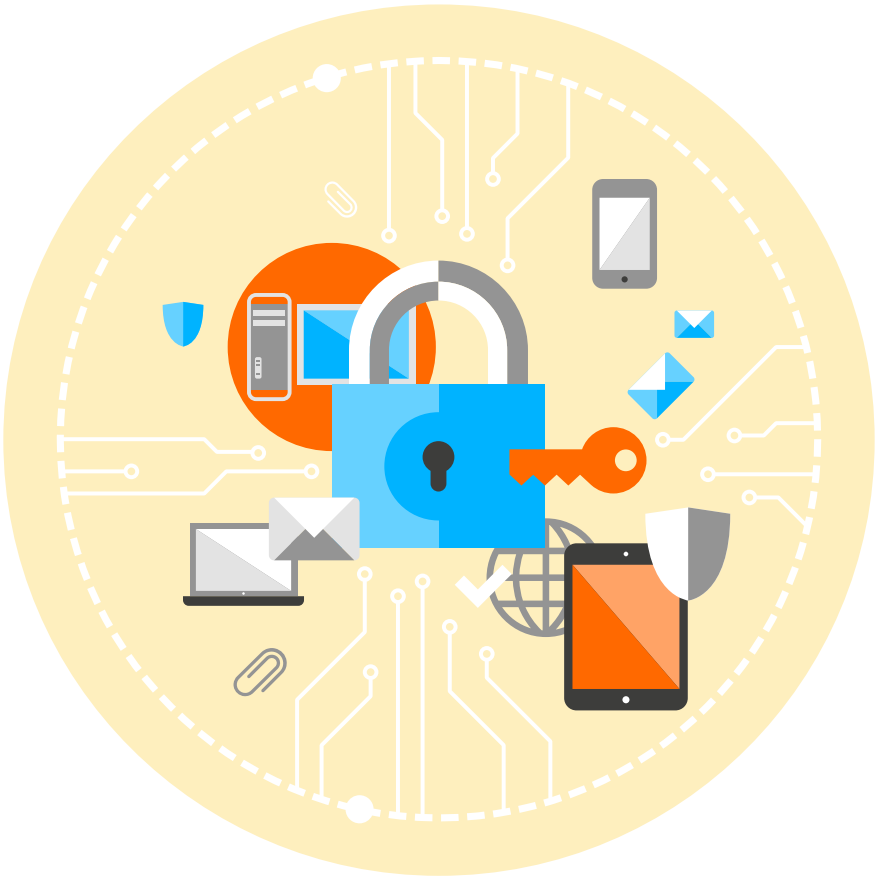
Data Protection

Guidance for community rail partnerships and groups on compliance



ACoRP
New life for local lines

Data protection: guidance for community rail partnerships and groups on compliance

Data protection is all about making sure that people's personal information, such as name, contact details, personal characteristics (such as gender, ethnicity, religion, sexuality, age, health conditions), are secure and are not used for a purpose that the person concerned hasn't agreed to. Although data protection regulations have existed for some time, on 25 May 2018 the new General Data Protection Regulations (GDPR) come in to force, which sees an update to and extension of the rules.

For some organisations, especially those doing a lot of direct marketing, or processing more sensitive data such as health, protected characteristics or political affiliations, GDPR will have a huge impact. For people involved in community rail who tend to process only limited amounts of personal data, the rules won't be a huge change. However, it is important to make sure you are abiding by the rules and are following good practice in the way that you handle people's personal data. With community rail partnerships (CRPs) and other groups that are hosted by, or with employees based within another organisation, such as a local authority, university or charity, the host organisation may take responsibility for data protection compliance. However, it is important to check if that is the case. Otherwise it is the responsibility of the CRP itself to make sure it complies.

