GDPR

Using phpList for compliance with the GDPR

This chapter provides an overview of features and functionality of phpList version 3.3.3 and higher, implemented for phpList administrators seeking to be compliant with the General Data Protection Regulation in their data management practices.

The GDPR is a regulation in EU law which includes legal requirements for how the data of people in the EU is handled, including the kind of data collected by installations of phpList. The laws affect all entities which handle such data regardless of where they are based. In addition, the EU's directive on electronic privacy contains rules on the use of email for the purposes of direct marketing.

Ultimately it is the administrators of a given installation of phpList who are responsible for managing data responsibly. The following technical features of phpList relate to common strategies for complying with the regulations as they stand.

Note: GDPR is a comprehensive set of regulations which covers much more than just technical operation of the newsletter software that you use. For comprehensive information about entities' responsibilities, consult the Information Commissioner's Office, the European Commission website, or independent legal advice. You can find the full text of the GDPR here.

Note: Features which are not present in older versions are labelled (⇧phpList-3.3.3) for convenience.

Sensitive ("special category") data

The GDPR makes distinctions between different types of data and the protections they require.

- Do not store particularly sensitive data within phpList (e.g. as user attributes). Examples of data in this category are data relating to medical history, sexuality, or ethnicity.
- If children are not your target audience, consider adding a required attribute to your subscribe pages and sign up forms for age confirmation

    - (⇧phpList-3.3.3) A Default Attribute exists for convenience which requires subscribers to confirm they are 16 or older – you can load it easily via the Config → Configure Attributes page

Justification for data processing

The GDPR requires that organisations have one of six possible legal justifications for processing subscriber data.

Consent

The justification most commonly used by newsletter and email marketers is that consent has been obtained from all their subscribers. In some situations, marketing by email can only be carried out with consent. The GDPR uses a specific definition of consent, and defines how it may be acquired and managed. phpList can easily be used to obtain and manage subscriber consent.

- If your subscribers sign up to phpList directly using subscribe pages, widgets, or custom forms:
    - Consider adding a required consent checkbox which links to your legal policies
        - (⇧phpList-3.3.3) A Default Attribute exists for convenience which requires consent to the website Terms of Service – you can load it easily via the Config → Configure Attributes page
    - Consider adding a comprehensive explanation of why, how, and for how long their data will be used, to either:
        - The confirmation email message text which they automatically receive
        - The subscribe page or form which into which they initially add their details
- Only import subscribers into phpList for which you have auditable evidence of adequate consent
- Send re-permission campaigns using the Invite Plugin to re-obtain consent from inactive subscribers
    - (⇧phpList-3.3.3) The Invite Plugin is included with phpList by default but must be enabled on the Config → Manage Plugins page
    - (⇧phpList-3.3.3) A template re-permission campaign is included by default as a draft for easy use and reference
- Use the “Delete subscribers who signed up and have not confirmed their subscription” option on the Reconcile Subscribers page to remove subscribers who have not provided adequate consent
- (⇧phpList-3.3.3) Use the “Delete subscribers who are blacklisted because they unsubscribed” button on the Subscribers → Reconcile Subscribers page to delete all blacklisted subscribers who unsubscribed from your lists
- Use the “Delete all blacklisted subscribers” button on the Subscribers → Reconcile Subscribers page to delete all blacklisted subscribers, including those who were blacklisted due to consecutive bounces, and are therefore unreachable

Legitimate interest

Another common legal justification for processing subscriber data is that the organisation responsible has a "legitimate interest" in doing so. "Legitimate interest" can apply in cases where a service has been requested by a subscriber, and storing their subscriber data is necessary for providing this service, or where an employer is processing the data in order to communicate with their staff. It can also apply to public relations professionals who maintain lists of journalists and associated data, depending on the circumstances.

Right of access

The GDPR grants people in the EU the right to access the data you have which relates to them.

- Check that your Admin Email address (“Person in charge of this system”) is accurately set so that subscribers can contact you
- (⇧phpList-3.3.3) When a subscriber requests their data, use the Data Export feature to download a report containing their data
- If you store data about subscribers in third party applications (e.g. Wordpress or a CRM system), export and include that data for the subscriber in response to their request as well

Right to rectification

The GDPR grants people in the EU the right to update inaccurate data which you store about them.

- Do not remove the preferences link placeholder within your campaigns to ensure easy access for subscribers
- (⇧phpList-3.3.3) Refer them to your phpList installation homepage (`http://your-domain.com/lists` by default) so they can find the preferences page if they don’t have a link
- (⇧phpList-3.3.3) Use the Preferences Page button on a Subscriber Details page to obtain a personalised preferences page link for a subscriber directly

Right to erasure

The GDPR grants people in the EU the right to have their data erased in some situations.

- To permanently delete a subscriber and all records related to them, first blacklist them and then Use the “Delete all blacklisted subscribers” button described above

---

Revision #2
Created 24 May 2019 14:00:38 by mariana

Updated 12 September 2019 19:52:02 by neil_brown