The European General Data Protection Regulation Factsheet

The European General Data Protection Regulation (GDPR) comes into effect across the EU on 25 May 2018. It replaces existing EU and UK data protection law and will continue in force even after the UK leaves the EU.
If you do not comply your organisation could be fined, so read on to find out more.

Disclaimer

CCVS are not lawyers or legal advisors. This information is for information and should not be taken as legal advice. We have taken all care to ensure that what we have written is correct but cannot be held responsible for any errors. If you are unsure you must seek appropriate, qualified advice. If you see something that you believe is wrong then please let us know so that we can correct or clarify it.

Introduction

This legislation will affect all organisations that hold personal data even very small ones. BUT don't worry it does not have to be an onerous problem and a few simple steps can help you ensure you are complying with the law. GDPR is concerned with how organisations obtain, store and use personal information.

What information does the GDPR apply to?

We don't use computers so we are OK

The Information Commissioner's Office (ICO) states that "The GDPR applies to both automated personal data and to manual filing systems where personal data are accessible according to specific criteria."

The legislation is 'technology neutral'. It is not just about computers and emails, it also covers files held on paper, the contents of filing cabinets, contact lists on phones, telephone calls and direct mail!

Personal data

Anything which enables an individual to be identified is 'personal data'. However work addresses are just that and, although employees are entitled to some privacy, for GDPR purposes they are not 'personal' emails. B2B is still ok but anything regarding private emails will need explicit consent.

So for most organisations this would include information held in these areas, this is not an exhaustive list but is for information:

- HR/personnel/payroll.
    - Basic employee data – name, address, age, job title, etc.
    - Basic volunteer data – name, address, age, role, etc.
    - Bank account details for payroll and expenses processing.
    - Tax details – benefits, family, total income, etc.
    - Appraisals.
    - Disciplinary records.
    - CVs – successful and unsuccessful candidates.
    - Medical details.
    - Criminal records.
    - Trade union participation.
    - Driving licence and passport numbers
    - Car insurance & MOT details
    - Vehicle registration number

- Marketing, project delivery and fundraising.
    - Donor or member data – name, address, age, etc.
    - Email address and IP address.
    - 'Profiling' information.
    - Bank account details.
    - Attendance history.
    - Payment history.
    - Delivery records.

- Other places you may not think of!
    - Accident record book.
    - Reception, post room, sign in.
    - Data shared with third parties (e.g. delivery contractor).
    - 'Personal' address books, customer data, etc.
    - Email systems.

Other considerations

- There are specific additional requirements around collecting, storing and using data about children.
- Seeking to identify website visitors without consent is probably unlawful.
- Gathering data from social media may be unlawful.
- If you are using Google Analytics, be aware that the Terms of Service require you to be GDPR compliant.

To comply with GDPR organisations must:

- Collect only the data they need.
- Keep data secure.
- Delete data when they no longer need it.
- Have a written policy in place, ensure all relevant employees know about it, and ensure there is evidence that it is implemented.

For most organisations there are three 'bases' on which data can be collected, stored and used under GDPR:

- To fulfil legal obligations – for example, recording details of accidents at work.
- To permit the organisation to pursue its legitimate interests. This will permit collection and use of data for HR purposes, for example. It may cover collection and use of client details for marketing purposes or project purposes if certain conditions are met.
- With the informed consent of people about whom data is collected, stored and used.

The above list is not exhaustive, but for most organisations the three categories above are the only ones likely to be lawful.

Where an organisation is relying on 'legitimate interests' as the basis for collecting and storing data it must:

- Carry out and document a 'legitimate interest assessment'. In effect, it must be able to demonstrate that its legitimate interests outweigh its customers' rights to privacy.

- Collect only the data it needs.
- Tell people whose data it is processing that it is doing so on the basis of a legitimate interest.
- Give people an easy way to opt out – and then ensure that the opt-out is acted upon.
- Have procedures in place to record opt-outs.

Where an organisation is relying on 'informed consent' as the basis for collecting and storing data it must:

- Collect only the data it needs.
- Tell people why it is collecting data, secure real 'informed consent' (which means people must positively agree to their data being collected – not simply fail to object) and allow them to opt out at any stage.
- Use data only for the purposes for which people were told the data would be used.
- Secure repeat 'informed consent' at 'reasonable intervals' – so it cannot keep people on a database indefinitely without asking them to confirm their consent.
- Have procedures in place to handle and record when the consent was given, exact details of what the person is consenting to receive from your organisation, exact details of what personal details you will be holding for each person: i.e. email address, postal address, telephone/mobile numbers, bank details etc. and any withdrawal of consent requests.

There will often be a 'fine line' in between when an organisation is able to rely on 'legitimate interests' and when it must seek informed consent.

What do you need to do?

If you store personal data you may need to register with the Information Commissioners Office (unless you are exempt. This applies to numerous not-for-profit organisations). This link will allow you to check.

Regardless of the need to register, you should appoint someone as the organisations 'data controller' to take responsibility for all GDPR-related activity. This could be a staff member or a trustee.

He or she should conduct an audit to see what data is collected, stored and 'processed' and develop an action plan to ensure the organisation is fully compliant with GDPR by May 2018.

He or she may require external expert assistance, particularly in drawing up and implementing a 'legitimate interest test'. This will be vital to determine whether or not you can rely on this as a basis for handling data or must move to the far more onerous requirements of 'informed consent'.

RESOURCES

There are a growing number of people providing support; some are very expensive but others are free.

The first place to start is the ICO website as they are the body tasked with implementing and enforcing the rules

- Webpage guidance by ICO on GDPR https://ico.org.uk/for-organisations/data-protection-reform/
- They have a section aimed at charities with some good links
- https://ico.org.uk/for-organisations/charity/
- They also have a useful summary page on steps organisations need to take now https://ico.org.uk/media/1624219/preparing-for-the-gdpr-12-steps.pdf

The Institute of Fundraising have produced some useful guidance https://www.institute-of-fundraising.org.uk/guidance/research/get-ready-for-gdpr/

There is a free guide to fundraising and Data Protection developed by an ex information commissioner who has been critical of some charities but has turned that into a guide on how to be more compliant. http://2040training.co.uk/downloads/

There are some interesting news articles and reports from

> NFP Synergy, about how the public might view the changes https://nfpsynergy.net/free-report/gdpr-change-charity-donors-want
>
> From Charity Digital news on what GDPR might mean for you https://www.charitydigitalnews.co.uk/2017/09/22/gdpr-what-does-it-mean-for-your-charity/ and about how and why you might retain data https://www.charitydigitalnews.co.uk/2017/09/28/gdpr-an-explanation-of-data-retention-and-why-it-is-important-for-charities/

There is information on the Data Protection Network https://www.dpnetwork.org.uk/