The legislation isn't intended to stop you doing your work, just to do it in a way that protects the rights of individuals to choose how their information is used. At the same time, it isn't something that can just be ignored. This legislation brings an increase in penalties for a data breach, including fines of up to 4% of your annual turnover. Although the Information Commissioner's Office (ICO) is likely to prioritise bigger organisations to start with, small organisations are already being fined under the current rules – see the examples here: **https://ico.org.uk/action-weve-taken/enforcement/**

Key principles

There are a few key principles of the current and new legislation which requires all personal data to be:

a) processed lawfully, fairly and in a transparent manner in relation to individuals

b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes

c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed

d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay

e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and

f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

A useful and easily accessible guide to the full text of the GDPR regulations can be found at **https://gdpr-info.eu/**

Main things you should do now

The ICO, which enforces rules on data protection, has produced some useful checklists and factsheets on preparing yourself for GDPR. However, they are still working on much of their sector specific guidance, and you should keep an eye on their website for potential changes until the regulations come into effect. Of particular use is their **12 steps to prepare for GDPR [PDF]** and **Getting ready for the GDPR checklist**. They also have a phone advice service for small organisations and charities on 0303 123 1113 (choose option 4).

Drawing on this, there are a few key things you should be doing now, set out below.

Awareness

Make sure everyone in your organisation – employees and volunteers – who use or process information understands there are new rules and the implications. This is useful to undertake alongside a data audit (see below) as colleagues may flag up data that others weren't aware of.

It is useful to make sure one person in your organisation is nominated as your 'Data Controller', with ongoing responsibility for ensuring everyone is aware of data protection rules and how to comply. That doesn't mean they carry the can if something goes wrong, (the regulations state that anyone who handles data must be responsible for complying), but it does mean that things aren't missed.

Undertake a data audit

This is simply compiling a list of everywhere you keep and/or use personal data – names, addresses, other contact details, etc. It includes membership lists, mailing lists for events, websites, email address books, laptops and portable storage and mailing services such as Mailchimp. Personal data is not just where someone is identified by name, but also anywhere there is sufficient information that can be used to identify an individual. As well as recording what data you have you should record what you use it for, how (or whether) it is ensured it is up to date, and where it came from. This data audit can then be used to work out what changes you need to make in processes or what data needs to be edited or destroyed. An example of the types of data or locations that may need to be recorded in your data audit is available at the end of this guidance.

Wording of sign-ups / opt-ins

In future people will need to opt-in to receiving your communications, you cannot just give the option of opting out. This is already good practice, but from 25 May it will be compulsory and so you need to make sure that anywhere where you ask for someone's contact details has an opt-in tick box. They must give consent 'freely' which means you cannot have any pre-filled tick boxes or hide the consent away in your terms and conditions. It also won't be possible to sign someone up to something on their behalf. For example, ACoRP used to ask members for details of all their staff/volunteers who should be added to our mailing list, but now individuals must add themselves. On an email list you should also have a double opt-in, which means that a new subscriber receives an email which they must respond to confirming that they wished to opt-in, before they start receiving your emails. Sign-up forms on email services can be set to do this automatically.

A key part of GDPR is making it clear what people are opting in to. This means you need to be more specific than just saying you will use their data to communicate with them: you should tell them what they can expect to get and a rough frequency. The best approach is to give people the ability to opt-in to different communication channels, e.g. email, post, text message, etc. You should also give them the option of choosing whether to sign-up for general news, information on events and so on, depending on your activities.

There will be occasions where this approach of asking consent is not appropriate, although this will be the exception rather than the rule. This applies if using their personal data is the only way you can fulfil an essential function, such as if someone joins a station adoption group you need to use their personal data in order to make them a member and to ask them to renew at a later date. You still need to inform them of what you will do with their data but you shouldn't ask for their permission when it isn't possible to make them a member if they choose to opt-out. However, the same person should still be asked if they want to receive marketing emails as this is not an essential part of them being a member.

