.php	81		'Delete My Site'
wp-includes/functions.php	6526	wp_site_admin_email_change_notification	'[%s] Notice of Admin Email Change'
wp-includes/pluggable.php	1637	wp_notify_postauthor	'[%1$s] Trackback: "%2$s"'
wp-includes/pluggable.php	1637	wp_notify_postauthor	'[%1$s] Pingback: "%2$s"'
wp-includes/pluggable.php	1637	wp_notify_postauthor	'[%1$s] Comment: "%2$s"'
wp-includes/pluggable.php	1808	wp_notify_moderator	'[%1$s] Please moderate: "%2$s"'
wp-includes/pluggable.php	1863	wp_password_change_notification	'[%s] Password Changed'
wp-includes/pluggable.php	1945	wp_new_user_notification	'[%s] New User Registration'
wp-includes/pluggable.php	2011	wp_new_user_notification	'[%s] Your username and password info'
wp-admin/includes/upgrade.php	611	wp_new_blog_notification	'New WordPress Site'
wp-admin/network/site-new.php	145		'[%s] New Site Created'
wp-admin/includes/misc.php	1294	update_option_new_admin_email	'[%s] New Admin Email Address'
wp-includes/ms-functions.php	987	wpmu_signup_blog_notification	'[%1$s] Activate %2$s', 'New site notification email subject'
wp-includes/ms-functions.php	1092	wpmu_signup_user_notification	'[%1$s] Activate %2$s', 'New user notification email subject'
wp-includes/ms-functions.php	1401	newblog_notify_siteadmin	'New Site Registration: %s'
wp-includes/ms-functions.php	1453	newuser_notify_siteadmin	'New User Registration: %s'
wp-includes/ms-functions.php	1611	wpmu_welcome_notification	'New %1$s Site: %2$s'
wp-includes/ms-functions.php	1702	wpmu_welcome_user_notification	'New %1$s User: %2$s'
wp-includes/ms-functions.php	2719	update_network_option_new_admin_email	'[%s] New Network Admin Email Address'
wp-includes/ms-functions.php	2814	wp_network_admin_email_change_notification	'[%s] Notice of Network Admin Email Change'
wp-admin/includes/file.php	2247	wp_privacy_send_personal_data_export_email	'[%s] Personal Data Export'
wp-admin/includes/class-wp-automatic-updater.php	816	send_email	'[%1$s] Your site has updated to WordPress %2$s'
wp-admin/includes/class-wp-automatic-updater.php	816	send_email	'[%1$s] WordPress %2$s is available. Please update!'
wp-admin/includes/class-wp-automatic-updater.php	816	send_email	'[%1$s] URGENT: Your site may be down due to a failed update'
wp-admin/includes/class-wp-automatic-updater.php	987	send_debug_email	'[%s] There were failures during background updates'
wp-admin/includes/class-wp-automatic-updater.php	987	send_debug_email	'[%s] Background updates have finished'

step c



Thanks for confirming your export request.

The site administrator has been notified. You will receive a link to download your export via email when they fulfill your request.

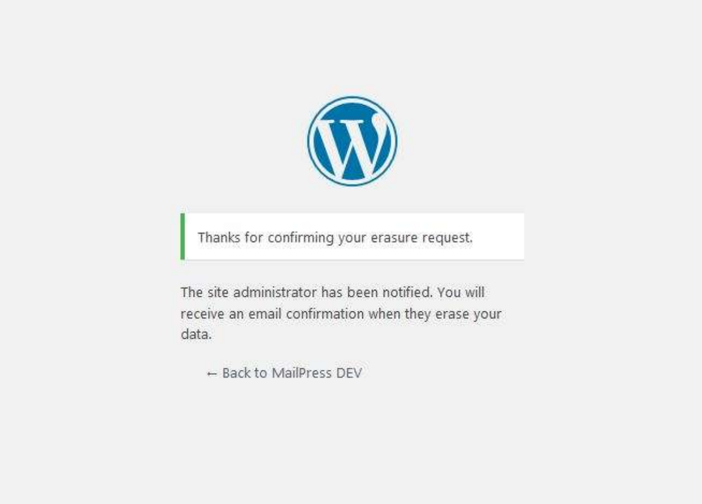
This message looks like a WP message : "When they fullfill your request" is inappropiate.

