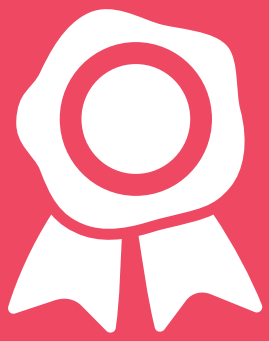
The GDPR and Engaging Networks

The General Data Protection Regulation (GDPR) aims to strengthen and unify data protection within the European Union. It becomes enforceable from 25 May 2018 and organisations that collect and use personal data will need to be aware of its principles and ensure they are compliant with them.



This document lists the features of Engaging Networks and how they can be used to tackle various requirements of GDPR.

Please note that there are other requirements of GDPR not referenced here because they are not related to the use of a digital engagement platform like Engaging Networks.

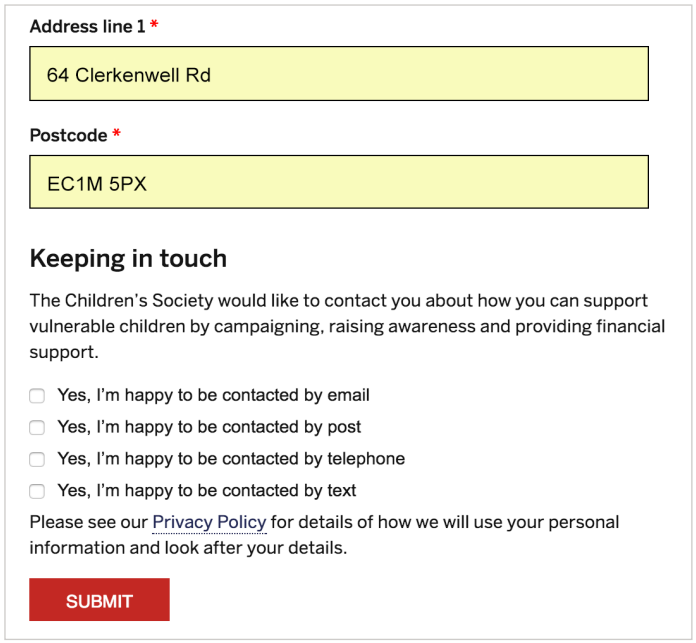
engaging NETWORKS
SOFTWARE LOVE

Opt-ins

Consent is managed in Engaging Networks using opt-ins. Opt-ins are "questions" that track a supporter's response to an on-screen statement as either Yes (Y) or No (N). The statement can be placed on any Engaging Networks page as a checkbox or radio buttons. It is also tied into your email campaigns' unsubscribe links.

When someone submits a page or changes their subscription status, the value of the opt-in is recorded as a transaction, which is a row of data which includes where and when they submitted their response. This means you build up an exportable audit log of a supporter's consent status and have proof of consent. In late March 2018, this data will also be viewable within each supporter record.

We will extend this functionality further this year, by creating a log of opt-in text changes, so you can more easily relate a supporter's consent to the statement they signed up to.



The Children's Society have multiple opt-ins and include a link to a privacy statement

Why is this important for GDPR?

One key component of GDPR is the Lawful basis for processing: Consent. In particular, you must "Keep evidence of consent – who, when, how, and what you told people". The design of our opt-in functionality means you are keeping an audit log of consent that you can export at any time.

Multiple opt-ins

You can have as many opt-ins as you need, each with different statements, and include as many or as few as required per page. In addition our 'locale' feature means you can use the same opt-in to record different statements in different languages depending on the supporters' preference.

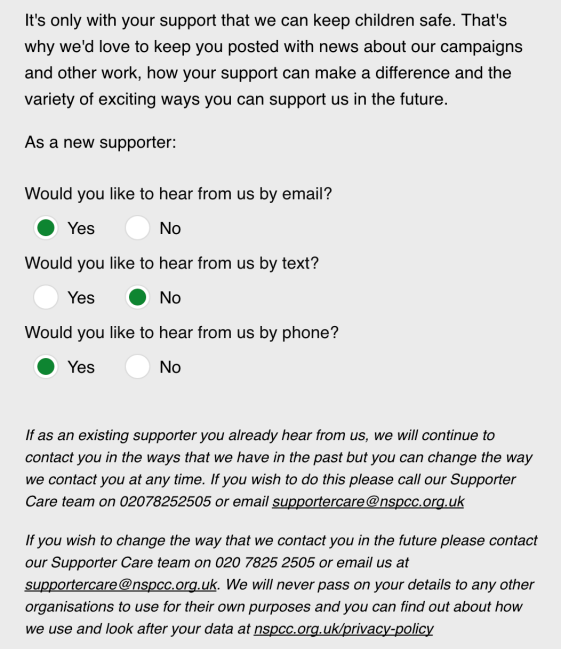
Why is this important for GDPR?

