Akeeba Data Compliance

Nicholas K. Dionysopoulos

Akeeba Data Compliance

by Nicholas K. Dionysopoulos

Table of Contents

I. User's Guide 1
1. Introduction 3
1. Introducing Akeeba Data Compliance 3
2. Server environment requirements 3
3. Technology overview 3
2. Installation, updates and upgrades 5
1. Installing Akeeba Data Compliance 5
1.1. Installing or manually updating the extension 5
1.1.1. Install from URL 5
1.1.2. Upload and install. 6
2. Automatic updates 6
3. Using Akeeba Data Compliance 8
1. Initial setup 8
2. Managing personal information 9
2.1. Captive login (consent page) in the front-end 10
2.2. Self-service page 11
2.3. Managing users' personal information from the backend 13
3. Dashboard (a.k.a. Control Panel) page 15
4. Setting up the email templates 17
5. Managing audit trails 19
5.1. User Consents 19
5.2. Profile Changes 19
5.3. Data Exports 19
5.4. Profile Deletions 19
6. Managing data actions 20
6.1. Expired user profiles 20
7. Automating data minimization actions 20
7.1. Notify users before their profile is automatically deleted 21
7.2. Automatically delete expired user profiles 21
8. Configuration 22
8.1. Component configuration 22
8.2. System plugin configuration 23
8.3. Data sources configuration (`datacompliance` plugins) 23
8.3.1. Joomla! Core User Data 23
8.3.2. Akeeba Subscriptions 24
8.3.3. Akeeba Release System 24
8.3.4. Akeeba Ticket System 24
8.3.5. Akeeba LoginGuard 25
8.4. Other plugins 25
8.4.1. The User plugin 25
8.4.2. Send emails on account deletion 25
8.4.3. Upload user deletion audit trail to Amazon S3 26
9. Other CLI tools 27
9.1. Delete a user from the CLI 27
4. Developer's reference 28
1. Translating 28
2. Interface customization / templating 28
3. Creating data source plugins 28
4. Creating other integration plugins 28
II. Appendices 29
A. GNU Free Documentation License 31

Part I. User's Guide

Table of Contents

1. Introduction 3
    1. Introducing Akeeba Data Compliance 3
    2. Server environment requirements 3
    3. Technology overview 3
2. Installation, updates and upgrades 5
    1. Installing Akeeba Data Compliance 5
        1.1. Installing or manually updating the extension 5
            1.1.1. Install from URL 5
            1.1.2. Upload and install. 6
    2. Automatic updates 6
3. Using Akeeba Data Compliance 8
    1. Initial setup 8
    2. Managing personal information 9
        2.1. Captive login (consent page) in the front-end 10
        2.2. Self-service page 11
        2.3. Managing users' personal information from the backend 13
    3. Dashboard (a.k.a. Control Panel) page 15
    4. Setting up the email templates 17
    5. Managing audit trails 19
        5.1. User Consents 19
        5.2. Profile Changes 19
        5.3. Data Exports 19
        5.4. Profile Deletions 19
    6. Managing data actions 20
        6.1. Expired user profiles 20
    7. Automating data minimization actions 20
        7.1. Notify users before their profile is automatically deleted 21
        7.2. Automatically delete expired user profiles 21
    8. Configuration 22
        8.1. Component configuration 22
        8.2. System plugin configuration 23
        8.3. Data sources configuration (`datacompliance` plugins) 23
            8.3.1. Joomla! Core User Data 23
            8.3.2. Akeeba Subscriptions 24
            8.3.3. Akeeba Release System 24
            8.3.4. Akeeba Ticket System 24
            8.3.5. Akeeba LoginGuard 25
        8.4. Other plugins 25
            8.4.1. The User plugin 25
            8.4.2. Send emails on account deletion 25
            8.4.3. Upload user deletion audit trail to Amazon S3 26
    9. Other CLI tools 27
        9.1. Delete a user from the CLI 27
4. Developer's reference 28
    1. Translating 28
    2. Interface customization / templating 28
    3. Creating data source plugins 28
    4. Creating other integration plugins 28

Chapter 1. Introduction

1. Introducing Akeeba Data Compliance

Akeeba Data Compliance is a simple to use solution for compliance with the European Union's General Data Protection Regulation (GDPR) which came into effect May 25th, 2018. It allows you to easily handle users giving or revoking their consent to data processing, as well as provide a self-service approach to data export and user profile deletion. Further to that it can help you with the data minimization requirements of GDPR by deleting inactive user profiles automatically, after users are suitably notified.

Akeeba Ltd has chosen not to charge a fee for this software and its documentation. However, we cannot guarantee user support or customization (including implementation of features we don't need on our own site). Thank you for your understanding!

2. Server environment requirements

In order to work, Akeeba Data Compliance requires the following server software environment:

- Joomla!™ and PHP version compatibilities are detailed in our Compatibility page [https://www.akeebabackup.com/compatibility.html]. At the time of this writing the minimum requirements are PHP 7.1 or later and Joomla! 3.8 or later.
- MySQL 5.6 or later. Akeeba DataCompliance does not support PostgreSQL and Microsoft SQL Server / Azure SQL Server databases.
- 32MB of PHP memory_limit. At least 128MB recommended for best performance.
- Ability to run **command line** CRON jobs. If your host only allows you to call a URL you will not be able to use the data minimization features.

As far as the browser is concerned, you can use any modern version (i.e. published within the last year) of Microsoft Edge, Safari, Opera, Firefox or Google Chrome. We no longer support Internet Explorer; our software will display incorrectly or not work at all on this old, buggy and obsolete browser.

In any case, you must make sure that Javascript is enabled on your browser for the backup to work. If you are using AVG antivirus, please disable its Link Checker feature (and reboot your computer) as it is known to cause problems.

You are very strongly advised to disable Internet firewalls, antivirus applications and browser extensions which interfere with the site's loading such as script blockers (such as NoScript) and ad blockers (such as AdBlockPlus) *only for the domains you are using the software on*. Remember that these applications and browser extensions are designed to protect you against third party sites. As a result they are very aggressive and WILL break your own sites. We can't do anything about it: your computer and your browser are under your control alone.

3. Technology overview

Akeeba DataCompliance is more than just a component. In fact, its component is only used to render the interface and handle some common work. Most of the features are implemented as plugins to ensure extensibility, even by third parties.

The System - Data Compliance plugin is used to implement the captive login page which requires your clients to give their consent to data processing before continuing to use your site.

The User - Data Compliance plugin is used to add links to Data Compliance in user profiles and handle other aspects of data processing consent.

There are a number of plugins of the `datacompliance` type. These are the integrations with personal information data sources, i.e. Joomla itself and third party components. Each of these plugins informs Data Compliance of the personal information kept for each user, lets it delete this information, informs Data Compliance whether a user profile can be deleted and provides information about which profiles are to be considered expired. Data Compliance ships with a number of plugins for core Joomla! and Akeeba extensions. The API is open and any third party developer can create their own plugins for their software.

Chapter 2. Installation, updates and upgrades

1. Installing Akeeba Data Compliance

Installing Akeeba Data Compliance is no different than installing any other Joomla!™ extension on your site. You can read the complete instructions for installing Joomla!™ extensions on the official help page [https://docs.joomla.org/Installing_an_extension]. Throughout this chapter we assume that you are familiar with these instructions and we will try not to duplicate them.

1.1. Installing or manually updating the extension

Just like with most Joomla! extensions there are two ways to install or manually update Akeeba Data Compliance on your site:

- Install from URL. It is the easiest and fastest one, if your server supports it. Most servers do support this method.
- Upload and install. That's the typical extension installation method for Joomla! extensions. It rarely fails.

Please note that installing and updating Akeeba Data Compliance (and almost all Joomla! extensions) is actually the same thing. If you want to update Akeeba Data Compliance please remember that you **MUST NOT** uninstall it before installing the new version! When you uninstall Akeeba Data Compliance you will lose all your settings. This is definitely something you do not want to happen! Instead, simply install the new version on top of the old one. Joomla! will figure out that you are doing an update and will treat it as such, automatically.

Tip

If you find that after installing or updating Akeeba Data Compliance it is missing some features or doesn't work, please try installing the same version a second time, without uninstalling the component. The reason is that very few times the Joomla! extensions installer infrastructure gets confused and fails to copy some files or entire folders. By repeating the installation you force it to copy the missing files and folders, solving the problem.

1.1.1. Install from URL

The easiest way to install Akeeba Data Compliance is using the Install from URL feature in Joomla!.

Important

This Joomla! feature requires that your server supports fopen() URL wrappers (`allow_url_fopen` is set to 1 in your server's `php.ini` file) or has the PHP cURL extension enabled. Moreover, if your server has a firewall, it has to allow TCP connections over ports 80 and 443 to GitHub's servers where the file is stored. If you don't see any updates or if they fail to download please ask your host to check that these conditions are met. If they are met but you still do not see the updates please file a bug report in the official Joomla! forum [http://forum.joomla.org/].

First, go to the download page for Akeeba Data Compliance [http://github.com/akeeba/com_datacompliance/releases]. Find the latest version (at the top of the page). Right click the ZIP file and copy the URL.

Now go to your site's administator page and click on Extensions, Manage. Click on the Install from URL tab. Clear the contents of the Install URL field and paste the URL you copied from our site's download page. Then click on the Install button. Joomla! will download and install the Akeeba Data Compliance update.

If Joomla! cannot download the package, please use one of the methods described in this section of the documentation. If, however you get an error about copying files, folder not found or a cryptic "-1"

error please follow our installation troubleshooting instructions [https://www.akeebabackup.com/documentation/troubleshooter/abinstallation.html].

1.1.2. Upload and install.

You can download the latest installation packages from the download page for Akeeba Data Compliance [http://github.com/akeeba/com_datacompliance/releases]. Please note that the latest version is always on top. Click on the ZIP file version you want to download and install.

