GDPR GUIDANCE FOR RESIDENTS ASSOCIATIONS

CONTENTS:

GDPR

- The General Data Protection Regulation (GDPR) is a legal framework that sets guidelines for the collection and processing of personal information of individuals within the European Union replacing the Data Protection Act of 1998.
- Residents Associations who collect, process and hold personal data should be mindful of the new legal requirements and obligations which came in to affect in May 2018.
- GDPR gives individuals a greater level of control over how their data is managed and requires organisations which collect, process and hold personal data to explain and justify , why they are collecting the data, where it is stored, and with whom they will share the personal data with . The shift is to greater transparency and accountability.
- Overall the greater purpose is for organisations to be mindful of data protection and to embed privacy by design and awareness within their organisation through staff training. There are greater financial consequences for breach and non compliance - Penalties up to 4% of turnover or 20 million Euros (€20m).

KEY PRINCIPLES

The GDPR sets out seven key principles These principles should lie at the heart of your approach to processing personal data:

- Lawfulness, fairness and transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality (security)
- Accountability

WHAT PERSONAL DATA DOES YOUR GROUP COLLECT, STORE AND USE?

Personal data is information about a living person which is identifiable as being about them. This includes basic things like names and addresses, and also more complex or sensitive information such as ethnicity, criminal record, employment history, sexual orientation, and health information -which includes special category data (see below)

KEY TERMS UNDER GDPR

- ***Person Data - Any*** information relating to an identified or identifiable natural person ('data subject');

- ***Data Subject*** - any living person - an identifiable natural person is one who can be identified, ***directly or indirectly***, by reference to an ***identifier*** such as a name, an identification number, location data, an online identifier or ***by one or***

more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person

- ***Special Category Data*** - this is data or information about a person that describes their racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data and biometric data, data concerning health or a person's sex life or sexual orientation.

- ***Processing*** - means an operations or setoff operations which is used on the personal data. This can include collection, recording, storing, retrieval, alteration, disclosure, deletion or destruction.

Personal data can be held electronically or on paper. Photographic and film images are also considered to be personal data if people are identifiable in them.

Think about what personal data your group holds about people. This is likely to include names and contact details, but may also include other more sensitive information.

It is important to understand whether personal data belongs to a group or to you personally. For very small groups this can be a bit confusing. A good rule of thumb is to consider whether you met a person, or gained their information, in the course of your involvement with the group. If you know someone because of your role in a group, and have only gained the information through the course of running group activities, the data you hold about that person belongs to the group and not to you personally. You should not use it for personal reasons without explicit consent.

WHAT IS YOUR GROUP'S PURPOSE FOR COLLECTING, STORING AND USING PERSONAL DATA?

Organisations should only collect, store or use personal data if they have a clear purpose for doing so. This means that your group must know *why* you have people's personal data. If there is no longer a purpose for holding someone's data, it should no longer be kept.

LAWFUL BASES FOR COLLECTING, STORING AND USING PERSONAL DATA

To comply with data protection law , your group should only collect, keep or use personal data if you are doing so to fulfil a purpose which fits into one of the following lawful bases:

- To serve your group's "legitimate interests", or
- Because you have explicit consent from the person whose data it is, or
- To fulfil a contract with the person whose data it is, or
- To meet a legal obligation, or
- To protect someone's life, or
- To perform a public task.

Any time you collect, store or use people's personal data, you should be clear which of these reasons you have for doing so. In all likeliness, your RA will be collecting

and storing data: **to serve your group's "legitimate interests",** or **Because you have explicit consent from the person whose data it is.**

Legitimate interests

Your group can use personal data if it is in your group's legitimate interests. This means that you can use data in ways that are necessary in order to run your group. You should only use the minimum amount of data that you need, and you should give people the option of having their data removed from your records.

When you use people's data to pursue your group's legitimate interests, this must be balanced against their rights and freedoms. Here are some things to check before using people's data.