You are advised to "Be specific and 'granular' so that you get separate consent for separate supporter activities. Vague or blanket consent is not enough." You can create your opt-ins to make each specific to channel or content, thereby collecting separate consent for separate activities.

Shared components

Opt-in questions are shared components, which means if you amend the opt-in label in one campaign, it will change it for any other campaign using the opt-in. They have two editable labels - one above the checkbox, or radio buttons, and also a label next to the opt-in field itself called the Default Content. You can manage these via the manage opt-ins button in form blocks.

But it's not just opt-ins that can be shared components. You can place a text block on your page to contain your privacy policy, or include the statement in your templates. This means that should you need to update a policy you don't need to worry about changing it in more than one place.



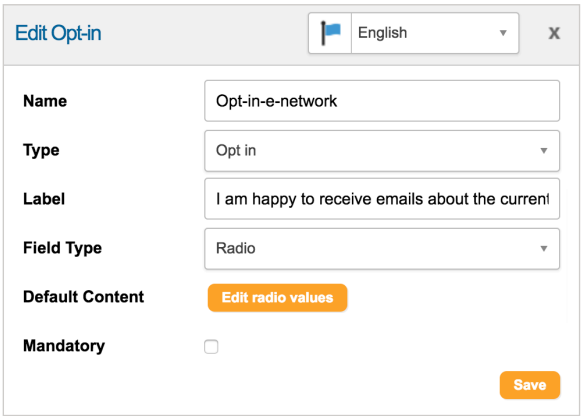
The NSPCC's opt-ins are shared components

Why is this important for GDPR?

For **Lawful basis for processing: Consent**, you should "Check your consent practices and your existing consents. Refresh your consents if they don't meet the GDPR standard." Shared components ensure your changes are immediately applied to all your live pages and can be used to display information and cover the GDPR's **Right to be informed**.

Opt-in question settings

You have many different options for your individual opt-in questions to ensure they meet your needs. As mentioned previously, you can either show them as a checkbox or as a pair of radio buttons. In addition, you can add an extra step so that your supporters have to confirm that they wish to opt-in via an email link.



Engaging Networks' opt-in manager offers several settings

Why is this important for GDPR?

GDPR says that "Consent requires a positive opt-in. Don't use pre-ticked boxes or any other method of default consent.". Further GDPR states "Avoid making consent to processing a precondition of a service.". If you are using a checkbox for your opt-in, uncheck the "pre-tick" option so it will display unchecked on a page. If you use a radio HTML format for your opt-in, then you do not have to have any of the two options pre-selected. Making this question mandatory will mean the supporter is prompted to choose an option, but do not have to choose Yes to continue.

Opt-in account settings

There are several account-wide settings that allow you to fine-tune what happens when an opted-in supporter chooses "No" on a page's opt-in question. And in the next mid-February release you will have the option to hide opt-in questions entirely for supporters that are already opted-in. If you choose to use this, this will greatly improve your retention of subscribed supporters.

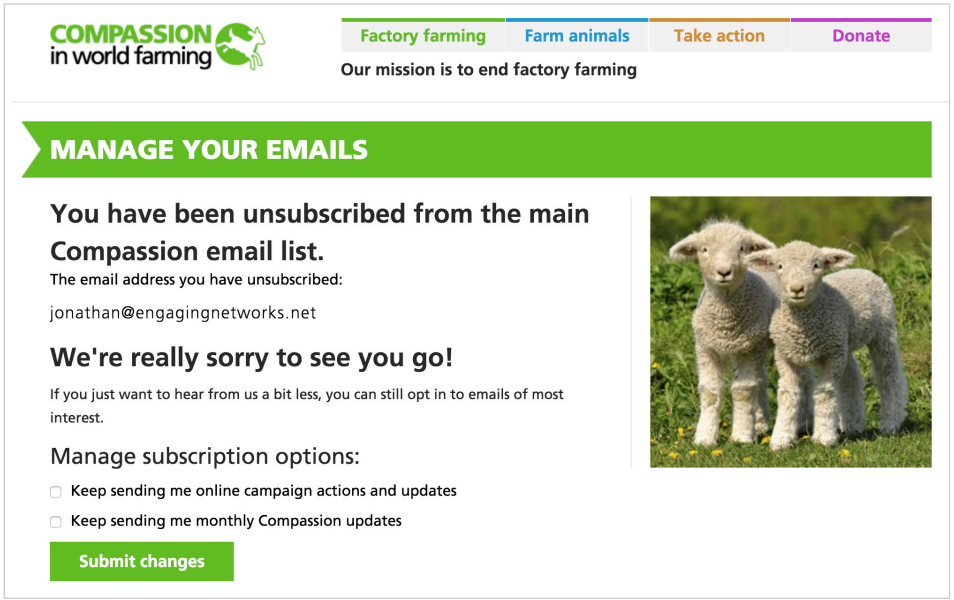
Why is this important for GDPR?