All Akeeba Data Compliance installation packages contain the component and all of its associated extensions. Installing it will install all of these items automatically. It can also be used to upgrade Akeeba Data Compliance; just install it *without* uninstalling the previous release.

In any case, do not extract the ZIP files yet!

Warning

Attention Mac OS X users! Safari, the default web server provided to you by Apple, is automatically extracting the ZIP file into a directory and removes the ZIP file. In order to install the extension through Joomla!'s extensions installer you must select that directory, right-click on it and select Compress to get a ZIP file of its contents. This behaviour was changed in Mac OS X Mountain Lion, but people upgrading from older versions of Mac OS X (Mac OS X Lion and earlier) will witness the old, automatic ZIP extraction, behaviour.

Log in to your site's administrator section. Click on Extensions, Manage link on the top menu. Please click on the Upload Package File tab. Drag and drop the installation ZIP file you had previously downloaded to start the upload and the installation. After a short while, Joomla!™ will tell you that the component has been installed.

Warning

Akeeba Data Compliance is a big extension. Some servers do not allow you to upload files that big. If this is the case you can ask your host to follow our installation troubleshooting instructions [https://www.akeebabackup.com/documentation/troubleshooter/abinstallation.html] under "You get an error about the package not being uploaded to the server".

If you have WAMPServer (or any other prepackaged local server), please note that its default configuration does not allow files over 2Mb to be uploaded. To work around that you will need to modify your php.ini and restart the server. On WAMPserver left-click on the WAMP icon (the green W), click on PHP, php.ini. Find the line beginning with `upload_max_filesize`. Change it so that it reads:

```
upload_max_filesize = 6M
```

Save this file. Now, left-click on the WAMP icon, click on Apache, Service, Restart Service and you can now install the component. Editing the `php.ini` file should also work on all other servers, local and live alike.

If the installation did not work, please take a look at our installation troubleshooting instructions [https://www.akeebabackup.com/documentation/troubleshooter/abinstallation.html].

2. Automatic updates

Akeeba Data Compliance can be updated just like any other Joomla! extension, using the Joomla! extensions update feature. Please note that Joomla! is fully responsible for discovering available updates and installing them on your site. Akeeba Ltd does not have any control of the update process.

Note

This Joomla! feature requires that your server supports fopen() URL wrappers (`allow_url_fopen` is set to 1 in your server's `php.ini` file) or has the PHP cURL extension enabled. Moreover, if your server

has a firewall, it has to allow TCP connections over ports 80 and 443 to GitHub's servers. If you don't see any updates or if they fail to download please ask your host to check that these conditions are met. If they are met but you still do not see the updates please file a bug report in the official Joomla! forum [http://forum.joomla.org/]. In the meantime you can use the manual update methods discussed further below this page.

You can access the extensions update feature in two different ways:

- From the icon your Joomla! administrator control panel page. You will find the icon in the left-hand sidebar, under the Maintenance header. When there are updates found for any of your extensions you will see the Updates are available message. Clicking on it will get you to the Update page of Joomla! Extensions Manager.
- From the top menu of your Joomla! administrator click on Extensions, Manager. From that page click on the Update tab found in the left-hand sidebar. Clicking on it will get you to the Update page of Joomla! Extensions Manager.

If you do not see the updates try clicking on the Find Updates button in the toolbar. If you do not see the updates still you may want to wait up to 24 hours before retrying. This has to do with the way Joomla! caches the update information.

If there is an update available for Akeeba Data Compliance tick the box to the left of its row and then click on the Update button in the toolbar. Joomla! will now download and install the update.

If Joomla! cannot download the package, please use one of the manual update methods described below. If, however you get an error about copying files, folder not found or a cryptic "-1" error please follow our installation troubleshooting instructions [https://www.akeebabackup.com/documentation/troubleshooter/abinstallation.html].

If you get a white page while installing the update please try either the Built-in method (described above) or the manual update method (described below).

Updating manually

As noted in the installation section, installing and updating Akeeba Data Compliance is actually the same thing. If the automatic update using Joomla!'s extensions update feature does not work, please install the update manually following the instructions in the installation section of this documentation.

Important

When installing an update manually you MUST NOT uninstall your existing version of Akeeba Data Compliance.

Sometimes Joomla! may forget to copy some files when updating extensions. If you find Akeeba Data Compliance suddenly not working or if you get a warning that your installation is corrupt you need to download the latest version's ZIP file and install it *twice* on your site, *without* uninstalling it before or in-between these installations. This will most certainly fix this issue.

If the error occurs again after a while, without you updating our software, please contact your host. Some hosts will delete or rename files automatically and without any confirmation as part of a (broken and unfit for purpose) "malware scanner / antivirus". Unfortunately, these scanners return a lot of false positives -innocent files mistakenly marked as malicious- but rename / delete them nonetheless, breaking software installed on the server. If you are on such a host we very strongly recommend that you move to a decent host, run by people who actually know what they are doing. It will be far less headache for you and would actually improve your site's security.

Chapter 3. Using Akeeba Data Compliance

In this chapter you are going to find detailed reference of all the pages, options and features of the Akeeba Data Compliance component.

1. Initial setup

After installing Akeeba Data Compliance there are a few things you need to do to get up to speed. In this section we are going to set up the minimum required features for the component to make sense.

Tip

We strongly recommend trying Data Compliance on a copy of your site first. If you do not know how to make a copy of your site we suggest that you take a look at our Akeeba Backup [https://www.akeebabackup.com/products/akeeba-backup.html] software. The free of charge Akeeba Backup Core version can be easily used to create copies of your site, e.g. running them on a local server such as MAMP, XAMPP or WAMPserver.

Before you take any further steps, you need to have a Privacy Statement saved as a Joomla! article. Per the GDPR it has to be written in plain and simple language, just like the rest of your site. If you are not sure what to write in there you can search for "GDPR privacy statement template" in your favourite search engine. Here's an example [https://www.itgovernance.co.uk/blog/how-to-write-a-gdpr-privacy-notice-with-documentation-template-example/]. Or you could even take a look at what other companies have. For example. here is our Privacy Statement [https://www.akeebabackup.com/privacy]. It's best to publish the article in the Uncategorized section of your site.

After doing that go to Components, Akeeba Data Compliance and click on the Options button. Find the Policy article option and click Select. Choose the article you have just created. Finally, click on Save & Close button in the toolbar.

Now go to Extensions, Plugins and publish the following plugins *in this order*:

- Data Compliance - Joomla! Core User Data
- User - Data Compliance
- System - Data Compliance

After publishing the last plugin you will immediately see a page asking you to consent to processing of your personal data and / or exercise your data rights. This is Data Compliance's self-service page. This is the same page your site's users will see the first time they log into your site.

You need to select Yes and click on Apply my preference to continue using your site. You are taken back to the Plugins page.

This is really all you need to do if the only personal information you are collecting is through Joomla! itself.

If you are collecting information through other components you will need to activate and configure the relevant plugin of the `datacompliance` type. Please note that Data Compliance only ships with a small number of plugins. You can always ask the developer of the third party extension you are using (e.g. VirtueMart, HikaShop, AcyMailing etc) to make Data Compliance plugins using our open, documented API [create-data-source-plugins].

While optional, we recommend that you set up the email templates. These are used to send out emails to your users. The default template is intentionally very generic.

The next logical step is to configure the component to choose who can see sensitive personal information in Data Compliance.

Finally, you may want to set up CRON jobs for automating data minimization (deletion of expired data profiles).

2. Managing personal information

The whole point of Data Compliance is to allow users to manage their Personally Identifiable Information (PII) they have stored with you. This means that they can:

- give or withdraw their explicit consent to your processing of their PII;
- export the PII you have on file for them;
- request that you remove or anonymize their PII profile (user profile) from your site.

This allows your site to meet the GDPR requirements without taxing the site's administrators with the laborious tasks associated with users exercising their data rights.

Frequently asked questions

Please read these questions before filing GitHub issues or feature requests. There's a reason why we have implemented certain things in a certain way.

Can I change the default PII processing preference to be "consent has been given"?

No. This is illegal. The GPDR requires you to obtain explicit consent and also record the date, time and IP address of the user giving or revoking their explicit consent. Implied consent is no longer admissible.

Can I change the default option of the slider to Yes instead of No?

No. The GPDR requires the users to take explicit action to provide their consent. According to most analysts this means that the default state of a slider / radio selection must be No and the default state of a checkbox must be unchecked.

Can I limit the consent only to people coming from the EU (GeoIP detection)?

No. The GDPR applies to natural persons based on their *nationality*, not their current location. For example, a German citizen currently in the United States of America enjoys the same protection under the GDPR as a German citizen currently in Berlin. This makes using GeoIP detection to determine the nationality of an individual legally unsound.

Things are even more interesting with individuals having dual (or multiple) citizenship. A person who's both a US citizen and a Czech citizen enjoys the protections of the GDPR regardless of whether they have ever set foot in the Czech Republic because they are EU citizens (the Czech Republic is in the EU).

Can an administrator change the PII processing consent of a user?

No. This is illegal. The GDPR requires you to obtain explicit consent and also record the date, time and IP address of the user giving or revoking their explicit consent. As a result you cannot give consent on behalf of a user.

While in theory you could be given written permissions or otherwise indisputable evidence of being given the power to change the user's consent setting we consider it beyond the scope of Data Compliance. These are very rare cases and they hardly make sense for a web site. Data Compliance is meant to be used by online-only businesses.

Can an administrator export the PII of a user or delete their profile?

Yes, they can. Their actions are also stored in the audit trail. The rationale behind this decision is that a user may have lost access to their email address and no longer remember their username or password. They can, however, contact you and provide evidence of their identity (e.g. a government issued photo ID) along with their request that you exercise their data rights on their behalf. In this case you are allowed to export the PII or delete the user profile of a user per their request.

After reading both this and the previous question you might wonder why this rationale doesn't apply to the processing consent. Instead of applying their consent preference on their behalf you can simply change their email address, username and / or password so they can log back into your site and apply their consent preference. This means that you are legally covered: you only changed the user's data on their behalf, something which is also stored in the audit log, and they get to apply their processing preference -after logging in- per the GDPR requirements.