You must also have a privacy notice on your website and any printed materials where people can sign up to receive communications from you. An example of an online privacy statement is here on the ACoRP website. On written materials you should use wording similar to this:

> **Data Privacy:** To operate effectively and fulfil legal obligations, **<INSERT CRP NAME>** needs to collect, maintain and use certain personal information about current, past and prospective members and stakeholders with whom it has dealings. All such personal information, whether held on computer, paper or other media, will be obtained, handled, processed, stored and transported lawfully and correctly, in accordance with the principles and safeguards contained in the Data Protection Act 1998 and GDPR Regulations (Article 5). We will use your personal data solely for your involvement in our activities and will not share it with any third party. Our Data Privacy Policy can be found at **<INSERT WEBSITE ADDRESS>**. I understand by ticking the box I am consenting to my details being stored and receiving relevant correspondence.
>
> I would also like to receive regular email updates to the address provided: **TICK HERE [ ]**. You can opt out again at any time by following the unsubscribe link at the bottom of the email.

Keeping data up to date

Any personal data that you hold must be kept up to date, and you must update or delete information on request. The best way to work out if you are keeping all of your data up to date is to ask yourself this question: if someone asked for all their personal data to be deleted, would you be able to say with certainty that you would know where to find it all? If the answer is no, you need to make changes so that you could find everything and make sure it is updated, with no data being missed. For that reason, organisations should ideally have one set of contacts rather than each person keeping copies on separate computers or different places. Consent also doesn't last forever, and so you should routinely – at least every year or two – check that people are still happy to hear from you.

Generally, the most likely request you will get is when someone asks if they can opt-out of mailing lists. The process for opting out must be as easy as the process the person went through when they signed up. All marketing emails must also an 'unsubscribe' link/button, usually in the footer of the email. This is included automatically in Mailchimp emails and most other suppliers of email services.

Sharing data for processing

The only legitimate way you can share data with someone from outside your organisation is if they are 'processing' it on your behalf. Processing is a specific term which means they are using the data to carry out a legitimate function on your behalf with your permission e.g. addressing a posted mailing. Before you can do this it is important to make sure that you have undertaken due diligence and that anyone who is processing your data understands data protection legislation and are able to confirm that they will comply with the rules. You must also sign a contract with them that confirms they abide by the law. You can find more about these contracts on the **ICO website here [PDF]**. See below for more information on sharing data.

Other good practice

Although the GPDR is changing how data can be used, it's always been important to look after any information you have. Here are some other tips to keep you secure and compliant. You can find a useful checklist on the **ICO website here [PDF]**.

Sending out emails

If you send out bulk emails to members, partners or a mailing list, then using an email service such as Mailchimp is best. This means excellent data security is built in automatically, as well as emails looking more professional. They allow easy opt-outs and they allow you to split mailing lists into different groups.

Never ever send out emails to a large group of people using the 'to' or 'cc' function in your email system. Always 'bcc' so they cannot see each other's addresses.

Passwords

Make sure that you password-protect any files or databases you use that contain people's personal details, especially if these are stored in a location that is accessible to other people who should not or do not need to have access. Also ensure that your computer locks if you leave your desk so no one can use your computer to access confidential information. These passwords (and log-ins to online tools such as Twitter and even alarm codes for your offices) should be changed periodically, especially when people leave the organisation. This is even more important if information is stored somewhere portable, such as on a laptop, data stick or a portable hard drive, or you are emailing data to someone else. This is easy to do in Word and Excel, just go to File > Info > Protect Workbook / Protect Document > Encrypt with password. If you do have to share a password with someone then do not send it to them using the same method that you sent the data.

Paper records

Any paperwork that you keep that contains personal details should be kept in a locked drawer or filing cabinet, and it should be destroyed when it is no longer needed. When you dispose of paperwork that contains people's personal details they should be shredded not just dumped in a bin. Also make sure you don't keep anything containing people's personal details or confidential information on your desk or in a place where other people can see it.

Sharing data

If someone has given you their details so they can be kept up-to-date on your activities, then you must not use this information for any other purpose. This includes passing details of your subscribers, partners or volunteers to other organisations, including ACoRP, without their express consent (ACoRP will now be asking people to confirm what details they are happy for us to give out to anyone who calls) or if you produce a directory of contacts. However, there is a key difference here between 'public' data and personal data. If an email address or phone number, for example, has been put in to the public domain with the intention of people contacting them for a stated purpose, e.g. a journalist wanting to be sent press releases or a train operator giving contact details for their community rail staff, then it is okay to keep, use and share. This is why it is important to use a different email addresses for work or personal use. If you currently use the same email address for work as for your own personal use then now is the time to change it and you shouldn't send personal data relating to your work or a committee you sit on to a personal email address.