1) Before contacting somebody, consider whether they would reasonably expect you to be contacting them. For example, do you have their contact details because they are involved in your group's activities? If so, you can probably safely assume they would expect to be contacted by your group. In contrast, if you have their details because they have been passed on by a third-party, and the person has never had anything to do with you before, they might not expect to be contacted by your group.
2) Can you identify a particular purpose for using the data, which is clearly in your group's interests? If so, is use of the data necessary to achieve the purpose? For example, you might need to contact people who regularly attend your group's sessions in order to tell them about a change of venue, so that people can keep attending. This is clearly in the interest of your group, and you need to use contact details in order to achieve it.

Consent

Your group can use an individual's personal data if you have their explicit recorded consent to do so. Consent is only valid for the particular purpose it was gained for (e.g. if you gain consent to use someone's address to send them a newsletter, it does not mean you have consent to use this information for other purposes). People must be well-informed in order to give consent. You must explain beforehand why you need the data and what you will use it for, and that the person can ask for it to be deleted in future.

To use consent as a basis for using data, you must keep a clear record of who has given you consent and for what. Consent must be positively given. You cannot assume consent just because somebody has not said anything. When using tick boxes, people must be required to actually tick a box to give consent. Pre-ticked boxes do not count.

You can get verbal consent, but you should still explain specifically what the data will be used for and that they can ask for it to be deleted in future. You still need to keep a written record so that you know who has given you consent, and for what. Consent for children under 13 must be given by a parent or guardian.

DATA SUBJECTS RIGHTS

Individuals have specific rights which they can exercise in relation to personal data. Therefore, more transparency and accountability is required over how their data is used and processed.

1. **The right to be informed** – the right to know what the RA's are collecting and using, the purpose of collection and how long the RA will keep the information for and with whom they will share it. This is usually be in a privacy notice given to the individual (see below).

2. **The right of access** – the right to request access to their own personal data generally referred to as a Subject Access Request (SAR). Requests can be made verbally or in writing. A request must be complied with within 30 calendar days and generally provided free of charge.

3. **The right to erase** – the right to be forgotten and have personal data deleted.

4. **The right to rectification** – the right to have inaccurate data corrected.

5. **The right to restrict processing** – In certain circumstances individuals can request data to be restricted or suppressed i.e. the RA will not be permitted to use but can continue to hold it.

6. **The right to data portability** – the right to obtain and reuse the data the RA holds for their own purposes or use by a different service provider.

7. **The right to object** – the absolute right to stop their data being used for direct marketing. The right to object applies unless the RA can demonstrate a very good reason for continuing to process the personal data.

8. **Right to restrict automated decision making and profiling -**
   Automated decision making - a decision made without any human involvement i.e. re an algorithm (set of rules built into a system) which is used to make a decision.

   Profiling - automated processing of personal data to evaluate certain things about an individual i.e. performance at work, financial status, health, interests.

PRIVACY NOTICES: TELLING PEOPLE ABOUT THE DATA YOU ARE USING

This is the right for individuals to be informed about the data to be collected and processed. When your group collects personal data, or uses someone's data to contact them, it should be made clear to them why you have their data, what you are using it for, and what their rights are. This means you should provide them with a privacy notice.

A privacy notice is a piece of written information which tells people why you need or have their data. It should include:

- the name of your group;
- what the data will be used for;
- which legal basis you have for using the data;
- how long the data will be kept;
- whether the data will be shared with a third-party, including if it will be stored on a third-party website (e.g. in Google Drive or DropBox);
- that individuals can ask to have their data removed at any time, and contact details to use to do this.

If you are collecting and using data on the basis of explicit consent, you should provide a privacy notice when you request the consent. For example:

Named RA needs your name and email address in order to send you information about group activities. Please tick the boxes below to give consent for us to use your details.

☐ *I consent for Named RA to send me details of their events and meetings.*

Your details will be stored securely online in our Google Drive folder/Excel spreadsheet/Dropbox , and will be removed within one month if you end your membership of Named RA. You can withdraw your consent for us to use your information, or ask us to amend or delete your details, by emailing secretary@namedra.com.