Can you create a plugin for a third party extension? It shouldn't be too hard...

No. We do not have the necessary time to analyze how a third party extensions works, figure out what PII it stores and how. Then we would have to create and test the plugin. And then we would have to maintain it forever, even when the third party extension changes substantially. This is a cost of several thousand Euros per year. It's not easy and it's not a cost we can afford for an extensions that makes us no money. Selling integrations would require putting a price of several hundred Euros per year on each to break even, a price everyone would complain about and few would pay.

We made this mistake with Akeeba Subscriptions and its payment plugins. We would create new plugins for just the initial cost of development. However, the maintenance cost started racking up. We ultimately had to discontinue Akeeba Subscriptions as a paid product and remove most of the payment plugins since we could no longer afford maintaining them. Instead of going through the same agony all over again we prefer to be honest and tell you upfront that we can't do that. No, we cannot make an exception for you. No, really, even if you pay us.

2.1. Captive login (consent page) in the front-end

Important

This feature requires that the System and User plugins of Data Compliance are published on your site and their access level is set to Public.

Akeeba Data Compliance allows users to give or withdraw their explicit consent to your processing of their Personally Identifiable Information. Per the GDPR, the default state is that no consent is given.

When the user has not provided their consent for their PII to be processed by you they cannot use the logged in section of the site. The reasoning is that being logged in inherently means that they have a cookie in their browser (Joomla's session cookie) which identifies them as a specific person. Therefore any action they take on the site can be attributed to them, the individual, which requires processing of their PII. The only action allowed in these circumstances is for them to exercise their data rights. That's why Data Compliance implements a “captive login” in this case.

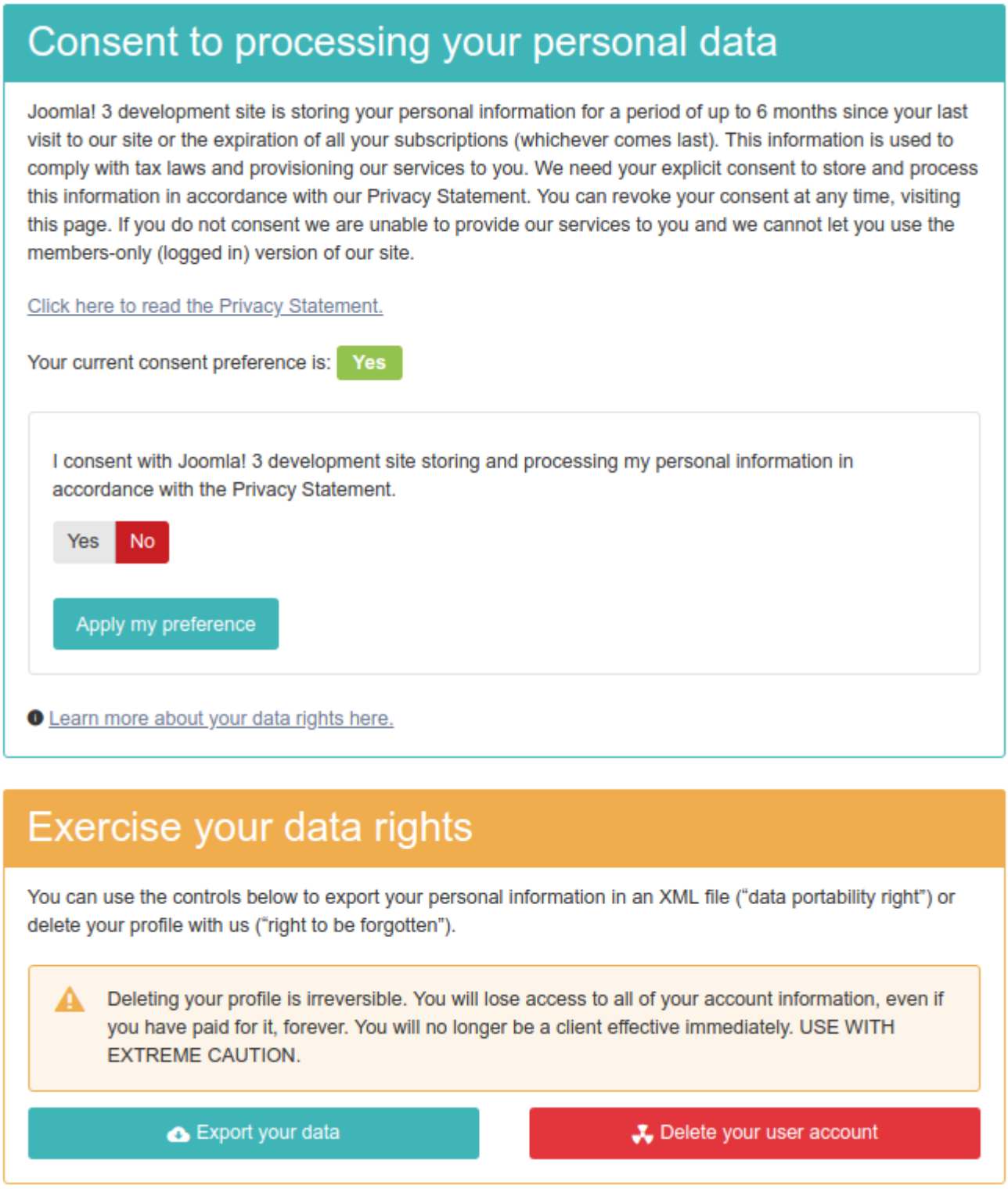
Explicitly: the “captive login” kicks in when the user has not yet consented to you processing their PII *or* if they have explicitly withdrawn their consent.

The captive login takes the user to the Self-Service page where they can exercise their data rights (review their consent, export their PII or delete their user profile). They will not be able to visit any other page unless they either log out first or consent to processing their PII.

2.2. Self-service page

The self-service page is where the users can manage their consent to your processing their Personally Identifiable Information (PII), export their PII in a machine readable format or remove their user profile.

The self-service page



How to get there?

There are several ways to get to that page.

If you have enabled Data Compliance's User plugin, you can edit your Joomla! user profile using the built-in Joomla! Users component. Please note that this method does not work with third party extensions which implement their own user profile, such as Community Builder. When a user is editing their profile they will see a Manage your personal data options link. Clicking on it leads you to the self-service page. This also applies in the backend of the site.

If you are a Super User you can click edit any user's profile and you will see the same link. This will take you to the same page with a slightly different interface: it will tell you which user's personal data preferences you are managing and you won't be able to change their consent settings (because it's disallowed by the GDPR).

Finally, you can create a Joomla frontend menu link to that page from Joomla's menu manager. It is recommended that you put this on your site's footer or the site's user menu (if applicable) to let users find their personal data options page more easily, fulfilling the GDPR requirement for easy access to the options to exercise your data rights.

Managing the consent

The top half of the self-service page allows you to manage your consent for processing the personal data. You can see the current setting for the consent preference and the controls to change it. Please note that the default option in the controls is always set to No, per the GDPR requirement for explicit action to provide consent. If you want to give your consent set it to Yes, then click on Apply My Preference. Conversely, if you want to revoke your consent set this to No and then click on Apply My Preference.

Above the controls there is a link which reads Click here to read the Privacy Statement. Clicking on it opens a slider with the Privacy Statement article, as selected in the component's Options page.

Below the controls there is the Learn more about your data rights here link. This opens a new browser tab or window to the European Union portal for Data protection. This link should not be removed as you are required by GDPR to provide a link to this or a similar resource to your users.

Exporting the PII

The bottom half section of the self-service page has two buttons. The first button allows you to export your user profile in a common, machine-readable format (XML). This lets you exercise your Data Portability Rights under the GDPR. Click on Export your Data to download an XML file to your computer. This contains all the PII about you which is currently known to Akeeba Data Compliance through its plugins.

Deleting the user profile

The bottom half section of the self-service page has two buttons. The second button allows you to wipe your user profile. Depending on the options made in the various Akeeba Data Compliance plugins this will either completely remove or at the very least completely pseudonymize the PII stored on record for you on the site. Please note that this process is **irreversible**. Furthermore, once it's complete it will be impossible to restore your user account and its PII. Therefore, clicking the Delete your user account button exercises your Right To Be Forgotten under the GDPR.

Sometimes it's not possible to exercise your right to be forgotten. This depends on the settings of the various Akeeba Data Compliance through its plugins. For example, people belonging to a privileged group (by default: Super Users) or who have bought a subscription within the last few days may be denied this right. You are told exactly why deletion is not possible though a standard Joomla error message. Having an administrator of the site resolve that condition is necessary before wiping the user account is possible. Administrators should look at the settings of the various Akeeba Data Compliance plugins to understand why th deletion is prevented.

If the deletion can proceed you are taken to the confirmation page. Here you are informed that the deletion is irreversible. Moreover, all the steps which will be carried out by Akeeba Data Compliance are explicitly stated.

These bullet points come from the various Akeeba Data Compliance plugins. You are also informed about the information which exists outside the scope of Joomla and which cannot be deleted by Akeeba Data Compliance. At the bottom of the page you are asked to type a phrase ("*I UNDERSTAND*" in all caps) and click on the DELETE MY USER ACCOUNT button. This is your last chance to abort! Navigate anywhere else or close the browser tab to abort. If the phrase was entered correctly and the button is clicked the user account is wiped forever and can not be restored.

Customization of the page

Akeeba Data Compliance uses Joomla! view templates which follow FOF 3's Blade template language syntax [https://github.com/akeeba/fof/wiki/Blade-Templates]. You can use standard Joomla template overrides [https://docs.joomla.org/How_to_override_the_output_from_the_Joomla!_core] to modify the look, feel and functionality of this page. By default, the HTML structure follows our Akeeba Frontend Framework which provides a unified look and feel for all of our extensions. If you need to use a different template framework, such as Bootstrap, you will have to do template overrides.