Subject access requests

Any individual can submit a 'subject access request', which requires you to give them a copy of all information you hold on them, whether on lists, in files or in emails, within a month of them requesting it (from 25 May this must be done for free). For this reason, it's important you do not write anything that you would not be happy with the individual seeing. If someone submits a request, you need to make sure that you are certain it is that individual asking for the information (never accept requests over the phone) and that you do not share with them anything not related to them or that mentions another individual. There isn't any specific format for a request, just make sure you have their request in writing.

Frequently asked questions

Does this only apply to electronic data?

No, it applies to everywhere you keep someone's personal details, whether it is electronically or on paper, as long as it is in a filing system of some sort, can identify a specific person, and can be retrieved when necessary.

I don't know where my data came from originally or what they agreed to. Can I still use it?

This depends on the nature of the information and what someone was told when they first subscribed. If you simply added details to your mailing list without their permission, or you don't know where the information came from, then you will need to delete their details. However, if the data was given to you freely and you have had regular contact with them since, then you MAY still be able to use the data, but you will need to 're-permission' them (**a good article on this is available here**). This means getting in touch to ask if you can continue to email or write to them. If they fail to respond, then you will need to delete their data.

Don't assume that it is okay to add someone to a mailing list just because you know them personally. Make sure you keep the evidence of when, how and to what communication someone agreed to in case there is a query later. Many online databases or email systems store this automatically.

I've heard that Dropbox, Mailchimp and other US based companies can't be used under the new rules.

The US has rules on data protection that aren't compatible with UK (and EU) legislation. This is why many US based companies, such as Amazon, store data for their European customers within the EU, and other companies such as Mailchimp or Dropbox will be ensuring they comply in time for the new legislation. It's worth checking that any data you store online, including cloud-based programs and websites, are hosted on servers within the European Economic Area or Canada (who have the same rules that we do).

The GDPR is an European Union directive, will it still apply when we leave the EU?

Yes. The rules come in to force before the date we are set to leave the EU. Government has also said that all existing EU-based laws will be brought into UK legislation automatically, and we need to abide by them if we wish to share data with EU companies after leaving.

Do these rules apply to personal or media contacts that I keep in Outlook, Gmail or Excel?

Yes, but if the information was given to you personally for a specific purpose then you can use it for that purpose. For example, if someone gave you their details for work reasons such as a journalist or an industry colleague then that is allowed but do make sure you update your contacts regularly. This is why it is best to store these details in one place within an organisation, so everyone is updated if it isn't just you who is contact with them.

Do I need to register with the ICO as a data controller?

At the moment, most organisations have to pay a fee and register with the ICO as a data controller, although many smaller organisations and charities are exempt. The government has announced a new system for working out who needs to pay and how much. Details are **available here** as a PDF.

What should I do if I lose any personal data?

Any loss of data or misuse of data within your organisation should be reported to whoever in your organisation is responsible for data protection. This should then be logged and any appropriate action taken to ensure the situation is rectified and not repeated. If any personal data reaches the public domain which could potentially compromise someone's right to privacy, or if it contains any of the 'special categories' of data these will need to be reported to the ICO directly within 72 hours. More information is **available here**.

Examples of personal data

This list gives you examples of the places where you may store personal data that you need to consider as part of your data audit. This is not intended to be an exhaustive list as every organisation is different, and so do think if there are other things that you need to include:

- Contact lists / mailing lists / membership databases
- Email systems e.g. Outlook, Mailchimp, where used to store mailing lists
- HR files and documents used for recruitment e.g. CVs
- Codes of conduct / volunteer sign-up forms
- Files stored on data sticks, external hard drives and server back-ups
- Mobile phones
- Visitor books or event booking forms (both online and paper)
- Bank account details and medical records