If you are using data without explicit consent (because you have a different lawful basis for using it, such as legitimate interest), you should provide a privacy notice either when you collect the data or, at the latest, the first time you contact someone. For example:

Named RA has your contact details because you have attended one of our open forums in the last 12 months. We only use these details to send you information about future open forums. We do this because it is in the legitimate interest of our group to publicise our sessions to regular attendees. Your details are stored securely by our committee and will be deleted if you do not attend a session for 12 months. You can ask us to amend or delete your details at any time by emailing secretary@namedra.com

It' a good idea to review policy every two years. Look at this sample Privacy Policy from Ruislip Residents Association:
http://www.ruislipresidents.org.uk/about-us/privacy-policy-gdpr/

STORING PERSONAL DATA

Personal data must be stored securely. If your group keeps personal data in computers, your computers should be password protected. You should have up-to-date software to protect them from malware and viruses. If you store information on paper, it should be filed securely.

If your group stores personal data on the internet (e.g. attached to emails, in Google Drive, in Dropbox, etc) you should check that the companies storing the data comply with GDPR regulations and that the data is not transferred outside of the EU. Most big companies have privacy policies which confirm they comply. However, email marketing company Mailchimp currently stores data outside of the EU, so it is simpler to choose a different mailing list provider, such as Freshmail or Send in Blue, which also offer free services to organisations with small mailing lists.

It is important that you know who is storing data on behalf of your group, and that everyone understands the need to keep it secure and up-to-date. It's best to agree a system, and to minimise the number of places you are storing data. Otherwise you can easily lose track of what you have. A simple way to do this is to have one central list of contacts, either on paper, on a computer, or securely stored online, which everyone refers to. It's best to nominate one person to look after the list. In many groups this would be the secretary's job.

For example, your group's secretary might keep an up-to-date copy of all your members' contact details on their computer. Another committee member is organising an event, and needs to contact all the members to tell them about it. The secretary sends them the list by email. The committee member downloads the list into their own personal computer. (The computer should be password protected and have up-to-date anti-spyware software.) Once the committee member has done the task, they should delete the copy from their computer and emails, so that the group does not lose track of who is storing what information.

Avoid keeping data for the group on an ad-hoc basis in personal phones and address books. If you write down someone's details when you are out and about, add them to the central list and then delete them from your private phone or address book.

Although it is useful to nominate one person to look after personal data for your group, it is very important that you do not refer to this person as a "Data Protection Officer". This is because the term "Data Protection Officer" has specific legal meaning, and organisations that have a Data Protection Officer have additional obligations which small groups do not need to worry about.

KEEPING IN TOUCH WITH YOUR COMMITTEE

To organise together as a group, the core people involved in making things happen need to be able to contact one another.

Your RA committee, generally need to have one another's contact details so that you can all work together well. This is different from the contact details of your wider membership, mailing list or other external contacts.

Even though you all need to be in touch, it is still important to work together to protect everyone's privacy and ensure people's details are not used in ways they wouldn't reasonably expect. It is useful to make a clear agreement among your

committee about how you will look after one another's contact details. This could include:

- That you will not pass them onto other people without specific consent
- That you will not use them for anything other than group business without specific consent
- That if someone leaves the committee, everyone will delete their details, and vice versa, unless specific consent is given to keep them
- That you will not put other people's contact details on group publicity without specific consent.

If your committee members do not wish to share their personal contact details with each other, you could consider setting up another way for everyone to communicate. One way of doing this is to allocate each committee member with an official email address. One person should still hold everyone's personal contact details securely though, because your committee is responsible for the running of the RA so it needs to be contactable.

SHARING PERSONAL DATA WITH OTHERS

You should request explicit consent if you wish to share personal data with third-parties, (unless you need to do so to fulfil a contract, comply with the law, protect someone's life or fulfil a public task). Third-parties might be other organisations, but they might also be members of your own group. Each individual in a group is separate from the group itself, and data should not be shared with group members to use in a personal capacity without explicit consent.