"We have been notified. You will receive a link to download your data via email once your request is processed" is better.

I don't know if in WordPress core this kind of message can be "themed" like a 404.php template.

Annexe IIb – Erase

step c



Thanks for confirming your erasure request.

The site administrator has been notified. You will receive an email confirmation when they erase your data.

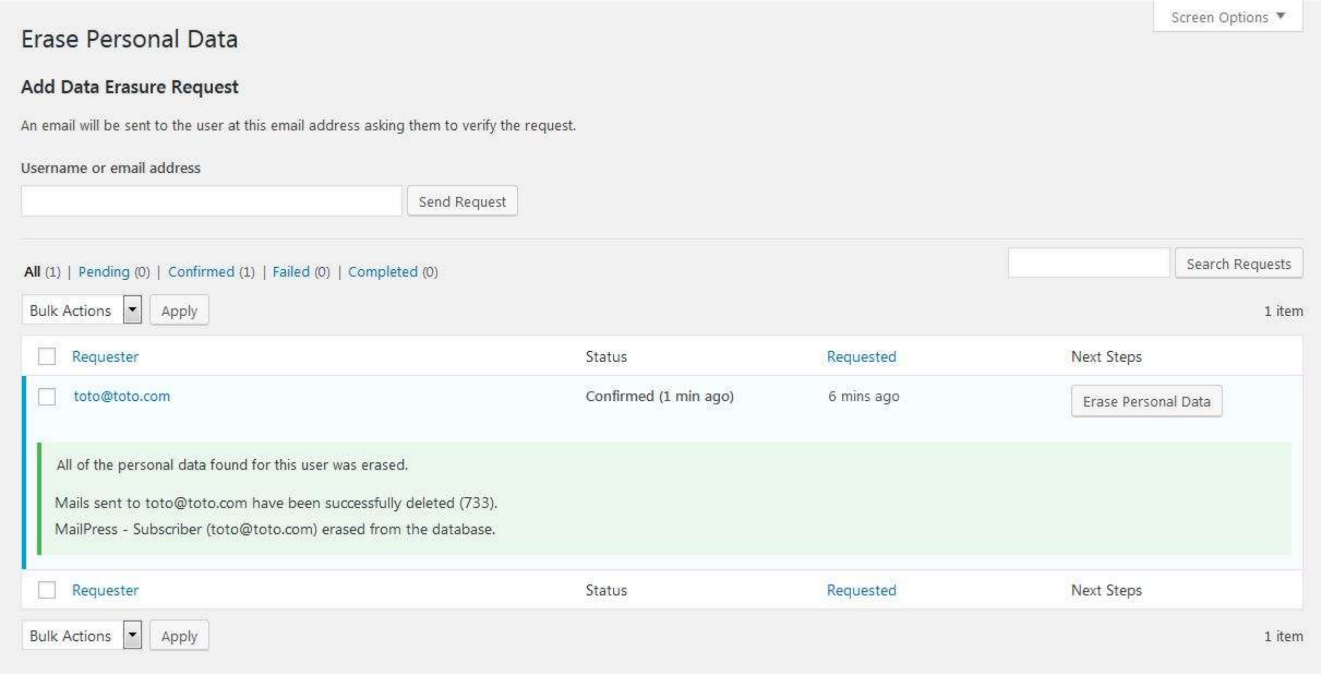
This message looks like a WP message :

“When they erase your data” is inappropiate.

“We have been notified. You will receive an email confirmation once your request is processed” is better.

I don’t know if in WordPress core this kind of message can be “themed” like a 404.php template.

step e.2



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

Send Request
All (1) | Pending (0) | Confirmed (1) | Failed (0) | Completed (0)
Search Requests
Bulk Actions ▾ Apply

1 item

□	Requester	Status	Requested	Next Steps
□	toto@toto.com	Confirmed (1 min ago)	6 mins ago	Erase Personal Data
□	Requester	Status	Requested	Next Steps

All of the personal data found for this user was erased.

