Setting up CiviCRM for UK GDPR

Tuesday 9th June 2026

Mads Mitchell
CiviCRM & Data Privacy Specialist

Pooka & Co Ltd
Great Michael House
14 Links Place
Edinburgh, EH6 7EZ
www.pooka.co

A word about UK GDPR, PECR, and consent

1. **The rules about email marketing sit outside of UK GDPR, in the Privacy and Electronic Communications Regulations (PECR).**
   We're going to talk about them anyway.

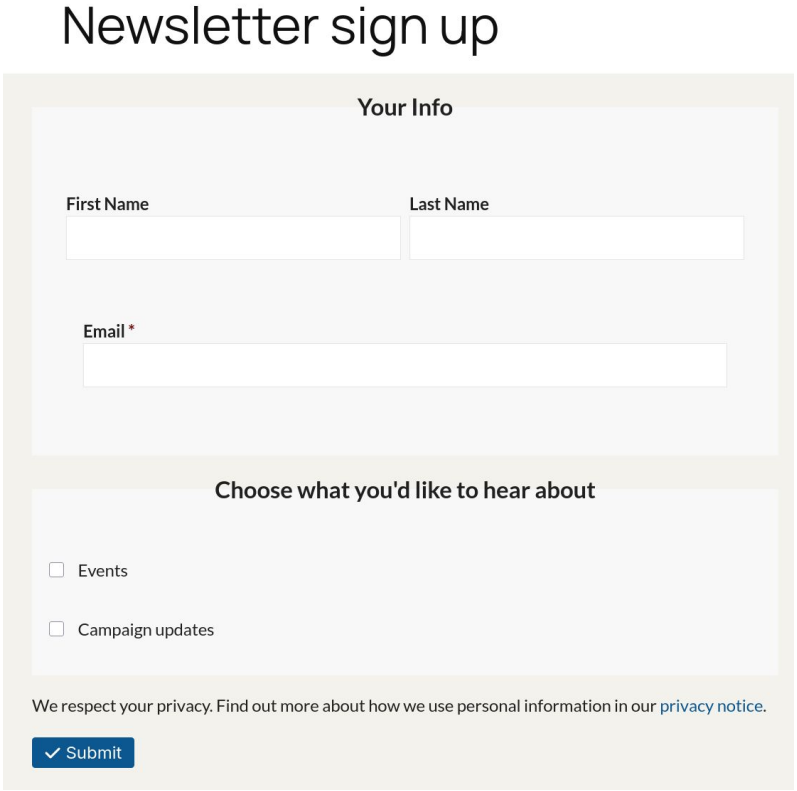
2. **Consent is (almost always) required when sending marketing emails.**
   If you're not asking for consent and you can't explain why, you might want to think again.

3. **Not all emails are marketing emails, so not all emails require consent.**
   You don't need permission to send service messages such as receipts or password reminders. But if you start including marketing content, you run the risk of turning these into marketing messages too.

4. **Your newsletter is almost certainly going to be classed as marketing.**
   You'll need to be able to show that recipients consented to be added to any mailing lists, and give them the option to revoke that consent.

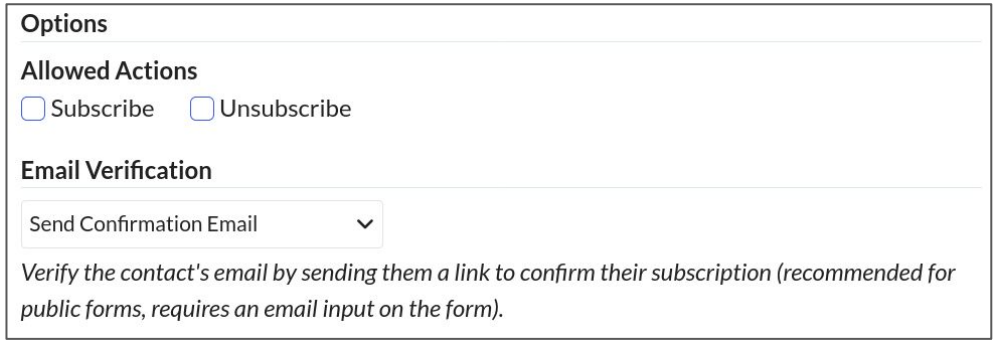
   (unless you're relying on the soft opt in, but if you're doing that then you already know what I'm talking about)

Creating sign-up forms in CiviCRM



FormBuilder Group Subscriptions:

