Data, data everywhere... GDPR - a practical guide

Version 1, August 2020

What is the GDPR?

The General Data Protection Regulation, or GDPR, is a set of EU (boo! hiss!) regulations covering the collection, storage and use of personal data. It doesn't go away with brexit either - it will then be incorporated as part of UK law. Just because you are a well-meaning community group fighting for landrights for gay whales, doesn't mean you are exempt. Falling foul of GDPR will cost time, money and credibility.

Why is complying with the GDPR so important?

As an activist organisation, people generally allow you to use their information because they share your beliefs and goals, and want to work with you to make them happen. They trust you to use their data as part of this. It's generally a good idea not to piss these people off. Selling their personal data to pyramid schemes and penis enlargement companies is a sure-fire way to make sure they never give you their data again, tell everyone they know that you can't be trusted, and generally make your life as difficult as possible. This probably won't help your campaign get off the ground.

But we're just trying to save the planet, surely this doesn't apply to us?

The EU doesn't care how well-intentioned you are or how curvy your bananas are. All organisations that process personal data need to comply with the GDPR. There are good reasons for this. Ultimately, personal data is information about people, and, if it isn't handled correctly, that information can be used to exercise power over them. When data gets into the wrong hands, or is used in the wrong ways, there can be serious, real-life consequences. Not keeping information secure could expose people to identity fraud. Sending information to the wrong email address might reveal an activist's trade union membership or chronic health condition to their employer, who can then use that against them. Or maybe it'll just be used to bombard them with nuisance calls all day, every day.

What happens if we don't comply with GDPR?

People will complain. A lot. Now that people know they have data protection rights, they will use them. So if you use the email address someone gave you for a Veganuary petition to try to sell them pangolin burgers, you'll hear about it. You will spend so much time reading and replying to complaints about how you are useless, and generally trying to make people trust you with their data again, that you won't have time to go out and get enough signatures for your petition, animals will die, the ice caps will melt and it will be your fault.

But we can just ignore the complaints, right?

Sure, but it won't end well. The GDPR also gives people the right to complain to the Information Commissioner's Office. The ICO is the regulator for data protection in the UK, and one of its jobs is to make sure organisations follow the GDPR. If you don't, they can come round to your house, break the door down and send you off to a re-education camp. They won't always go that far – they might just tell you to fix the mess you created and tell you how not to be so rubbish next time. For more serious breaches, they can legally require you to get your shit together, or else. If you mess up really badly, they can fine organisations, up to 20 million euros or 4% of their annual turnover, whichever is larger. This might be more than your group can cover. If they do take action against you, they'll also publish this, and everyone will know you are officially Not To Be Trusted.

Even if you do not end up getting sent into information exile, an investigation by the ICO will take up your time, involve answering difficult questions about why you messed up, and require you to prove that you won't be so useless again.

OK, OK, I'm convinced! Just tell me exactly what I need to do to comply with GDPR.

Sadly, there isn't an easy set of boxes to tick here. The GDPR applies to all organisations, so it's a general set of principles and rights rather than an instruction manual. You will need to look at the core concepts and principles and spend time working out how you are going to make these work in the context of your organisation's activities.

Help me out a bit, what are the main things I should know?

First of all, you need to be clear and open with people about how you are going to use their personal data. The right to be informed (Article 12) gives people the right to know how you are going to use their data, *before* you use it. If you haven't told someone how you

will use their data, you can't use it. And you can't make up new and exciting ways to use their data once you have it. If you are going to use someone's email address to register for a petition AND to contact them about more petitions later on, you need to tell them that you are going to use it for both things. You also can't tell them it's just for this one petition, and then later on decide that you have all these other important petitions you definitely need to tell them about. You have to be open and transparent, so that people know what to expect and there aren't any nasty surprises lurking later on.

You also need a damn good reason to be processing their personal data. The GDPR gives you six damn good reasons, which it chooses to call a 'lawful basis'. The most famous of these is consent, and it is the one that will likely apply to most of what you do. There are five other lawful bases, as consent isn't always appropriate for things that still need data to be processed – if you could just not consent to letting the taxman have your information, life would be a lot cheaper. However, for most activism, consent will be the right lawful basis. This is pretty logical – if you are representing people's voices, you can't really do that without them agreeing to it. So, if you want to add someone to your mailing list, you will need their consent to do so.

You do need to be able to demonstrate you obtained consent though, you can't just assume it. That way, if someone says they never consented to you emailing them, you can show that they did, actually, and you were right all along.

Security. You need to keep information secure, and stop it falling into the wrong hands, or getting lost. You can't just keep people's information in a big pile in your car, or just upload it to your facebook profile. It needs to be stored, and in a way that no one without a legitimate reason can access it. This might mean storing it in a locked filing cabinet, or on a secure, firewall-protected computer. This also applies when you are sending information. Two of the most common ways that information gets disclosed is by sending it to the wrong address (postal or email), and by CCing instead of BCCing when sending emails. CCing lets you see everyone else's email address. It might not sound like a big deal, but it might let someone unscrupulous contact them. And if you are dealing with sensitive issues, simply revealing that you sent an email to a person can be a big deal. What if your organisation supports asylum seekers, or provides services to people with HIV+ status? That one email can reveal a lot of information about someone's life.

Access. People have the right to see what information you hold about them, so that they can find out if you are using it correctly. So they can ask you for it, and in most cases you will need to provide it, within a month. They won't have to pay, and they do not have to ask in any special way – as long as they have asked for some information about themselves that you have, you probably need to give them a copy.

How can I move from novice level to practitioner level at this?
Read this guide, put it in practise and use the development resources! Ask us questions (we may not know the answer). Check out our website

*Novice and practitioner level is a reference to the Active Citizenship Toolkit, which CEM and allies are developing. See here

[Version 1.0 August 2020 Text by A CEM Supporter]

www.climateemergencymanchester.net
@climateemergmcr

Development resources

These are all from the ICO website. GDPR is kind of their thing, and because they've put together a bunch of useful free GDPR resources, no one else has.

Practitioner

Here's a relatively simple checklist of the basic things you'll need to do to comply with the GDPR. There are extra tips on how to do those things by clicking the more information options.

https://ico.org.uk/for-organisations/business/assessment-for-small-business-owners-and-sole-traders/

Here's a set of FAQs that are often asked by small organisations. Chances are the thing you need to know is on here.

https://ico.org.uk/for-organisations/business/sme-faqs/

Their advice to the general public is not too technical and explains a lot of what you'll need…

Consent and other ways to process data

https://ico.org.uk/your-data-matters/does-an-organisation-need-my-consent/

The right of access

https://ico.org.uk/your-data-matters/your-right-to-get-copies-of-your-data/

Expert

There's no way around it, you're going to have to dive into some incredibly technical stuff here. If you fancy a little light reading, there's a very detailed guide to the GDPR. Key sections are:

What is personal data?

https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/key-definitions/what-is-personal-data/

Lawfulness, fairness and transparency

https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/lawfulness-fairness-and-transparency/

Security

https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/security/

Consent

https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/consent/

Right of access

https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-of-access/

If you've read those and you still have the will to live, read the rest of the guide and you'll be a GDPR ninja in no time.