Ensuring you do not lose supporters as a result of tightening your opt-in procedures in response to GDPR and Consent is vital. These tools, and ones in development in response to client discussions, will help ensure this.

Unsubscribe links and pages

It is a simple process to add unsubscribe links to your email campaigns, or to a template, so that every email campaign you send includes these links by default. Unsubscribe links work in one of two ways:

- a supporter clicking on an unsubscribe link immediately sets the opt-in question to an 'N' value and displays the supporter a confirmation page when clicked
- it is also possible to create a special subscription management page, showing the supporter their current status of opt-in questions so they can manage them or give reasons for leaving.



Compassion in World Farming have an unsubscribe landing page that allow you to manage the kinds of messages you receive

Why is this important for GDPR?

As part of **consent**, you need to "make it easy for people to withdraw consent and tell them how". Email templates will ensure there is always an easy way to unsubscribe, and you can present other methods to withdraw consent in email and page templates.

Email to target

Email to target campaigns allow your supporters to email messages to a target, or targets, for example their local MP. You can allow for the message to be editable by the supporter so that they can amend the message they send or add personal comments. There is an account setting to control whether the system stores these messages for your records.

Also, by default, messages are sent immediately from your supporter to the target. If you wish for the supporter to instead confirm first that they wish to send the message, then you can switch on a setting that postpones the send until the supporter has clicked a confirmation link in an auto-generated email.

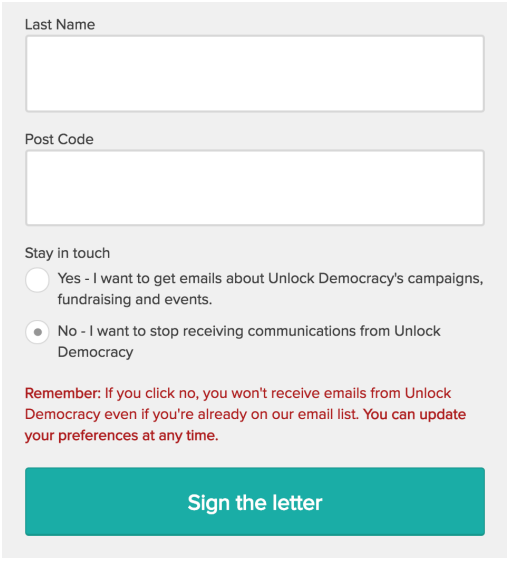
Why is this important for GDPR?

The settings you choose will help ensure your supporters' **right to be informed** is adhered to and that you are following the concept of **data protection by design and default**.

Page design flexibility

The Engaging Networks system is fully flexible; we don't restrict your page design, page function, or page content. Code blocks enable you, or the agencies you work with, to add bespoke javascript and regex validations. This enables form fields to respond quickly to data that is incorrectly entered. Some examples of this that are GDPR-related include:

- only asking for the data you need to ask for - the only required field is email address for any form, and postcode is required when setting up email to target campaigns that need the supporter matched to a local or regional decision-makers
- there is one exception to the point above - it is possible to hide the email address field for anonymous surveys, but still save responses
- displaying a message when a supporter selects "No" for their opt-in status (radio button HTML format) increases opt-in rates (this is available to implement now using simple javascript, but will be added as an opt-in setting in a release this year)
- adding address-lookup / validation plugins to ensure the data you collect is accurate at the time of collection
- recording the opt-in statement text on submission along with the status.



Unlock Democracy use a custom alert when a supporter chooses No

Why is this important for GDPR?

The settings you choose will help ensure your supporters' **right to be informed** is adhered to and that you are following the concept of **data protection by design and default**.

The supporter database, exports and imports

Every supporter has a unique record in Engaging Networks that can be viewed on amended individually or in a batch via import. Data can also be exported batches directly from the account dashboard.

