Plugin Topics: Thinking about privacy

Privacy in the context of a web application like WordPress goes beyond legal requirements. It's also answering the following questions:

- What information we collect
- Why we collect it
- How we use it
- how we protect it

Taken from ISO 29100/Privacy Framework standard, the following checklist provides a good starting point for thinking about privacy in general but more applicable in the context of a WordPress plugin that collects data from users and uses that data to create a service or site:

- **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.

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

In Food for Thought for Your Plugin, the WordPress theme provides a privacy checklist for you to use when planning your plugin and this is WordPress specific:

1. How does your plugin handle personal data?
    1. Use wp_add_privacy_policy_content to disclose to your users any of the following:
        1. Does the plugin share personal data with third parties (e.g. to outside APIs/servers)
            1. If so, what data does it share with which third parties
            2. Do the third partieshave a published privacy policy you can link to?
        2. Does the plugin collect personal data?
            1. If so, what data and where is it stored?
            2. Think about places like user data/meta, options, post meta, custom tables, files, etc.
        3. Does the plugin use personal data collected by others?
            1. If so, what data?
            2. Does the plugin pass personal data to a SDK?
            3. What does that SDK do with the data?
        4. 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.
        5. Does the plugin enqueue Javascript, tracking pixels or embed iframes from a third party?
        6. Does the plugin store things in the browser?
            1. If so, where and what? Think about things like cookies, local storage, etc.
2. If your plugin collects personal data...
    1. Does it provide a personal data exporter?
    2. Does it provide a personal data eraser callback?

    3. 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?
    1. Does it avoid logging personal data if possible?
    2. Could you use things like wp_privacy_anonymize_data to minimize the personal data logged?
    3. How long are log entries kept? Who has access to them?
4. In wp-admin:
    1. what role/capabilities are required to access/see personal data?
    2. Are they sufficient?
5. What personal data is exposed on the front end of the site by the plugin?
    1. Does it appear to logged-in and logged-out users?
    2. Should it?
6. What personal data is exposed in REST API endpoints by the plugin?
    1. Does it appear to logged-in and logged-out users?
    2. What roles/capabilities are required to see it? Are those appropriate?
7. Does the plugin properly remove/clean-up data, including especially personal data:
    1. During uninstall of the plugin?
    2. When an related item is deleted (e.g. from the post meta or any post-referencing rows in another table)?
    3. 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?

There's a lot to think about when it comes to WordPress, privacy and using third party plugins. If you're in doubt your best bet is always to ask a lawyer, preferably one with experience in privacy and its legal requirements.