Personal email addresses are personal data. Therefore, RAs should take care not to accidentally share such personal data when sending group emails or using distribution lists, including with other members of the group. For example, if you send an email to everyone on your mailing list, do not simply type all the email addresses into the "To" field. By doing this you are actually sharing all the email addresses with everyone on the list. Use the "Bcc" field instead. This hides everyone's email addresses.

This is especially important if your group members all share a particular personal characteristic or are being contacted around particular issue (e.g. ASB). Accidentally sharing the names or contact details of your group members could mean revealing that they have a particular personal characteristic or a dealing with an sensitive issue, which they may not wish to be public knowledge and which could affect their lives in significant ways.

REMOVING PERSONAL DATA

Once you have finished using personal data for the purpose it was collected for, it should be deleted. It should not be kept indefinitely or just in case you want to use it again, but don't know what for. When you delete data, make sure it cannot be accessed by someone else.

Individual's have the right to object to their data been held or for it to be erased. You should also delete people's data when they ask you to, unless you need to keep it because of a specific legal obligation. If you send out emails to a list of contacts, you must put information at the end of every email explaining how to unsubscribe from the list. If you use an email newsletter provider this will happen automatically. If you send ordinary emails to a list of people, create an email signature which tells people who they should contact to be removed from the list.

PEOPLE'S RIGHT TO THEIR OWN DATA

Individuals have a right to be given a copy of their data, and information about how it is being used. This is usually referred to as a Subject Access Request. This must be provided within one month of a request. They also have a right to have their information amended or deleted within one month of a request (unless you need to keep it for legal reasons). To help you do this, make sure you know where data is being stored, and by who.

DATA BREACHES

There are lots of ways that a community group might have a "data breach". These include, for example:

- Theft of a laptop or phone with contact details stored in it
- Accidentally sending an email with everyone's email addresses visible
- Sending personal information to the wrong recipient by mistake
- Losing a paper sign-up sheet on which people have written their names and addresses

The most important thing is to recognise if something has gone wrong, so that you can take steps to reduce the impact it will have, and to avoid it happening again in future. Try to keep data protection in mind, so that you notice if there has been a possible data breach.

Some examples of data being breached:

- Low: Email to all members without BCC informing them of the next meeting.
- Medium: Wrong person internal to the organisation is emailed about a personal matter or issue involving named individuals
- High: A sign up sheet with vulnerable adults and their addresses is lost or a wrong person external to the organisation is emailed about a personal/sensitive matter or issue involving named individuals

If you have a data breach, the first thing to do is try to get the data back. For example, if you have accidentally emailed someone's details to the wrong person, contact that person and ask them to delete the information.

The next step depends on whether the data breach is likely to have a significant impact on someone's life. If it is not likely to have an impact, you should still record that it has happened and take steps to avoid it happening again.

In some cases, the breach isn't likely to risk anybody's freedoms or rights, and therefore does not need to be reported to anybody. Instead, the group records what happened in the minutes of the meeting at which it was discussed, and puts in place a system to avoid it in future

Some data breaches are more serious though, and need to be reported to the person whose data is affected and to the Information Commissioner's Office (ICO). Some breaches could potentially affect the individuals involved in significant ways, and should be reported to them so that they can take steps to protect themselves if they want to (e.g. by changing their phone number). It should also be reported to the ICO.

Remember that it is much better for the ICO to hear about your data breach from you than from someone else. This will show them that you are a responsible organisation that takes data protection seriously, which makes it less likely they will have significant concerns about you or issue a penalty fine. Remember that large fines are not intended for small groups, but that data protection is for everyone.

Info from ICO website and Resource Centre:
https://www.resourcecentre.org.uk/information/data-protection-for-community-groups/#legitimate

FURTHER READING AND CASE STUDIES

- ICO guide https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/
- ICO self assessment: https://ico.org.uk/for-organisations/resources-and-support/data-protection-self-assessment/
- Lee Residents Association guide to GDPR: https://www.leeresidents.org.uk/WebDataProtection170318.pdf
- GDPR and local societies: http://www.balh.org.uk/news/gdpr-and-local-societies-general-advice-1
- NHG Privacy Policy Privacy policy | Notting Hill Genesis (nhg.org.uk)