Mails sent to toto@toto.com have been successfully deleted (733).

MailPress - Subscriber (toto@toto.com) erased from the database.

1 item

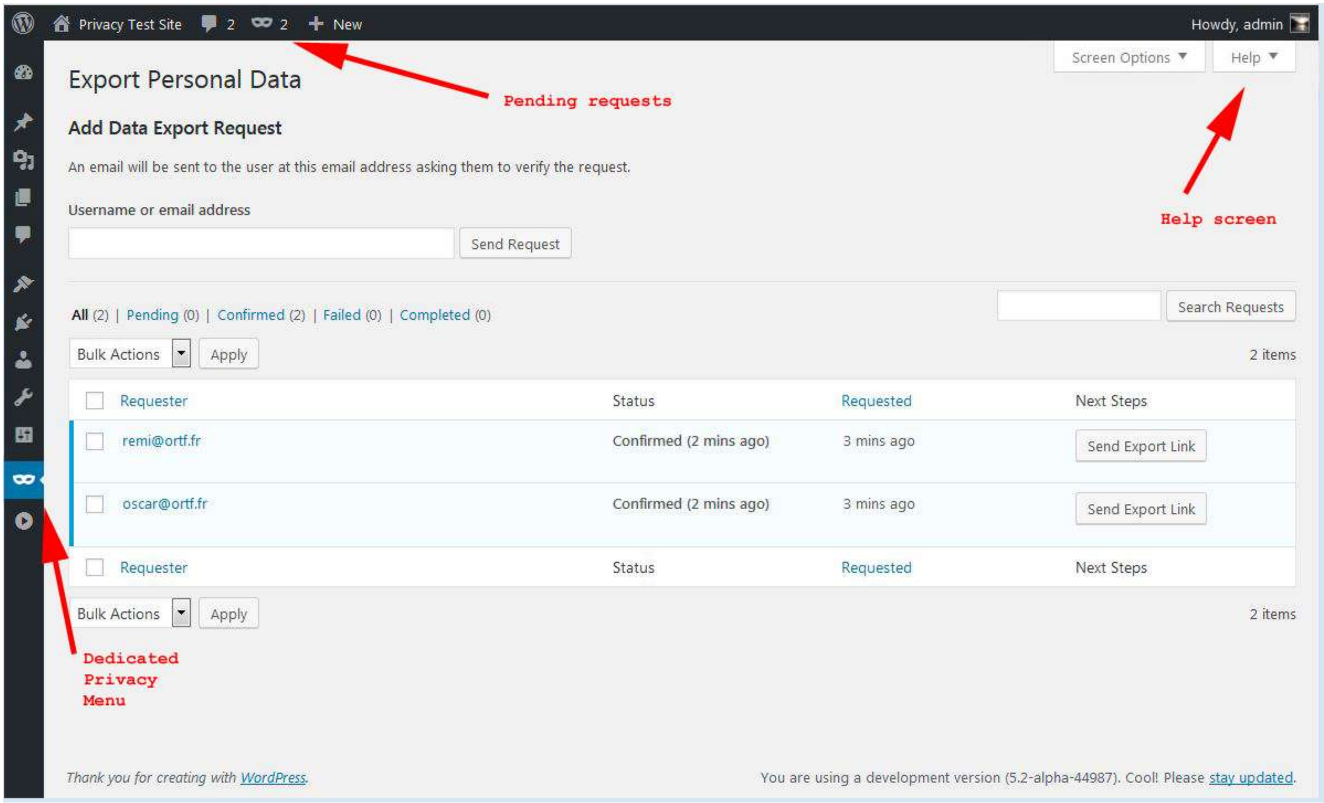
Annexe III – Privacy section in readme.txt

