The CAG Project Overview of: General Data Protection Regulation

This overview was compiled in 2018 by The CAG Project, with support from our GDPR volunteer, Marta Lomza.

Contents

1. What on earth is GDPR?
2. What are the key general considerations for CAG groups?
3. Checklist
4. How is the CAG project going to support groups?
5. Further reading

1. What on earth is GDPR?

General Data Protection Regulation (GDPR) is a strengthening of the existing Data Protection regulations to bring control back to us individuals over how our personal data is being used – this is a very positive move.

Because each CAG holds some personal data, there is a legal requirement for all CAGs to be ready for GDPR when it comes into effect on the 25th May 2018.

Definitions

General Data Protection Regulation (GDPR) intends to strengthen and unify data protection for all individuals within the European Union (EU). Ultimately control is being given back to citizens and residents over their personal data.

Personal data – any information relating to an individual which can be used to identify this individual (name, address, phone number, CCTV footage, etc.)

Sensitive personal data – data which is 'particularly sensitive in relation to fundamental rights and freedoms', for example ethnicity, religion, sexuality, health.

2. What are the key general considerations for CAGs?

The main points you need to think about are: what you do with the personal data you hold and how you protect individuals' rights specified under GDPR. You will also need to create a set of documents as proof that your measures are in line with GDPR.

CAGs will need to be able to answer these five basic questions:

Q1. What personal data do you hold?

For example, volunteer email addresses, members' names, information about payments to individuals, CVs, CCTV footage, photos.

Writing down all the types of personal data you hold, where it came from, who has access to it and what you do with it, will be the basis of your GDPR documentation.

Q2. Where you hold this data?

For example, on your laptop, Dropbox, Datto, email account, MailChimp, word or excel document, in paper form? Listing all the places where it is stored is important because of the need to ensure individual rights specified in GDPR.

For example, individuals have the right to access their data, and for their data to be amended and deleted without delay when they ask – so you need to know where their data is if you want to do any of these actions.

Q3. Why do you hold this data?

In GDPR terms, what is your 'lawful basis' for holding it? You can choose one of six 'lawful basis' options for storing your personal data.

- Legitimate needs (of the group or organisation)
- Vital information (life or death)
- Contract with individual
- Comply with legal obligation (required by UK law or EU law to process these data)
- Public task (official functions or tasks in public interest)
- Consent

For most CAGs, this will be one of two: 'legitimate interests' or 'consent'.

'Legitimate interest':
This will likely be the best option if your organisation collects people's data to enable you to carry out your regular, day-to-day operations, and where you will use these data in a way individual's will expect. For example, if you ask people to sign up as volunteers, and then use their details to send them your organisation's newsletter or contact them to tell them you're closing over Christmas, all of this is covered under your 'legitimate interests'.

'Consent':
This is quite a complicated category, aimed at giving individuals very close control over their data. This will often be the most appropriate option for sensitive data, such as people's medical records or any data relating to their religion, ethnicity or sexuality. When you choose consent, you will need to keep documentation proving the individual did grant their consent, and if you ever want to use their data for a purpose different than the one you had originally told them about, you will have to get back in touch with them and ask for consent again.

> **Tip:** *Remember – whatever 'lawful basis' you go for, you will need to explain to individuals why you collect personal data and how you process it, so your volunteers or members can decide whether they want you to have their data. This is actioned through publishing a document called a 'privacy notice' and clearly communicating it with individuals whose data you collect.*

Q4. How you hold this data? How secure is it? How do you share and process it?

This is about reviewing how you keep personal data. Look at your security measures and think about who has access to your data, how you share this data within your group, and how easily this data could be accessed by someone who is not authorised to see it.

This might mean you need to introduce strong passwords to your spreadsheets, not sharing via email, but it also refers to simply taking caution to ensure you're not working on these data in a public space - where these details could be exposed. Have a think about what formats you keep your data in – remember it

needs to be 'portable', which means the individual concerned must be able to easily copy it and carry it away for their own purpose if they'd like to.

Q5. How long do you hold this data for?

Only keep data for 'as long as necessary'. Each type of data has its own advised 'retention period' – the timeframe you should be keeping it for – and you should not keep personal data beyond that specified timeframe. For more information about the retention principle check this website.

By gathering together all this information you will have the basis to create your organisation's own data protection policy, which will be part of your GDPR documentation - to make you GDPR ready.