Important

Do not change the URLs, the hidden fields or remove form elements when doing overrides. This could cause Akeeba Data Compliance to behave erratically with your overrides.

You may remove or change static links, i.e. the link to "Learn more about your data rights".

Do NOT make template overrides to modify the text on the page. Use language overrides [https://docs.joomla.org/J3.x:Language_Overrides_in_Joomla] instead.

The view template files you need to override is located in:

`PATH_TO_JOOMLA/components/com_datacompliance/ViewTemplates/Options/default.blade.php` The self-service page

`PATH_TO_JOOMLA/components/com_datacompliance/ViewTemplates/Options/wipe.blade.php` The confirmation page for wiping your user account

You can create frontend (public site) overrides for these files in:

`PATH_TO_JOOMLA/templates/YOUR_TEMPLATE/html/com_datacompliance/Options/default.blade.php` The self-service page

`PATH_TO_JOOMLA/templates/YOUR_TEMPLATE/html/com_datacompliance/Options/wipe.blade.php` The confirmation page for wiping your user account

You can create backend (administrator) overrides for these files in:

`PATH_TO_JOOMLA/administrator/templates/YOUR_TEMPLATE/html/com_datacompliance/Options/default.blade.php` The self-service page

`PATH_TO_JOOMLA/administrator/templates/YOUR_TEMPLATE/html/com_datacompliance/Options/wipe.blade.php` The confirmation page for wiping your user account

Please note that Blade templates are compiled and cached as PHP view templates. If you do not see your changes taking effect please go to your site's backend, Cache and clear your frontend or backend cache.

2.3. Managing users' personal information from the backend

So far we have seen how Akeeba Data Compliance can be used by a user of your site to manage their own Personally Identifiable Information. While this is what is mostly required, sometimes an administrator may have

to be involved. For example, a user may no longer remember their username or password and have lost access to their email address associated with it. In these cases they might have to contact you through different means, such as a contact form, email or even by an old-fashioned letter, to seek your assistance in exercising their data rights. Per the GDPR, you are required to respond to them within thirty days since the receipt of their request.

Tip

If a user contacts you to exercise their data rights it's a good idea to ask them for some form of identification which is legally acceptable in case of a dispute over who authorized this action. Typically that's a government issued photo ID such as an identity card or passport, or a business ID / signed form from their manager if it's a company site and your user is an employee. There are many different cases. WE ARE NOT LAWYERS. Ask your lawyer if you are not sure.

From the backend of your site you can go to Joomla's User, Manage (Users) page. Click on a user you want to manage and click on the Personal Data Options tab. There is a link here which takes you to a version of the Self-Service Page.

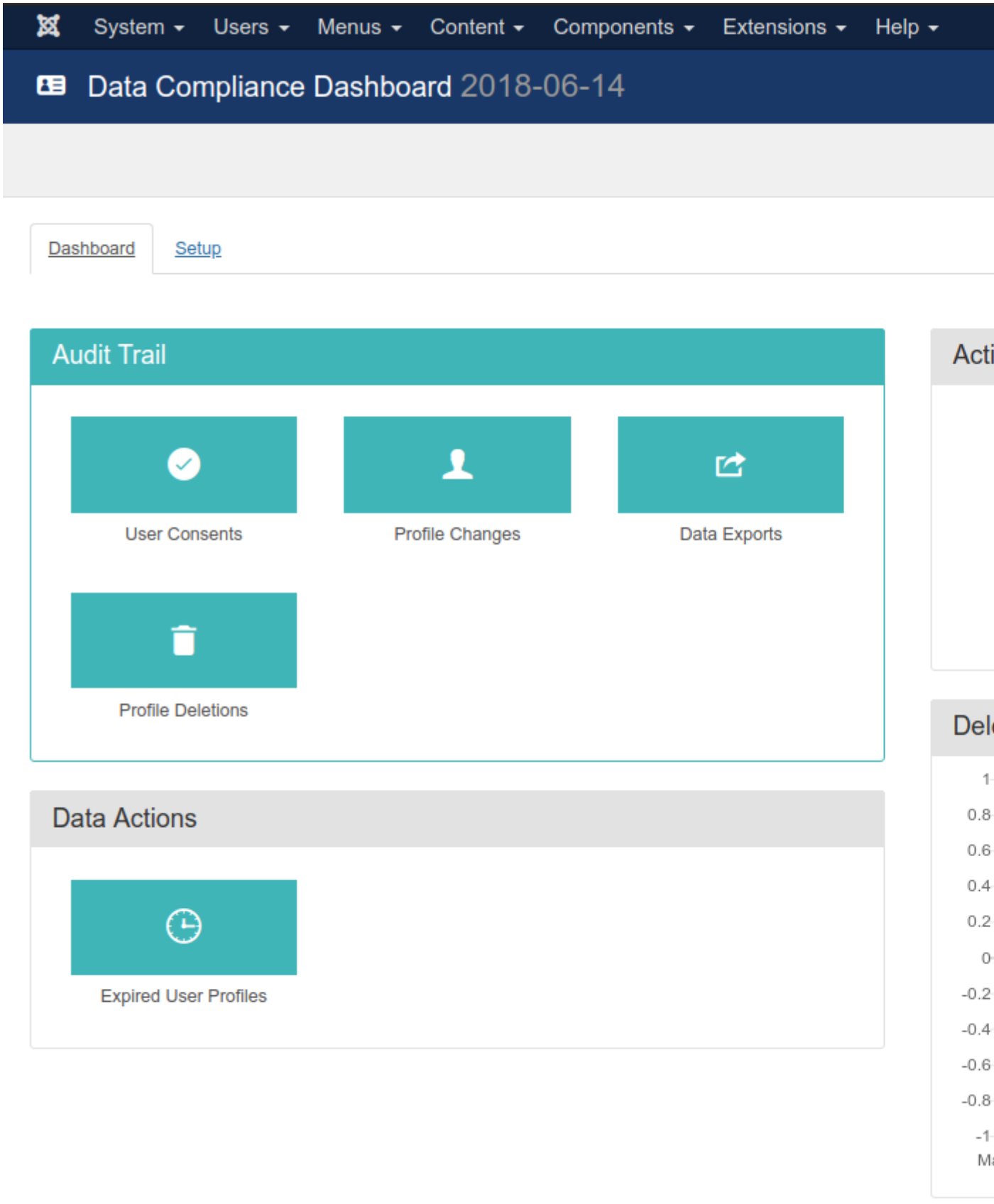
Important

If you do not see the link to this page in the User profile please make sure that you have published and enabled both the System and the User plugin of Akeeba Data Compliance. They are both required for this feature to work.

Please note that you CAN NOT change the consent preferences for personal data processing on behalf of your user. It's illegal to do so. See the FAQ earlier in this documentation. You can, however, export their profile and / or delete their user account. The same notes regarding the possibility to delete their account apply as noted in the previous section.

3. Dashboard (a.k.a. Control Panel) page

The Dashboard page



This is the main backend page of Data Compliance. It allows you to quickly access its features.

The top part of the page is Joomla's toolbar. Clicking on the Options button will take you to the component configuration page.

There is a tab bar below the toolbar. This lets you view the Email Templates setup page and get back to the Dashboard.

The buttons in the left hand side of the main are of the page allow you to access the various logs and management features of Akeeba Data Compliance. They are covered further ahead in this documentation.

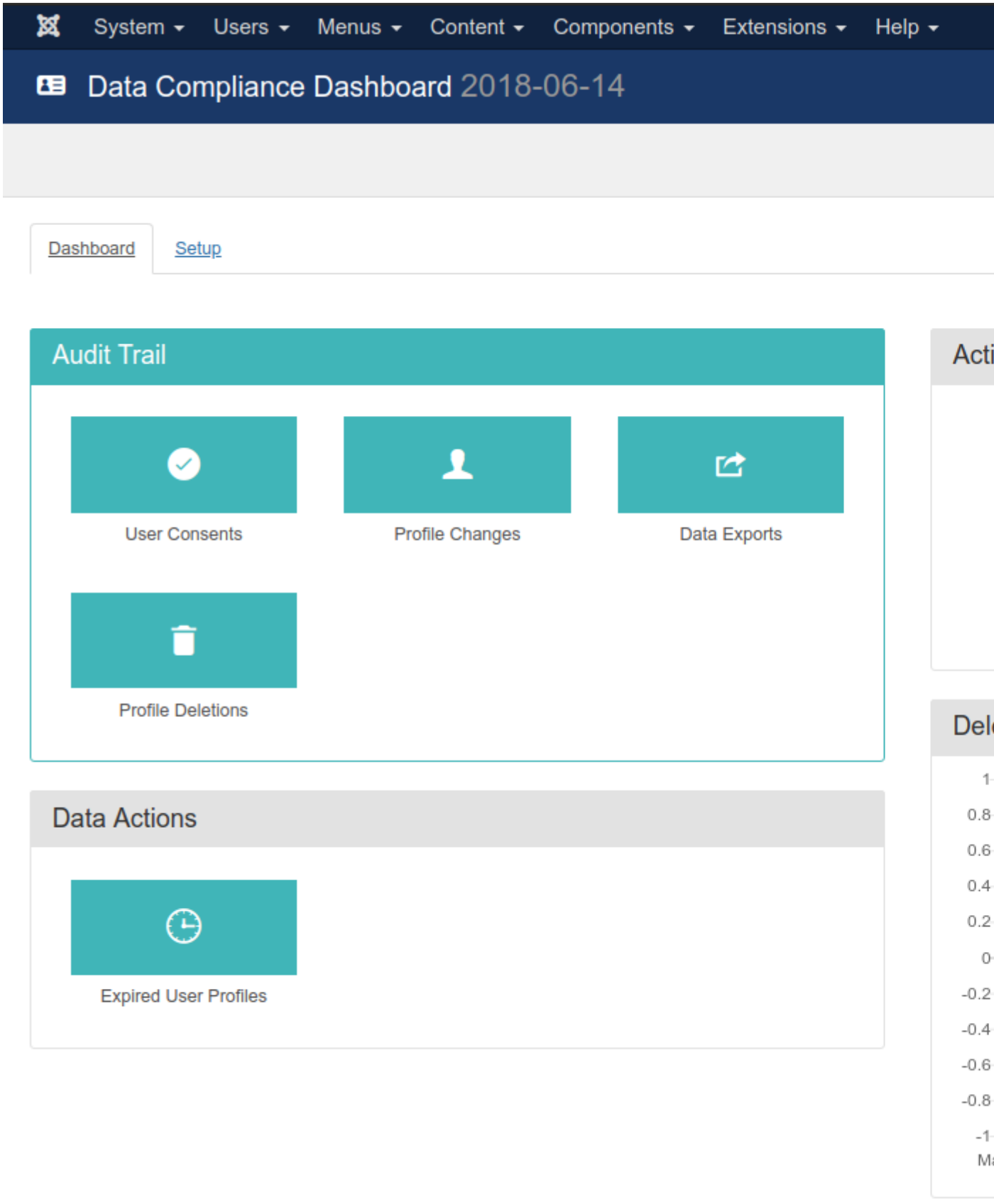
The right hand site contains a set of graphs for quick overview of actions taken with Akeeba Data Compliance.

