Privacy

- What is Privacy?
- Privacy By Design
- Food for Thought for Your Plugin
- External Resources

Are you writing a plugin that handles personal data – things like names, addresses, and other things that can be used to identify a person? You'll want to take care with that data and protect the privacy of your users and visitors.

What is Privacy?

WordPress.org made several enhancements ahead of Europe's General Data Protection Regulation. Following the launch of this work, we have made Privacy a permanent focus in core trac development, which will allow us to continue making enhancements on privacy and data protection outside specific legislation.

But what kind of issues might fall under the definition of "privacy", and how do we define it? Although privacy requirements vary widely across countries, cultures, and legal systems, there are several general principles applicable across any situation:

- **Consent and choice:** giving users (and site visitors) choices and options over the uses of their data, and requiring clear, specific, and informed opt-in;
- **Purpose legitimacy and specification:** only collect and use the personal data for the purpose it was intended for, and for which the user was clearly informed of in advance;
- **Collection limitation:** only collect the user data which is needed; don't make extra copies of data or combine your data with data from other plugins if you can avoid it;
- **Data minimization:** restrict the processing of data, as well as the number of people who have access to it, to the minimum uses and people necessary;
- **Use, retention and disclosure limitation:** delete data which is no longer needed, both in active use and in archives, by both the recipient and any third parties;
- **Accuracy and quality:** ensure that the data collected and used is correct, relevant, and up-to-date, especially if inaccurate or poor data could adversely impact the user;
- **Openness, transparency and notice:** inform users how their data is being collected, used, and shared, as well as any rights they have over those uses;

- **Individual participation and access:** give users a means to access or download their data;
- **Accountability:** documenting the uses of data, protecting it in transit and in use by third parties, and preventing misuse and breaches as much as is possible;
- **Information security:** protecting data through appropriate technical and security measures;
- **Privacy compliance:** ensuring that the work meets the privacy regulations of the location where it will be used to collect and process people's data.

(Source: ISO 29100/Privacy Framework standard)

While not all of these principles will be applicable across all situations and uses, using them in the development process can help to ensure user trust.

Privacy By Design

Many of these principles are espoused in the Privacy by Design framework, which states that:

- Privacy should be proactive, not reactive, and must anticipate privacy issues before they reach the user. Privacy must also be preventative, not remedial.
- Privacy should be the default setting. The user should not have to take actions to secure their privacy, and consent for data sharing should not be assumed.
- Privacy should be built into design as a core function, not an add-on.
- Privacy should be positive sum: there should be no trade-off between privacy and security, privacy and safety, or privacy and service provision.
- Privacy should offer end-to-end lifecycle protection through data minimization, minimal data retention, and regular deletion of data which is no longer required.
- The privacy standards used on your plugin (and service, if applicable) should be visible, transparent, open, documented and independently verifiable.
- Privacy should be user-centric. People should be given options such as granular privacy choices, maximized privacy defaults, detailed privacy information notices, user-friendly options, and clear notification of changes.

Food for Thought for Your Plugin

To help your plugin be ready, we recommend going through the following list of questions for every plugin that you make:

1. How does your plugin handle personal data? Use `wp_add_privacy_policy_content()` to disclose to your users any of the following:

- Does the plugin share personal data with third parties (e.g. to outside APIs/servers). If so, what data does it share with which third parties and do they have a published privacy policy you can provide a link to?
- Does the plugin collect personal data? If so, what data and where is it stored? Think about places like user data/meta, options, post meta, custom tables, files, etc.
- Does the plugin use personal data collected by others? If so, what data? Does the plugin pass personal data to a SDK? What does that SDK do with the data?
- Does the plugin collect telemetry data, directly or indirectly? Loading an image from a third-party source on every install, for example, could indirectly log and track the usage data of all of your plugin installs.
- Does the plugin enqueue Javascript, tracking pixels or embed iframes from a third party (third party JS, tracking pixels and iframes can collect visitor's data/actions, leave cookies, etc.)?
- Does the plugin store things in the browser? If so, where and what? Think about things like cookies, local storage, etc.

2. If your plugin collects personal data…
   - Does it provide a personal data exporter?
   - Does it provide a personal data eraser callback?
   - For what reasons (if any) does the plugin refuse to erase personal data? (e.g. order not yet completed, etc) – those should be disclosed as well.
3. Does the plugin use error logging? Does it avoid logging personal data if possible? Could you use things like `wp_privacy_anonymize_data()` to minimize the personal data logged? How long are log entries kept? Who has access to them?
4. In wp-admin, what role/capabilities are required to access/see personal data? Are they sufficient?
5. What personal data is exposed on the front end of the site by the plugin? Does it appear to logged-in and logged-out users? Should it?
6. What personal data is exposed in REST API endpoints by the plugin? Does it appear to logged-in and logged-out users? What roles/capabilities are required to see it? Are those appropriate?
7. Does the plugin properly remove/clean-up data, including especially personal data:
   - During uninstall of the plugin?
   - When a related item is deleted (e.g. from the post meta or any post-referencing rows in another table)?
   - When a user is deleted (e.g. from any user referencing rows in a table)?
8. Does the plugin provide controls to reduce the amount of personal data required?
9. Does the plugin share personal data with SDKs or APIs only when the SDK or API requires it, or is the plugin also sharing personal data that is optional?
10. Does the amount of personal data collected or shared by this plugin change when certain other plugins are also installed?

External Resources

- Privacy Blog

- WordPress.org Privacy Policy

□□□ #2
□ □□□ □□□ 2026-10-26 07:37:07 UTC
□ □□□ □□□ 2026-10-26 07:37:07 UTC