Importantly, as always, the CAG project will provide support (see section 3) every step of the way - to make sure this compliance process as smooth as possible for you all.

> **Tip:** *Useful template to help you to do an audit based on the questions above can be downloaded here.*

3. Checklist

As a small organisation, you need to document personal data processing activities which are 'not occasional' (the means activities which you carry out regularly, as part of your regular day-to-day work).
You need the following documentation:

1. Data Protection Policy

At the minimum, your policy should include the following (most of which is related to the five questions outlined in section 1):

- The name and contact details of your organisation (and where applicable, of other controllers)
- The purposes of your processing (why you collect the data)
- A description of the categories of individuals and categories of personal data (what data you collect)
- The categories of recipients of personal data
- Details of your transfers to third countries including documenting the transfer mechanism safeguards in place (if applicable)
- Retention schedules (how long you keep each category of data for)
- A description of your technical and organisational security measures (this is where you describe where your data is stored, how it is protected through passwords etc., who has access to the data, who in your organisation is responsible for overseeing data protection issues and reporting data security breaches, etc.)

You might also want to use your policy document to detail how you will ensure your organisation will protect the eight individuals' rights listed under GDPR.

☑ **Privacy policy template – download here.**
☑ **8 Data protection principles checklist – download here.**

2. Privacy Notice

The Privacy Notice is how you ensure the 'right to be informed' is upheld – this is where you inform your data subjects about what you do with their data. At a minimum, the privacy notice should include:

- Your name and contact details
- What you are going to do with their information

- Why you collect it – this is where you tell them what is your 'lawful basis' for processing. If it is 'legitimate interests', you should explain what these are
- Who you will share the information with
- Individuals' rights (as listed under GDPR)
- Anything else you think you need to tell them which will ensure your data processing will be fair, transparent and lawful, for example telling people how they can contact you to have their data withdrawn or corrected

☑ **Privacy Notice Template – download here.**

3. Data Breach Procedure

This is where you describe how you would deal with a data breach. A data breach is 'breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data'.

You must keep a record of every data breach you are aware of, and of how you have dealt with it. 'Dealing' with would normally mean fixing the issue as soon as possible, but also investigating how to prevent similar incidents in future.

Where the data breach can result in a risk to people's rights and freedoms, you must report it to the Information Commissioner's Office. You do not need to report it if there is no such risk, but you still need to deal with it and keep a record of how you dealt with it.

For further guidance on data breach management download this guide.

☑ **Template Data Breach Incident Form – download here.**
☑ **Template Data Breach Preparation Checklist – download here.**

4. Records of Consent

If your lawful basis for processing the data is 'consent', you must document each individual consent. This will include a record of 'when and how' you got consent from the individual, and exactly what they were told at the time.

☑ **Consent guide link – download here.**
☑ **Consent request email template – download here.**
☑ **Valid declaration of consent checklist – download here.**

> **Tip:** *You also need to document activities where the data you collect may put the rights or freedoms of individuals at risk; where the data is classed as 'special category data'; and criminal conviction and offence data. Contact us for more guidance if you think any of these apply to your group/organisation.*

4. How is the CAG Project supporting groups?

- Bespoke **webinar(s)** with a GDPR advisor to support CAG groups and address specific queries
- A bespoke **face to face workshop (if required & Oxford only)** with a GDPR advisor to support CAG groups and address specific queries
- **On the phone/email advice & support** via Kerry (with support from a GDPR advisor)
- Provision of a **checklist** of key documentation required

- **Signposting** to key available templates via our CAG web platform (for privacy notices, data protection policies, retention schedules, information security policy, data breach reporting procedures, etc.)
- Production of a **GDPR CAG guide** - building upon this overview and using specific case studies from the webinars/face to face session as an on-going reference.

Please don't hesitate to get in touch for more assistance:
Kerry Lock (Community Engagement Manager): kerry.lock@resourcefutures.co.uk / 07793647190

5. Further reading

- IT Governance - list of free GDPR resources online
- NCVO - Data Protection Guidance online
- Information Commissioners Office - Guide to GDPR download
- Charity Finance Group - General Data Protection Regulation: A Guide for Charities download
- Information Commissioners Office - Accountability and Governance Documentation download
- Information Commissioners Office – Documenting Processing Activities Guide download