The Active / Inactive Profiles doughnut chart gives you a quick glance of the user profiles status on your site. Active (non-expired) profiles are shown in green. Expired profiles which have not been deleted are shown in red. Expired profiles which have already been deleted are shown in grey. To conform with the GDPR data minimization rules the red area of this graph needs to be minimized and converted to grey. Not all red can disappear: some expired profiles are not allowed to be deleted according to the rules applied by the Data Compliance plugins, e.g. you can't remove Super User accounts even if they haven't logged into your site in years.

The Deleted User Profiles stacked bar chart gives you more insight into when and how user profiles have been deleted. For each day on the last calendar month you will see a stacked bar with the number of profiles deleted on that day. Profiles deleted by the users themselves are shown in green. Profiles deleted by an administrator are shown in red. Profiles deleted automatically, using the lifecycle policy CRON job are shown in grey.

4. Setting up the email templates

Email templates



Akeeba Data Compliance can send out emails to the user or the administrator on different occasions. More specifically, it can send out emails when a user profile is deleted by the user themselves, when an administrator deletes a user profile, when the profile is deleted by the lifecycle policy CRON job or as a notification before the profile is deleted by the lifecycle policy.

Important

The Akeeba Data Compliance - Emails plugin must be activated and have the access level Public for emails to work.

Each template can be customized *per language*. Akeeba Data Compliance will determine the correct language to use by looking at the user profile. If no language preference is set for the user's site (frontend) language, it will use the site's default language as defined in Joomla's Languages page. Then it will try to find the email template in this language. If this is not possible, it will try to fall back to the en-GB (English, Great Britain) email template. If that's not found either it will try to fall back to the email template marked as "(All languages)". If none is found still no email will be sent. Only enabled email templates are used.

While Data Compliance comes with built in email templates we strongly advise you to customize them to match your site's branding and the tone of language you commonly use. All email templates fully support HTML.

Warning

All URLs in your emails, be it links to your site or static media files such as images, *must* be absolute – they must contain the protocol and domain name to your site. Some Joomla editors will convert absolute links to relative on saving and convert them back to absolute when you try to edit the content. For example, JCE (JoomlaContentEditor.net) does this. This will NOT work with emails.

We recommend that you use CodeMirror, the HTML source code editor shipped with Joomla, to edit email templates.

The Subject and Email body of each email template can contain the following variables, in square brackets and all capital letters. They are expanded to the correct text right before the email is sent.

- [NAME] The full name of the user on whom the action is taken
- [EMAIL] The email address of the user
- [USERNAME] The Joomla username of the user
- [REGISTERDATE] The date the user account was registered on the site
- [LASTVISITDATE] The last time the user logged into their user account on the site
- [REQUIRERESET] Is a password reset required (0/1)
- [RESETCOUNT] How many times the password has been reset in the past
- [LASTRESETTIME] Last date and time (GMT) the password was reset
- [ACTIVATION] Activation code (there's no point using it, it's hashed)
- [BLOCK] Is the user account blocked? (Yes/No)
- [ID] The user's numeric account ID
- [PARAM:*param_name*] The value of the user profile parameter *param_name*. For advanced users.
- [SITENAME] The name of your site, as configured in Joomla
- [SITEURL] The URL to your site

- [ACTIONS] A bullet list of the actions which will be taken when the account is wiped
- [ADMIN:NAME] The administrator's full name, when sending emails to an administrator
- [ADMIN:USERNAME] The administrator's username, when sending emails to an administrator
- [ADMIN:EMAIL] The administrator's email address, when sending emails to an administrator

You can take a look at the default email templates to see how these variables can be used inside a template.

5. Managing audit trails

One of the fundamental requirements in GDPR is that you keep an audit log of all of the actions taken when your users are exercising their data rights. This tells us who did what, removing any doubt over who and why exported or removed a user's PII – or when this information changes. Akeeba Data Compliance can help with all of that by keeping audit trails.

5.1. User Consents

This audit log keeps track of the *last* time the user modified their consent to processing of their Personally Identifiable Information (PII). It records the user account, the consent date, the IP address the consent came from and whether consent was given or withdrawn.

You can search by consent status ("Enabled") and by user. The user search box allows you to type a numeric user ID or a partial username, full name or email address.

5.2. Profile Changes

This audit log keeps track of every change in the core Joomla! user data and the user profile parameters. It records the profile being modified, who modified it, the date and time this took place, the IP address where this change was initiated as well as the changes made.

You can search by the user being modified. The user search box allows you to type a numeric user ID or a partial username, full name or email address.

If you click on the profile being modified you can see a detail page with all the information which was changed in the profile. The From column contains the old values, the To value contains the new values.

Important

This audit log's records are deleted when a user account is wiped trough Data Compliance since it contains Personally Identifiable Information.

5.3. Data Exports

This audit log keeps track of who and when exported the PII for a user. It records the profile the data was exported for, who exported the profile, when the profile was exported and the IP address which initiated the export. The exported data is NOT logged for privacy reasons.

You can search by the user whose profile was exported. The user search box allows you to type a numeric user ID or a partial username, full name or email address.

5.4. Profile Deletions

This audit log keeps track of the user profiles which have been deleted from the site. It records which user profile has been deleted, who initiated the deletion, what kind of deletion it was (user initiated, administrator initiated or

lifecycle management), when the deletion took place and the IP address which initiated the deletion (or the text CLI when it was initiated by the lifecycle management CRON job).

You can search by the user whose profile was deleted and by who initiated the deletion. The user search boxes allow you to type a numeric user ID or a partial username, full name or email address.

6. Managing data actions

As already explained, exporting and deleting users is possible through the Joomla! User Manager. However, this is not a convenient interface to find out which profiles are expired and so on. This is why Data Compliance comes with its own pages to manage data actions.

6.1. Expired user profiles

This page displays all users whose profiles have expired. Expired profiles are determined by your Data Compliance plugin settings. Some of the profiles cannot be deleted even though they are expired, e.g. when they belong to a privileged user group. These profiles appear in pink background color.

Note

Why not hide the profiles which cannot be deleted? For performance reasons.

Identifying expired profiles is a relatively fast query with the same criteria for all users. This means that we can get thousands of users matching these criteria and paginate the results for display.

Finding the exceptions, which expired profiles cannot be deleted, is a set of slow queries which have to be run per user. On sites with thousands of users, like our own business site, executing these queries would take a lot of time and memory. In fact, it would end up crashing either PHP or the server itself.

When we display a page of a few dozen expired profiles we can run these slow queries. Even though the page takes a while to display it doesn't crash PHP or the server. The difference is that in this case we run the slow queries to a fraction of all the expired profiles at a time, therefore taking a fraction of the processing power required. The only drawback is that we cannot exclude the exceptions from the display.

Each profile has a Manage Data Options button at the right hand corner. This takes you to the page to manage data options, i.e. export the user's profile or delete it.

You can search by the maximum expiration date and by user. The user search box allows you to type a numeric user ID or a partial username, full name or email address.

7. Automating data minimization actions

The GDPR calls for data minimization, i.e. removing the personally identifiable information of users when it's no longer needed for business purposes. While there are no hard limits in the law, it's generally agreed that a reasonable amount of time for needing PII for business purposes is around 6 months after the client last had an active business relationship with you. On most sites this means about 6 months after the last time the user logged in, had an active subscription and so on.

Akeeba Data Compliance lets you automatically notify users with expired profiles that their profile will be deleted after a specific date unless they log in or take another action to affirm a business relation with you before that date. After that date and only if the notification email has been sent these expired profiles will be deleted in the same way as if the user chose to delete their profile. This is called a “lifecycle policy” deletion. These actions take place through command line scripts which can be automated with CRON jobs.

Important

Your host must support real CRON jobs which lets you run PHP scripts on the command line. If you can only set up a URL in your “CRON jobs” it will NOT work with Akeeba Data Compliance. We are not

trying to be difficult about this. We know how to write a web interface alternative, as evidenced by doing the same with Akeeba Backup, it's just that we haven't found the time yet to do so.

The conditions to consider a profile “expired”, i.e. the user account lifecycle policies for your site, are controlled by the options of the Data Compliance plugins.

7.1. Notify users before their profile is automatically deleted

Script location: *JOOMLA_ROOT*/cli/datacompliance_lifecycle_notify.php

This script notifies users that their account is going to be deleted due to user account lifecycle policies on your site and gives them information to prevent that. The Akeeba Data Compliance - Email plugin must be enabled for this to work correctly. Your site must be configured to be able to send out email. Check your Joomla Global Configuration if you are not sure.