(still under progress)

```
== Privacy ==

This plugin is using the following external softwares :
1. Swiftmailer "Free Feature-rich PHP Mailer" (https://swiftmailer.symfony.com/)
       2. doctrine/lexer "Base library for a lexer" (https://github.com/doctrine/lexer)
       2. egulias/EmailValidator "PHP Email validator"
(https://github.com/egulias/EmailValidator)
1. [Import Addon] Excel parsing library (http://code.google.com/p/php-excel-reader/)
modified for php7 compatibility
1. [Import Addon] CSV parsing library   (https://github.com/parsecsv/parsecsv-for-php)
modified for php7 compatibility

This plugin is using - depending on your settings - the following external services &
softwares
1. [Maps] Bing maps (https://www.microsoft.com/en-us/maps) (javascript and REST api)
1. [Maps] Google maps (https://cloud.google.com/maps-platform/?hl=en) (javascript and REST
api)
1. [Maps] Here maps (https://www.here.com/) (javascript and REST api)
1. [Maps] Mapbox GL JS (https://docs.mapbox.com/mapbox-gl-js/api/) (javascript and REST
api)
1. [Maps] OpenStreetMaps and Leaflet (https://www.openstreetmap.org &
https://leafletjs.com/) (javascript and REST api)

This plugin is using - randomly - the following external services (ip adress transmitted)
1. [Ip Geocoding] https://extreme-ip-lookup.com/ (REST Api)
1. [Ip Geocoding] http://www.geoplugin.net/ (REST Api)
1. [Ip Geocoding] https://ipapi.co (REST Api)
1. [Ip Geocoding] http://ip-api.com/ (REST Api)
1. [Ip Geocoding] http://ipinfo.io/ (REST Api)
1. [Ip Geocoding] https://ipstack.com/ (REST Api)

This plugin is storing data
1. [core] Subscribers
1. [core] Mails and recipients informations
1. [Comment addon] Subscriptions
1. [Mailinglist addon] Subscriptions
1. [Newsletter addon] Subscriptions
1. [Tracking addon] any activity on sent mails when clicking on mail links

This plugin authorize data export in csv format [Import addon]

For any privacy questions on external services, please refer to their privacy policy.
```

Annex IV – Ergonomics

Admin bar, admin menu, Help panel ...



Export Personal Data

Pending requests

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

Help screen

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

Search Requests

Bulk Actions ▾ Apply

2 items

□ Requester	Status	Requested	Next Steps
□ remi@ortf.fr	Confirmed (2 mins ago)	3 mins ago	Send Export Link
□ oscar@ortf.fr	Confirmed (2 mins ago)	3 mins ago	Send Export Link
□ Requester	Status	Requested	Next Steps

