

Data protection & privacy when you support OCA's projects

We have decided to clarify the best practices that we expect all volunteers to follow in order to contribute to transparency, a climate of trust, and also to comply with our legal obligations regarding data protection (including the GDPR, General Data Protection Regulation).

If you have any questions or suggestions, please write to us at privacy@odoo-community.org

Data protection at OCA

When you contribute to OCA projects as a volunteer, you may sometimes be required to handle information about other volunteers or participants in online workshops, for example when you help others who are using Odoo ERP, when you give a presentation about Odoo or OCA, when you are helping us with our communication or our website.

This information, when it allows a human being to be identified (directly or in combination with other information), is considered personal data.

Whether you receive it by participating in OCA activities, using the platforms set up by OCA (Odoo forum, Github, Discord,..) or directly from the person. For example, a picture or a custom image used as an avatar, voice, name, pseudonym, phone number, email address,...

Purpose of the volunteer assignment

When you receive access to personal data in order to carry out certain volunteer tasks :

- Use the personal data only to perform the intended task
- Do not disclose to third parties any information (including personal data) you have access to without OCA's approval
- Do not change anything (unless it is part of your mission)
- Use only the tools (software, hardware, online platform, app) that have been validated in advance by OCA
- Do not collect or use « special categories » of personal data without OCA's approval. Special categories are personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

Security and data breach

Be careful and attentive whenever you use personal data in any aspect of your work as a volunteer.

In case of any event impacting personal data and that could lead to a breach

- from a confidentiality perspective (e.g., someone accesses data that they should not be able to access),
- from an availability perspective (e.g., data can no longer be accessed because a document has been misplaced),
- from the integrity of personal data (e.g., someone has modified information contained in the database without authorization)

We ask that you notify us as soon as possible at privacy@odoo-community.org whether the event is accidental (e.g. loss of a USB key containing personal data, sending an email to the wrong person) or malicious (email containing a virus or scam/phishing).

You will be given further instructions as appropriate.

Question about data protection

If someone you interact with in the course of your volunteer work asks you questions about data protection at OCA (for example, they wish to exercise their right of access, or they want to know how OCA is using their personal data):

- Notify us as soon as possible at privacy@odoo-community.org
- Confirm to the person that you have forwarded his/her question internally and that we will get back to him/her as soon as possible.

What is at stake if you don't follow our guidelines ..

..for you ?

If you use personal data that you have accessed through OCA's projects to perform something for your own purpose, outside a purely personal / household activity, you can be considered as a data controller under GDPR (General Data Protection Regulation), and other data protection laws.

Being a data controller implies to respect a lot of legal obligations :

- to follow principles when using the personal data and implement tools and documentation to be able to prove compliancy ;
- to allow data subjects to exercise their rights.

In case you are considered as a data controller and you don't respect GDPR obligations, the penalties include fines up to 4% of worldwide annual turnover or €20 million (whichever amount is the greatest) and, in certain very specific cases, criminal fines.

..for the human being to whom the personal data refers ?

Taking care of someone else's personal data is caring about her/his privacy and safety.

If you don't do this, instead of building trust, you will contribute to increasing the risk of this person's rights and freedoms being violated. That can mean physical or moral aggression, being exposed to scams, anxiety, manipulation, discrimination,...

Remember that the disclosure of personal data that seems harmless to you can put the person in danger, depending on her/his own context.