You can schedule this script using the following command line to your host's CRON interface:

```
/usr/local/bin/php JOOMLA_ROOT/cli/datacompliance_lifecycle_notify.php --confirm=0
```

where */usr/local/bin/php* is the path to your PHP CLI executable and *JOOMLA_ROOT* is the absolute path to your web site's root. You can get this information from your host.

The script accepts the following parameters

- `--debug` When present it turns on debug mode. Only for developers. Do not use on live sites.
- `--period interval_spec` How long before the account expiration date should users be notified? The interval_spec is a PHP DateInterval interval specification [http://php.net/manual/en/dateinterval.construct.php]. The default value is *P1M* which means one month.
- `--confirm` Should I ask for confirmation before sending out each email? Default is 1 (ask for confirmation, expecting input from the keyboard). When using in CRON scripts use `--confirm=0` to prevent this behaviour.
- `--dry-run` No emails will be sent. The script will run normally and output all actions it would be taking without really sending out the emails. Useful for the first few runs while you're getting things set up.

7.2. Automatically delete expired user profiles

Script location: *JOOMLA_ROOT*/cli/datacompliance_account_lifecycle.php

This script deletes expired user accounts as long as they have already been notified. The Akeeba Data Compliance - Email plugin must be enabled for emails to be sent out to users when their accounts are being deleted. In this case your site must be configured to be able to send out email. Check your Joomla Global Configuration if you are not sure.

You can schedule this script using the following command line to your host's CRON interface:

```
/usr/local/bin/php JOOMLA_ROOT/cli/datacompliance_account_lifecycle.php --confirm=0
```

where */usr/local/bin/php* is the path to your PHP CLI executable and *JOOMLA_ROOT* is the absolute path to your web site's root. You can get this information from your host.

The script accepts the following parameters

- `--debug` When present it turns on debug mode. Only for developers. Do not use on live sites.
- `--memdebug` Displays additional information about memory consumption. For developers and power users.

- `--force` Delete expired user accounts even if they have not been notified. This is useful for the first run on a site with thousands of expired accounts you do not want to notify before deleting. **THIS IS EXTREMELY DANGEROUS!** Use it with --dry-run first to make sure that it does what you think it should be doing.
- `--confirm` Should I ask for confirmation before deleting each user? Default is 1 (ask for confirmation, expecting input from the keyboard). When using in CRON scripts use `--confirm=0` to prevent this behaviour.
- `--dry-run` No deletions will take place. The script will run normally and output all actions it would be taking without really deleting any user account. Useful for the first few runs while you're getting things set up.

8. Configuration

GDPR compliance is most definitely not a one-size-fits-all affair. It is tied to the way your site is collecting and using personally identifiable information. Decisions about how to delete this data or when a profile is expired, or when it shouldn't be deleted, may also vary depending on your business needs and what your lawyer has consulted you.

Akeeba Data Compliance gives you plenty of options to tailor it to your needs. These options can be found either at the component itself or its plugins.

8.1. Component configuration

Component configuration is accessible from the backend of your site in the same way that's customary for all Joomla! components. The easiest way is going to Components, Akeeba Data Compliance and clicking the Options button in the toolbar.

Alternatively, you can go to System, Global Configuration and click on Akeeba Data Compliance from the left-hand list of Components.

Consent Page Options

The first tab is called Consent Page Options and it controls the way the self-service page of Data Compliance works on your site.

The Policy Article options lets you choose a Joomla article which contains your site's Privacy Statement per the GDPR requirements. Remember that when the self-service page is shown to a user who has not yet provided their consent they cannot navigate outside of that page. Therefore it's advisable to not include any links to other pages on your site in this article as they will be inaccessible to the user.

The Show Export Button and Show Delete Button options control whether the button to export the personal information to XML and to delete the user profile, respectively, will be shown to the user. If they are not shown you will have to take and fulfil these requests manually.

FEF Handling

Our software is using Akeeba Frontend Framework (FEF) to style its output in the frontend (public site) and backend (administrator) of your site. If you would rather provide your own styling by doing template overrides and / or loading your own CSS it's recommended that you disable loading of FEF's CSS files. You can control this behavior with these options.

Load Akeeba FEF controls when the FEF CSS will be loaded: Never, Frontend Only, Backend Only or Both (frontend and backend). Kindly note that the backend interface will look broken if you do not load FEF and you do not supply template overrides for every single backend page.

Load CSS reset with Akeeba FEF controls an optional behavior of FEF. We load a CSS reset (forcing the values of several CSS attributes to predictable values) inside the DIV that contains Akeeba Data Compliance's output. This is done to prevent third party CSS, such as the Joomla-supplied Bootstrap 2 files, from interfering with the

layout. If you are going to be overriding the layout with your own CSS you should not be loading the CSS reset. The options here are the same as for the previous setting.

Permissions

This is the standard Joomla! ACL configuration page for the component. Apart from Joomla's typical permissions, Akeeba Data Compliance comes with its own, special permissions.

Audit trails controls whether the backend user can view any of the audit trails kept by Akeeba Data Compliance. Please note that this is a unique case of a permission in that it controls *viewing information*, not taking an action on it.

Delete profiles controls whether the user is allowed to delete the profiles of other users.

Export profiles controls whether the user is allowed to export the personal information of other users.

Due to the way Joomla! works, Super Users (that is: any user belonging to a group with the Super User privilege) has all of these privileges and *they can not be taken away from them*. For better GDPR compliance it's advisable to create a new user group with more permissions than Administrator but less than Super User for those administrators who need extended privileges on the site but who should not be able to take actions or view personally identifiable information of other users. Doing that is outside the scope of Akeeba Data Compliance: the tools to do that (Permissions) are given to you by Joomla itself!

8.2. System plugin configuration

The System - Data Compliance plugin makes it possible to capture the login of users who have not yet consented to processing of their personal information. It's advisable to keep it published at all times.

The captive login works by means of redirections. If the current user has not provided their consent (or has withdrawn their consent) they are immediately redirected to Data Compliance's self service page. Trying to navigate to another page causes another redirection. This way the user is captured in the self-service page until they provide consent (they can also log out of the site if they want to).

The same trick may be used by other components to provide a captive login. For example, Akeeba LoginGuard (our Two Step Verification component for Joomla) does the same thing. To prevent a redirection loop you must let Data Compliance know which third party components are allowed to be accessed without the user providing their consent. Moreover, you can specify other components here which don't collect personal information and are therefore allowed (e.g. com_content which is the Joomla articles component).

The Exempt components / views / tasks takes one specification on each line. Each specification consists of a component, view and task separated by dots. When you want to match any value in a position using `*`. For example, to allow access to single article views in com_content use the specification `com_content.article.*`

By default, only Akeeba LoginGuard is allowed to be accessed: `com_loginguard.*.*`

8.3. Data sources configuration (`datacompliance` plugins)

Akeeba Data Compliance, the component, does not know what personally identifiable information looks like, where to find it and where to handle it. This is the job of the plugins of the `datacompliance` type. These provide the interface to the personally identifiable data sources and take actions on that data.

8.3.1. Joomla! Core User Data

Plugin: Data Compliance - Joomla! Core User Data

It allows Data Compliance to handle information stored by Joomla! itself, as well as any profile fields managed by third party components and plugins.

Options

Exempt user groups. The users who belong in these user groups cannot be deleted, either manually or automatically (lifecycle policies). Please note that users who belong in any group which has the Super User privilege are always exempt, regardless of this setting.

User account lifecycle. Do you want this plugin to tell Akeeba Data Compliance which user records are considered expired according to the options below? If you set this to No the following options are ignored.

Last login threshold (months). User accounts which have not logged into your site for at least this many months are considered expired.

Never visited. User accounts who have never visited your site after the user account creation are considered expired.

Blocked accounts. User accounts marked as Blocked are considered expired. **THIS IS DANGEROUS**! Joomla will also mark user accounts as blocked when the user tries to reset their password and until they do so. This may result in active user accounts being deleted because they were trying to reset their password. We recommend AGAINST using this option.

8.3.2. Akeeba Subscriptions

Plugin: Data Compliance - Akeeba Subscriptions

It allows Data Compliance to handle information stored by Akeeba Subscriptions.

Options

User account lifecycle. Do you want this plugin to tell Akeeba Data Compliance which user records are considered expired according to the options below? If you set this to No the following options are ignored.

Last expired subscription this many months ago. User accounts whose last subscription expired at least this many months ago are considered expired.

Exclude users who have visited the site in the meantime. Modifies the above option. If the user with the expired subscription has visited the site after their subscription expires they are not considered expired accounts. For most sites it's recommended to set this to Yes and use the “Last login threshold (months)” option in the Data Compliance - Joomla! Core User Data plugin to handle expiration of these user accounts.

Non-lifecycle deletion exemption threshold (days). Users who created a subscription within this many days ago will not be allowed to be deleted. It's recommended to set this to the maximum chargeback period allowed by the payment services you are using on your site. For example, if they allow chargebacks for up to 90 days since the transaction was made you should put 90 in here.

8.3.3. Akeeba Release System

Plugin: Data Compliance - Akeeba Release System

It allows Data Compliance to handle information stored by Akeeba Release System.

Options

There are no options for this plugin.

8.3.4. Akeeba Ticket System

Plugin: Data Compliance - Akeeba Ticket System

It allows Data Compliance to handle information stored by Akeeba Ticket System.

Options

There are no options for this plugin.

8.3.5. Akeeba LoginGuard

Plugin: Data Compliance - Akeeba LoginGuard

It allows Data Compliance to handle information stored by Akeeba LoginGuard.

Options

There are no options for this plugin.

8.4. Other plugins

Akeeba Data Compliance comes with optional plugins. They add functionality to Akeeba Data Compliance.

8.4.1. The User plugin

Plugin: User - Data Compliance

> ### Warning
>
> If you disable this plugin logging into the site may result in user accounts being deleted by the Lifecycle Policy feature *WITHOUT* being sent a warning email first! If unsure, publish the plugin.