Bulk Actions ▾ Apply

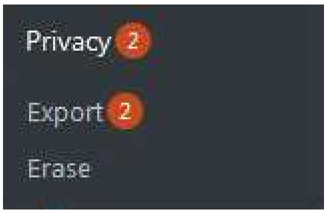
2 items

Dedicated Privacy Menu

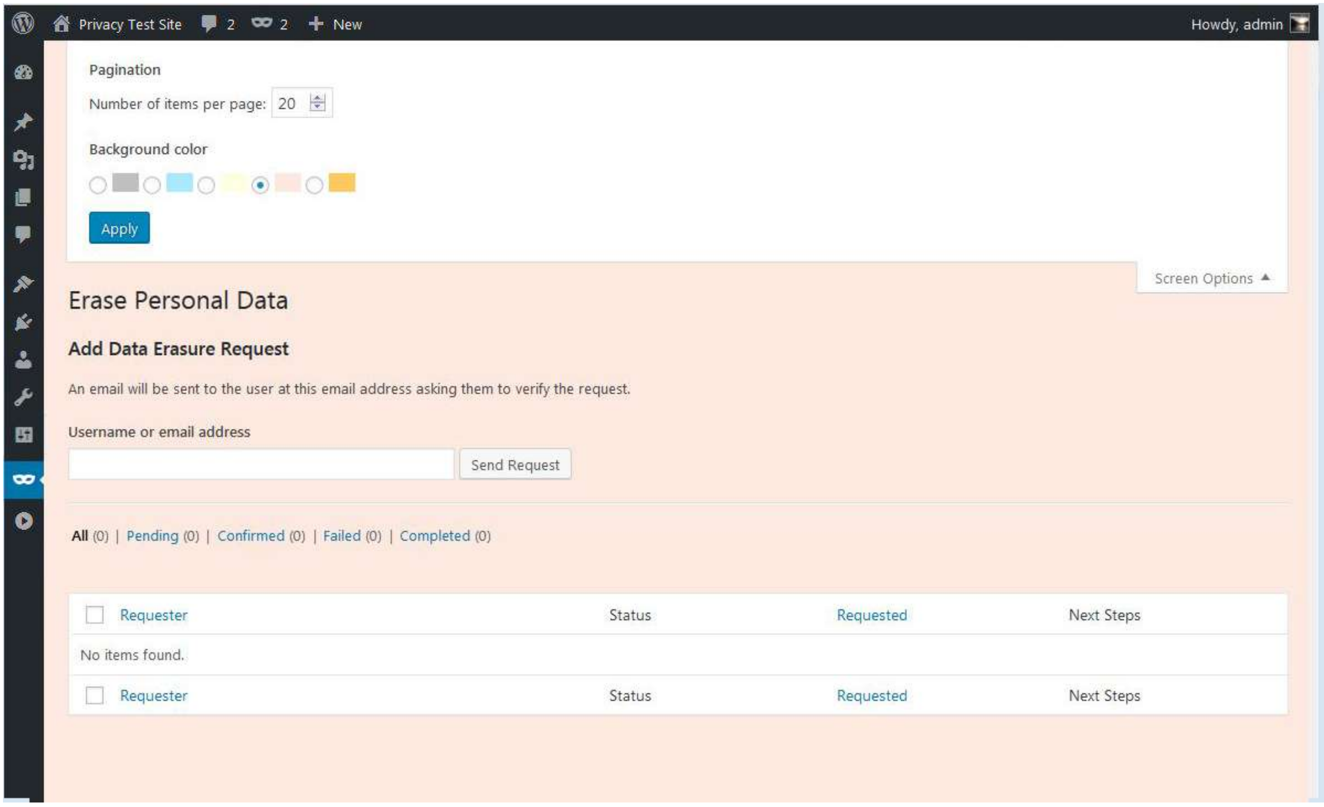
Thank you for creating with WordPress.

You are using a development version (5.2-alpha-44987). Cool! Please stay updated.

Menu detail



different background colors



Pagination

Number of items per page: 20

Background color

○ ▨ ○ 🟦 ○ ▨ ● 🟥 ○ 🟨

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.