Every time a supporter submits their data on Engaging Networks page our software records a transaction. This applies to all activity (e.g. someone completing a form to signup for a newsletter, makes a donation, or sends an email message to their local MP. The data includes the date and time of the transaction, along with the page name, and other information to give you a complete picture of activity. In March 2018, we are adding functionality that records what we call the 'origin source'. This will preserve the information that identifies how someone is initially added to the database, until the record is deleted.

You can delete a supporter and their transactions from your Engaging Networks database by looking up their record in the Supporter Lookup, and clicking the red X icon next to their name.

Why is this important for GDPR?

GDPR gives individuals the right to have personal data rectified if it is inaccurate or incomplete under their **right to rectification**. The **right to be informed** asks that you keep track of "the source the personal data originates from and whether it came from publicly accessible sources".

You can delete a supporter and their associated transaction by searching for and deleting their record, obeying their **right to erasure**.

Exports mean you can pass on any information to your supporter should they request it, obeying their **right to access** and **right to data portability**.

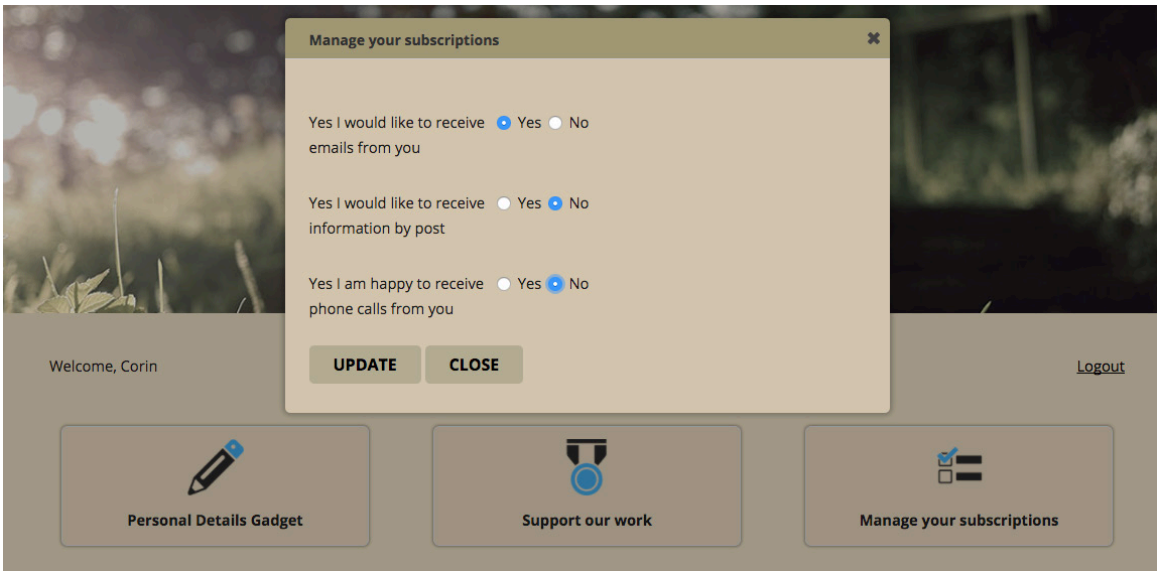
The Hub

The Hub allows your supporters to manage their constituent data at any time. This new technology uses an email challenge and response login system, and offers separate gadgets to display to the supporter their stored data values such as their address or phone number, as well as their subscription status (opt-in responses). A link for supporters to access The Hub can be added to your website, or email communication.

Additional gadgets can be added to encourage your supporters to increase a monthly donation, or find out how the campaigns they have taken part in are progressing.

Why is this important for GDPR?

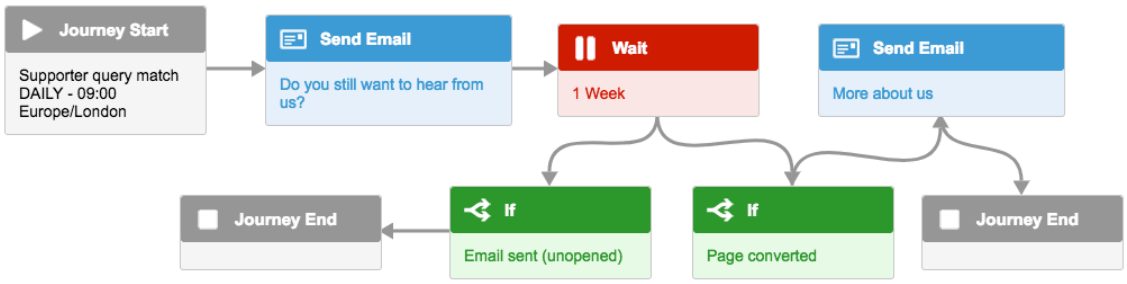
This covers many aspects of the GDPR. One requirement, as discussed earlier, requires you to have active consent for communication, and "the right to withdraw consent at any time, where relevant". As a self-management tool, supporters can opt-in or opt-out using The Hub. As part of their **right to rectification** supporters can amend their personal data and as part of their **right to access** to see what data you hold.