This plugin is responsible for the following features of Akeeba Data Compliance:

- Add the Manage your personal data options link to the user profile edit page.
- Log any changes to the user's personal information (Joomla! core user profile information, user group changes, user profile field changes, user custom field changes).
- When a user logs in remove the information from the user profile which indicates that the user has already received warning about their account being ready to be removed due to the Lifecycle Policy. This means that next time their account is eligible for Lifecycle Policy deletion they will receive a new email. If this information is not removed they will not receive any further email in the future if their user account becomes expired again BUT their account will be deleted by Lifecycle Policy!

It allows Data Compliance to handle information stored by Joomla! itself, as well as any profile fields managed by third party components and plugins.

8.4.2. Send emails on account deletion

Plugin: Akeeba Data Compliance - Send emails on account deletion

Enables all email features for Akeeba Data Compliance. It's recommended that you always enable this plugin.

Options

Email users. Should emails be sent to users when their account is being deleted?

Email administrators. Should administrators (Super Users) receive emails when a user's account is being deleted?

Administrator emails. A list of email addresses to be emailed. One email per line. The emails must correspond to the email used by Super User accounts on your site, otherwise they will not receive any emails. If you leave it blank all Super Users on the site will be emailed.

8.4.3. Upload user deletion audit trail to Amazon S3

Plugin: Data Compliance - Upload user deletion audit trail to Amazon S3

Uploads the user deletion audit log records to Amazon S3. One JSON file per deleted user account is uploaded. You should configure it to use an Amazon S3 bucket with a suitable policy which disallows deletion of files. This helps you positively fulfill the recommendation of having an immutable audit log for data deletion actions on your site.

Options

Access Key — Your Amazon S3 Access Key

Secret Key — Your Amazon S3 Secret Key

Use HTTPS — If enabled, HTTPS will be used to connect to Amazon S3. Strongly recommended.

Bucket — The name of your Amazon S3 bucket where your files will be stored in. The bucket must be already created; the application can not create buckets.

> **Warning**
>
> **DO NOT CREATE BUCKETS WITH NAMES CONTAINING UPPERCASE LETTERS. AMAZON CLEARLY WARNS AGAINST DOING THAT**. If you use a bucket with uppercase letters in its name it is very possible that the application will not be able to upload anything to it.
>
> Please note that this is a limitation imposed by Amazon itself. It is not something we can "fix" in the application. If this is the case with your site, please create a new bucket whose name only consists of lowercase unaccented latin characters (a-z), numbers (0-9), dashes and dots.
>
> Moreover, you cannot use a bucket name with a dot in its filename together with the Use HTTPS option. This is a limitation of the HTTPS setup in Amazon S3 servers and cannot be worked around.

Amazon S3 Region — Please select which S3 Region you have created your bucket in. This is MANDATORY for using the newer, more secure, v4 signature method. You can see the region of your bucket in your Amazon S3 management console. Right click on a bucket and click on Properties. A new pane opens to the left. The second row is labelled Region. This is where your bucket was created in. Go back to Akeeba Data Compliance and select the corresponding option from the drop-down.

> **Important**
>
> If you choose the wrong region the connection WILL fail.

Signature method — This option determines the authentication API which will be used to "log in" the backup engine to your Amazon S3 bucket. You have two options:

- **v4 (preferred for Amazon S3)**. Recommended. You MUST specify the Amazon S3 Region in the option above. This option implements the newer AWS4 (v4) authentication API. Buckets created in Amazon S3 regions brought online after January 2014 (e.g. Frankfurt) will only accept this option. Older buckets will work with either option.
- **v2 (legacy mode, third party storage providers)**. Legacy option. We strongly advise against using it unless you have a specific reason we can't think of.

Directory — The directory inside your Amazon S3 bucket where your files will be stored in. If you want to use subdirectories, you have to use a forward slash, e.g. `directory/subdirectory/subsubdirectory`.

Storage Class — This determines how Amazon will store your files. We recommend using Standard - Infrequent Access. This offers decent data durability and results in smaller storage costs if you don't retrieve the files too often, as is the case with the audit log files.

9. Other CLI tools

Akeeba Data Compliance offers some optional command line interface (CLI) tools. CLI tools are meant for advanced users only who manage their sites using the command line, e.g. through an SSH console. Most people should use the administrator web interface in Joomla! instead.

9.1. Delete a user from the CLI

Script location: *JOOMLA_ROOT*`/cli/datacompliance_account_delete.php`

This script deletes any user account. It's equivalent to using the Delete option from the self-service page of that account.

Warning

THIS IS IRREVERSIBLE. Once you delete it with this script, the user's personal information is gone forever.

You can call this script using the following command line:

/usr/local/bin/php JOOMLA_ROOT`/cli/datacompliance_account_lifecycle.php --username=fooba`

where */usr/local/bin/php* is the path to your PHP CLI executable and *JOOMLA_ROOT* is the absolute path to your web site's root. You can get this information from your host.

The script accepts the following parameters

- `--debug` When present it turns on debug mode. Only for developers. Do not use on live sites.
- `--username` The username you want to delete, e.g. `--username=foobar`
- `--id` The numeric user ID you want to delete, e.g. `--id=123`
- `--force` Do not ask for confirmation, delete the user anyway. DANGEROUS!!!
- `--dry-run` No deletions will take place. The script will run normally and output all actions it would be taking without really deleting any user account. Useful to test what will happen.

Chapter 4. Developer's reference

1. Translating

(Translations have not been set up yet - This section will be updated in the future)

2. Interface customization / templating

See the Self-service page documentation.

3. Creating data source plugins

(TODO - This section has not been written yet)

4. Creating other integration plugins

(TODO - This section has not been written yet)

Part II. Appendices

Table of Contents

A. GNU Free Documentation License 31

Appendix A. GNU Free Documentation License

0. PREAMBLE

The purpose of this License is to make a manual, textbook, or other functional and useful document "free" in the sense of freedom: to assure everyone the effective freedom to copy and redistribute it, with or without modifying it, either commercially or noncommercially. Secondarily, this License preserves for the author and publisher a way to get credit for their work, while not being considered responsible for modifications made by others.

This License is a kind of "copyleft", which means that derivative works of the document must themselves be free in the same sense. It complements the GNU General Public License, which is a copyleft license designed for free software.

We have designed this License in order to use it for manuals for free software, because free software needs free documentation: a free program should come with manuals providing the same freedoms that the software does. But this License is not limited to software manuals; it can be used for any textual work, regardless of subject matter or whether it is published as a printed book. We recommend this License principally for works whose purpose is instruction or reference.

1. APPLICABILITY AND DEFINITIONS

This License applies to any manual or other work, in any medium, that contains a notice placed by the copyright holder saying it can be distributed under the terms of this License. Such a notice grants a world-wide, royalty-free license, unlimited in duration, to use that work under the conditions stated herein. The "Document", below, refers to any such manual or work. Any member of the public is a licensee, and is addressed as "you". You accept the license if you copy, modify or distribute the work in a way requiring permission under copyright law.

A "Modified Version" of the Document means any work containing the Document or a portion of it, either copied verbatim, or with modifications and/or translated into another language.

A "Secondary Section" is a named appendix or a front-matter section of the Document that deals exclusively with the relationship of the publishers or authors of the Document to the Document's overall subject (or to related matters) and contains nothing that could fall directly within that overall subject. (Thus, if the Document is in part a textbook of mathematics, a Secondary Section may not explain any mathematics.) The relationship could be a matter of historical connection with the subject or with related matters, or of legal, commercial, philosophical, ethical or political position regarding them.

The "Invariant Sections" are certain Secondary Sections whose titles are designated, as being those of Invariant Sections, in the notice that says that the Document is released under this License. If a section does not fit the above definition of Secondary then it is not allowed to be designated as Invariant. The Document may contain zero Invariant Sections. If the Document does not identify any Invariant Sections then there are none.

The "Cover Texts" are certain short passages of text that are listed, as Front-Cover Texts or Back-Cover Texts, in the notice that says that the Document is released under this License. A Front-Cover Text may be at most 5 words, and a Back-Cover Text may be at most 25 words.

A "Transparent" copy of the Document means a machine-readable copy, represented in a format whose specification is available to the general public, that is suitable for revising the document straightforwardly with generic text editors or (for images composed of pixels) generic paint programs or (for drawings) some widely available drawing editor, and that is suitable for input to text formatters or for automatic translation to a variety

of formats suitable for input to text formatters. A copy made in an otherwise Transparent file format whose markup, or absence of markup, has been arranged to thwart or discourage subsequent modification by readers is not Transparent. An image format is not Transparent if used for any substantial amount of text. A copy that is not "Transparent" is called "Opaque".

Examples of suitable formats for Transparent copies include plain ASCII without markup, Texinfo input format, LaTeX input format, SGML or XML using a publicly available DTD, and standard-conforming simple HTML, PostScript or PDF designed for human modification. Examples of transparent image formats include PNG, XCF and JPG. Opaque formats include proprietary formats that can be read and edited only by proprietary word processors, SGML or XML for which the DTD and/or processing tools are not generally available, and the machine-generated HTML, PostScript or PDF produced by some word processors for output purposes only.

The "Title Page" means, for a printed book, the title page itself, plus such following pages as are needed to hold, legibly, the material this License requires to appear in the title page. For works in formats which do not have any title page as such, "Title Page" means the text near the most prominent appearance of the work's title, preceding the beginning of the body of the text.

A section "Entitled XYZ" means a named subunit of the Document whose title either is precisely XYZ or contains XYZ in parentheses following text that translates XYZ in another language. (Here XYZ stands for a specific section name mentioned below, such as "Acknowledgements", "Dedications", "Endorsements", or "History".) To "Preserve the Title" of such a section when you modify the Document means that it remains a section "Entitled XYZ" according to this definition.

The Document may include Warranty Disclaimers next to the notice which states that this License applies to the Document. These Warranty Disclaimers are considered to be included by reference in this License, but only as regards disclaiming warranties: any other implication that these Warranty Disclaimers may have is void and has no effect on the meaning of this License.