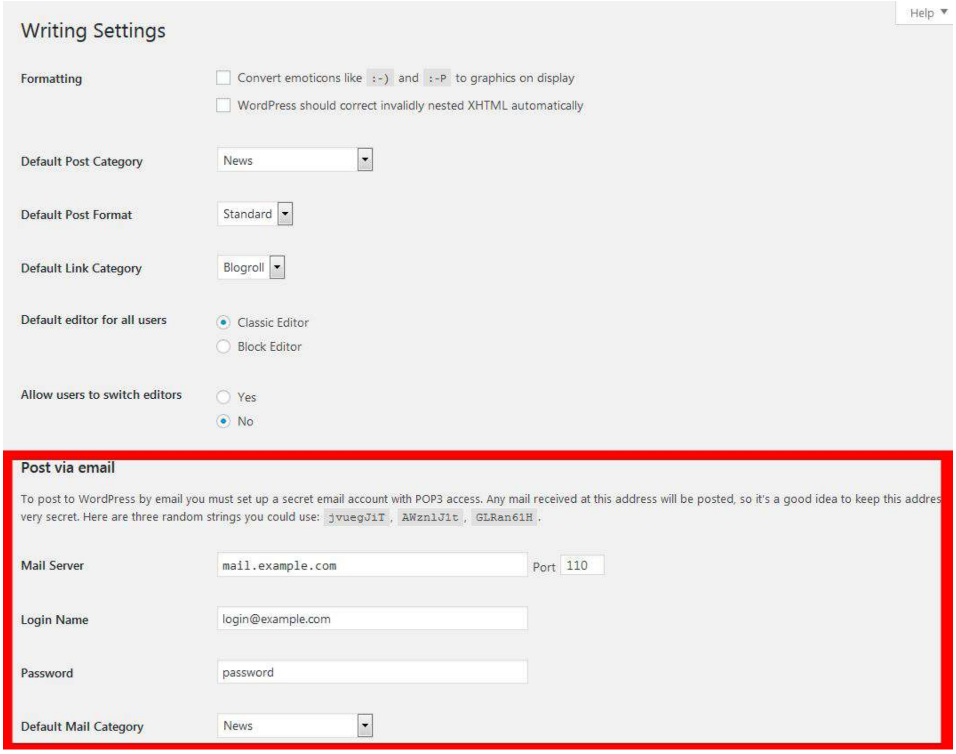
Username or email address

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

□ Requester	Status	Requested	Next Steps
No items found.			
□ Requester	Status	Requested	Next Steps

Annexe VI – Posting requests

WordPress Writing settings



Help ▾

Writing Settings

Formatting
□ Convert emoticons like `:-)` and `:-P` to graphics on display
□ WordPress should correct invalidly nested XHTML automatically

Default Post Category: News

Default Post Format: Standard

Default Link Category: Blogroll

Default editor for all users
● Classic Editor
○ Block Editor

Allow users to switch editors
○ Yes
● No

Post via email

To post to WordPress by email you must set up a secret email account with POP3 access. Any mail received at this address will be posted, so it's a good idea to keep this addres
very secret. Here are three random strings you could use: `jvuegJiT`, `AWznlJ1t`, `GLRan61H`.

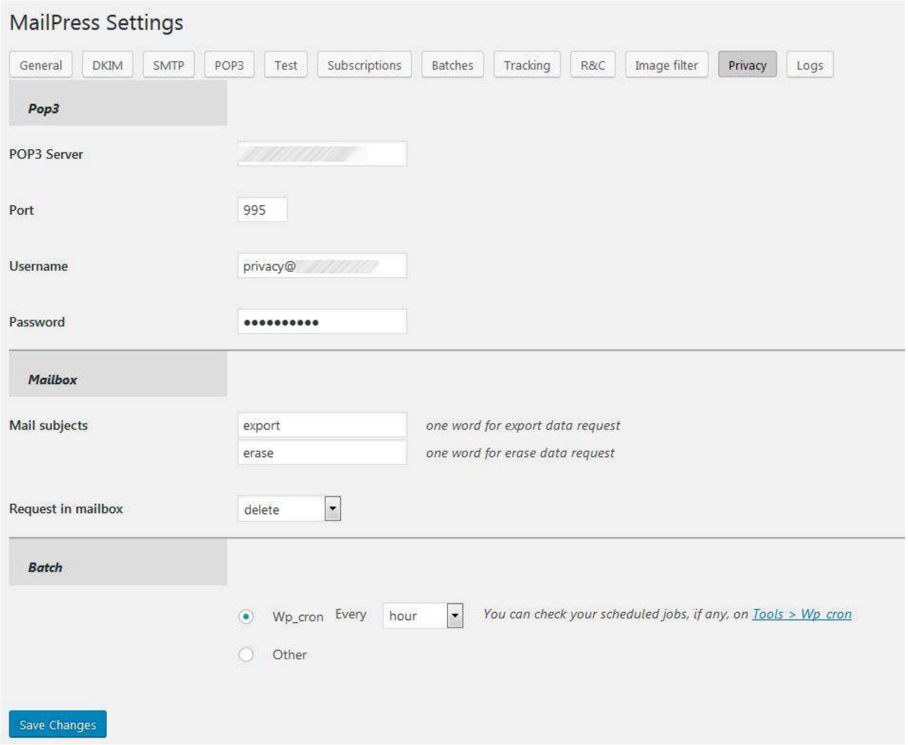
Mail Server: mail.example.com Port 110

Login Name: login@example.com

Password: password

Default Mail Category: News

Plugin privacy settings



MailPress Settings

Pop3

POP3 Server: [redacted]

Port: 995

Username: privacy@[redacted]