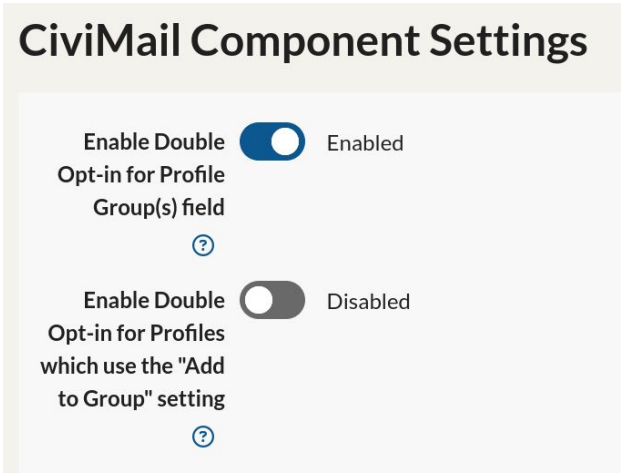
- Choose whether your form subscribes or unsubscribes users, or both
- This means that you can include these fields in different scenarios without essentially prompting the user to opt out of mailing lists
- Send an email confirmation - double opt in!



Creating sign-up forms in CiviCRM

Where using profiles:

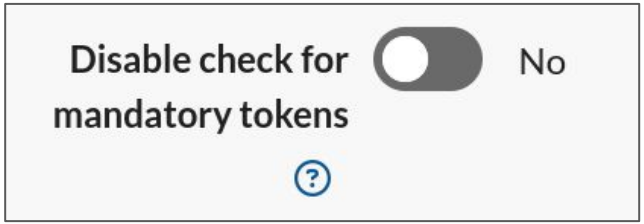
Enable settings to ensure double opt-in is in place - which one you use depends on how you choose to configure your profile



Opting out and unsubscribing

Mandatory tokens

- CiviCRM checks for 'mandatory tokens', meaning any mailings you send must include these or you'll see an error message.
- Add these as links in your mailing template to make sure they're included every time.
- When a Contact receives a mailing, clicking on one will automatically update CiviCRM.
- **{action.unsubscribeUrl}** 'Unsubscribe' removes the user from that specific Mailing Group.
- **{action.optOutUrl}** 'Opt out' will add the 'bulk opt out' privacy flag to a contact record, and they won't receive any bulk mailings that you send through CiviCRM



You need to include these tokens in each mailing - including 'b2b' mailings, and where you've used the soft opt in.

UK GDPR - applying the principles

Purpose limitation

- How did this get here and what's it for??

Data minimisation

- … do you actually need all of this info, or did you collect it because you could?

Storage limitation

- Do you still need it?

Accuracy

- Is it correct? If you've had it for a while, does it need to be reviewed?

Integrity & confidentiality

- Who needs access to it? Who doesn't - but is able to access it anyway?

Making use of CiviCRM features

Collecting personal data

Review what you collect using profiles or forms for membership sign up, events registration, donations etc

- Identify the information that you absolutely must have in order to do the thing you're doing. Do you really *need* to collect a date of birth, or a home address?
- If not, make sure it's clear why you're asking for it and that folk can decide whether to give it
- Take steps to help ensure what you collect is accurate. Consider address validation - there are various extensions available

Go self service

- Consider asking contacts to review their contact information for accuracy - consider providing a profile for logged-in users to access, or use checksum to let Contacts do this via a special link in an email
- Be careful about this - don't go asking for marketing consent when you're doing this
- If for any reason you decide to ask for fresh consent for marketing, bear in mind you'll invalidate existing consent if folk don't reply!

Making use of CiviCRM features

Think about your Contact Records

- Consider using contact subtypes - you might find it simplifies things where there are bits of information you only want to collect for volunteers, or politicians, or other distinct types of stakeholder. It keeps things a bit neater, and helps identify genuine gaps in your data.

Should everyone be able to access this?

- Not everybody in your organisation needs access to everything. Think about roles and specific tasks that members of your team need to carry out
- Grant access on a need-to-know basis using ACLs - *access control lists*
- Limit what different users can see using either Groups of Contacts, or specific fields
- Limit the actions that users can take - you might want to grant read-only access to certain bits of data
- **Extra tip:** FormBuilder is a great way of providing access to specific bits of data without granting access to the back end of CiviCRM

Making use of CiviCRM features

Deduping - your enemy and your friend

- Understand the implications of any dedupe rules you're using - what sort of damage could accidentally merging or updating records cause?
- There's value in allowing duplicates!
- Build in time for regular deduping work - you'll understand your data better and it'll help build confidence in the accuracy of what's being stored.

And finally, a word of warning - if you're not confident that your data is totally deduped, or you're not totally on top of understanding your organisation's retention schedules, tools like the GDPR extension can be incredibly destructive. Approach with caution.

Thanks!

Pooka&Co

Mads Mitchell

CiviCRM & Data Privacy Specialist

mads@pooka.co

www.pooka.co