2. VERBATIM COPYING

You may copy and distribute the Document in any medium, either commercially or noncommercially, provided that this License, the copyright notices, and the license notice saying this License applies to the Document are reproduced in all copies, and that you add no other conditions whatsoever to those of this License. You may not use technical measures to obstruct or control the reading or further copying of the copies you make or distribute. However, you may accept compensation in exchange for copies. If you distribute a large enough number of copies you must also follow the conditions in section 3.

You may also lend copies, under the same conditions stated above, and you may publicly display copies.

3. COPYING IN QUANTITY

If you publish printed copies (or copies in media that commonly have printed covers) of the Document, numbering more than 100, and the Document's license notice requires Cover Texts, you must enclose the copies in covers that carry, clearly and legibly, all these Cover Texts: Front-Cover Texts on the front cover, and Back-Cover Texts on the back cover. Both covers must also clearly and legibly identify you as the publisher of these copies. The front cover must present the full title with all words of the title equally prominent and visible. You may add other material on the covers in addition. Copying with changes limited to the covers, as long as they preserve the title of the Document and satisfy these conditions, can be treated as verbatim copying in other respects.

If the required texts for either cover are too voluminous to fit legibly, you should put the first ones listed (as many as fit reasonably) on the actual cover, and continue the rest onto adjacent pages.

If you publish or distribute Opaque copies of the Document numbering more than 100, you must either include a machine-readable Transparent copy along with each Opaque copy, or state in or with each Opaque copy a computer-network location from which the general network-using public has access to download using public-standard network protocols a complete Transparent copy of the Document, free of added material. If you use the latter option, you must take reasonably prudent steps, when you begin distribution of Opaque copies in quantity, to

ensure that this Transparent copy will remain thus accessible at the stated location until at least one year after the last time you distribute an Opaque copy (directly or through your agents or retailers) of that edition to the public.

It is requested, but not required, that you contact the authors of the Document well before redistributing any large number of copies, to give them a chance to provide you with an updated version of the Document.

4. MODIFICATIONS

You may copy and distribute a Modified Version of the Document under the conditions of sections 2 and 3 above, provided that you release the Modified Version under precisely this License, with the Modified Version filling the role of the Document, thus licensing distribution and modification of the Modified Version to whoever possesses a copy of it. In addition, you must do these things in the Modified Version:

A. Use in the Title Page (and on the covers, if any) a title distinct from that of the Document, and from those of previous versions (which should, if there were any, be listed in the History section of the Document). You may use the same title as a previous version if the original publisher of that version gives permission.

B. List on the Title Page, as authors, one or more persons or entities responsible for authorship of the modifications in the Modified Version, together with at least five of the principal authors of the Document (all of its principal authors, if it has fewer than five), unless they release you from this requirement.

C. State on the Title page the name of the publisher of the Modified Version, as the publisher.

D. Preserve all the copyright notices of the Document.

E. Add an appropriate copyright notice for your modifications adjacent to the other copyright notices.

F. Include, immediately after the copyright notices, a license notice giving the public permission to use the Modified Version under the terms of this License, in the form shown in the Addendum below.

G. Preserve in that license notice the full lists of Invariant Sections and required Cover Texts given in the Document's license notice.

H. Include an unaltered copy of this License.

I. Preserve the section Entitled "History", Preserve its Title, and add to it an item stating at least the title, year, new authors, and publisher of the Modified Version as given on the Title Page. If there is no section Entitled "History" in the Document, create one stating the title, year, authors, and publisher of the Document as given on its Title Page, then add an item describing the Modified Version as stated in the previous sentence.

J. Preserve the network location, if any, given in the Document for public access to a Transparent copy of the Document, and likewise the network locations given in the Document for previous versions it was based on. These may be placed in the "History" section. You may omit a network location for a work that was published at least four years before the Document itself, or if the original publisher of the version it refers to gives permission.

K. For any section Entitled "Acknowledgements" or "Dedications", Preserve the Title of the section, and preserve in the section all the substance and tone of each of the contributor acknowledgements and/or dedications given therein.

L. Preserve all the Invariant Sections of the Document, unaltered in their text and in their titles. Section numbers or the equivalent are not considered part of the section titles.

M. Delete any section Entitled "Endorsements". Such a section may not be included in the Modified Version.

N. Do not retitle any existing section to be Entitled "Endorsements" or to conflict in title with any Invariant Section.

O. Preserve any Warranty Disclaimers.

If the Modified Version includes new front-matter sections or appendices that qualify as Secondary Sections and contain no material copied from the Document, you may at your option designate some or all of these sections

as invariant. To do this, add their titles to the list of Invariant Sections in the Modified Version's license notice. These titles must be distinct from any other section titles.

You may add a section Entitled "Endorsements", provided it contains nothing but endorsements of your Modified Version by various parties--for example, statements of peer review or that the text has been approved by an organization as the authoritative definition of a standard.

You may add a passage of up to five words as a Front-Cover Text, and a passage of up to 25 words as a Back-Cover Text, to the end of the list of Cover Texts in the Modified Version. Only one passage of Front-Cover Text and one of Back-Cover Text may be added by (or through arrangements made by) any one entity. If the Document already includes a cover text for the same cover, previously added by you or by arrangement made by the same entity you are acting on behalf of, you may not add another; but you may replace the old one, on explicit permission from the previous publisher that added the old one.

The author(s) and publisher(s) of the Document do not by this License give permission to use their names for publicity for or to assert or imply endorsement of any Modified Version.

5. COMBINING DOCUMENTS

You may combine the Document with other documents released under this License, under the terms defined in section 4 above for modified versions, provided that you include in the combination all of the Invariant Sections of all of the original documents, unmodified, and list them all as Invariant Sections of your combined work in its license notice, and that you preserve all their Warranty Disclaimers.

The combined work need only contain one copy of this License, and multiple identical Invariant Sections may be replaced with a single copy. If there are multiple Invariant Sections with the same name but different contents, make the title of each such section unique by adding at the end of it, in parentheses, the name of the original author or publisher of that section if known, or else a unique number. Make the same adjustment to the section titles in the list of Invariant Sections in the license notice of the combined work.

In the combination, you must combine any sections Entitled "History" in the various original documents, forming one section Entitled "History"; likewise combine any sections Entitled "Acknowledgements", and any sections Entitled "Dedications". You must delete all sections Entitled "Endorsements".

6. COLLECTIONS OF DOCUMENTS

You may make a collection consisting of the Document and other documents released under this License, and replace the individual copies of this License in the various documents with a single copy that is included in the collection, provided that you follow the rules of this License for verbatim copying of each of the documents in all other respects.

You may extract a single document from such a collection, and distribute it individually under this License, provided you insert a copy of this License into the extracted document, and follow this License in all other respects regarding verbatim copying of that document.

7. AGGREGATION WITH INDEPENDENT WORKS

A compilation of the Document or its derivatives with other separate and independent documents or works, in or on a volume of a storage or distribution medium, is called an "aggregate" if the copyright resulting from the compilation is not used to limit the legal rights of the compilation's users beyond what the individual works permit. When the Document is included in an aggregate, this License does not apply to the other works in the aggregate which are not themselves derivative works of the Document.

If the Cover Text requirement of section 3 is applicable to these copies of the Document, then if the Document is less than one half of the entire aggregate, the Document's Cover Texts may be placed on covers that bracket

the Document within the aggregate, or the electronic equivalent of covers if the Document is in electronic form. Otherwise they must appear on printed covers that bracket the whole aggregate.

8. TRANSLATION

Translation is considered a kind of modification, so you may distribute translations of the Document under the terms of section 4. Replacing Invariant Sections with translations requires special permission from their copyright holders, but you may include translations of some or all Invariant Sections in addition to the original versions of these Invariant Sections. You may include a translation of this License, and all the license notices in the Document, and any Warranty Disclaimers, provided that you also include the original English version of this License and the original versions of those notices and disclaimers. In case of a disagreement between the translation and the original version of this License or a notice or disclaimer, the original version will prevail.

If a section in the Document is Entitled "Acknowledgements", "Dedications", or "History", the requirement (section 4) to Preserve its Title (section 1) will typically require changing the actual title.

9. TERMINATION

You may not copy, modify, sublicense, or distribute the Document except as expressly provided for under this License. Any other attempt to copy, modify, sublicense or distribute the Document is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

10. FUTURE REVISIONS OF THIS LICENSE

The Free Software Foundation may publish new, revised versions of the GNU Free Documentation License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns. See http://www.gnu.org/copyleft/ [http://www.gnu.org/copyleft/] .

Each version of the License is given a distinguishing version number. If the Document specifies that a particular numbered version of this License "or any later version" applies to it, you have the option of following the terms and conditions either of that specified version or of any later version that has been published (not as a draft) by the Free Software Foundation. If the Document does not specify a version number of this License, you may choose any version ever published (not as a draft) by the Free Software Foundation.

ADDENDUM: How to use this License for your documents

To use this License in a document you have written, include a copy of the License in the document and put the following copyright and license notices just after the title page:

> Copyright (C) YEAR YOUR NAME.
>
> Permission is granted to copy, distribute and/or modify this document under the terms of the GNU Free Documentation License, Version 1.2 or any later version published by the Free Software Foundation; with no Invariant Sections, no Front-Cover Texts, and no Back-Cover Texts. A copy of the license is included in the section entitled "GNU Free Documentation License".

If you have Invariant Sections, Front-Cover Texts and Back-Cover Texts, replace the "with...Texts." line with this:

> with the Invariant Sections being LIST THEIR TITLES, with the Front-Cover Texts being LIST, and with the Back-Cover Texts being LIST.

If you have Invariant Sections without Cover Texts, or some other combination of the three, merge those two alternatives to suit the situation.

If your document contains nontrivial examples of program code, we recommend releasing these examples in parallel under your choice of free software license, such as the GNU General Public License, to permit their use in free software.