Password: ••••••••••

Mailbox

Mail subjects
export — *one word for export data request*
erase — *one word for erase data request*

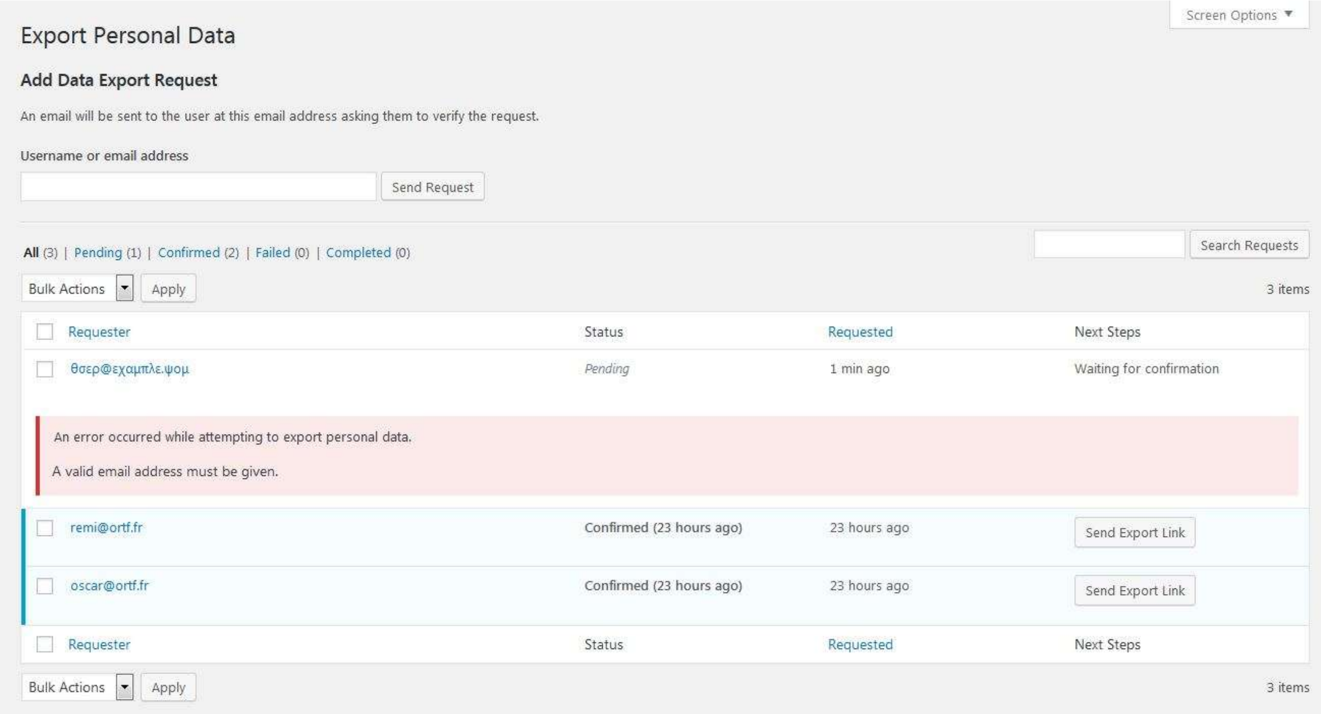
Request in mailbox: delete

Batch

● Wp_cron Every hour *You can check your scheduled jobs, if any, on Tools > Wp cron*
○ Other

Annexe VII - bypass is_email result

θσερ@εχαμπλε.ψομ is a valid email address !



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 (3) | Pending (1) | Confirmed (2) | Failed (0) | Completed (0)

3 items

□	Requester	Status	Requested	Next Steps
□	θσερ@εχαμπλε.ψομ	*Pending*	1 min ago	Waiting for confirmation
	An error occurred while attempting to export personal data. A valid email address must be given.			
□	remi@ortf.fr	Confirmed (23 hours ago)	23 hours ago	Send Export Link
□	oscar@ortf.fr	Confirmed (23 hours ago)	23 hours ago	Send Export Link
□	Requester	Status	Requested	Next Steps

3 items