Manage your subscriptions gadget in The Hub

Marketing automation

Marketing automation allows you to create a series of dynamic email workflows (workflows change as a supporter engages with the content.) Amongst other things, they can be used together with our email engagement scoring to send emails to supporters that have not responded to your email communication (for example their engagement score suggests they have not opened an email for over a year).



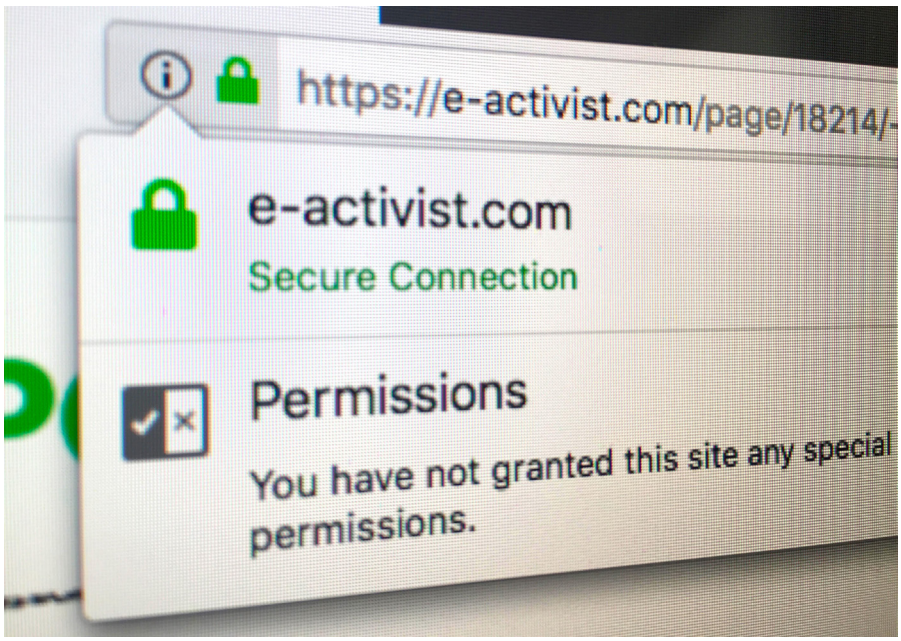
We are extending the functionality of marketing automation this year to automatically send an email to supporters asking them to re-subscribe if they have not responded to any communication for a specified period of time since they last confirmed their opt-in status.

Why is this important for GDPR?

You may interpret GDPR's consent requirements to mean that you should regularly check-in with your supporters to ensure their Consent is recent and that they are aware they are opted-in to receive your communications.

Security

You have full control over which members of your organisation can access Engaging Networks, and permission groups give you fine-grained permissions so that users can only access certain areas of the software, or see certain supporter data.



We implement onboarding and exit procedures to make certain that you know how to provision the minimum access required for team members to perform their duties. We also review with you the process for terminating access as appropriate as job responsibilities change.

We can help you through the procedures to add secure certificates to your pages so that the browser reports the page as fully secure and your supporters' data is encrypted.

Engaging Networks is PCI Compliant (VISA Merchant Level II). In addition, our Managed hosting provider is ISO 27001 certified and also maintains PCI certification.

Maintaining PCI Compliance requires that Engaging Networks engage in ongoing activities that include, but are not limited to, build and maintain a secure network, protect sensitive data, maintain a vulnerability management programme, implement strong security measures, and regularly test and monitor networks and systems.

Engaging Networks is required to produce an annual Self-Assessment Questionnaire (SAQ D), quarterly network scans, and Certificate of Compliance from our security consultancy.

As with any other part of the platform, we continue to add additional functionality to make the software even more secure. For example, we are introducing two-factor authentication for logging in later this year.

Why is this important for GDPR?

Data protection and security is a key component of GDPR.