Newcastle Council for Voluntary Service

General Data Protection Regulation (GDPR)

FAQs

What is the GDPR?

The EU's General Data Protection Regulation (GDPR) aims to bring data protection legislation into line with new, previously unforeseen ways that data is now used. The UK currently relies on the Data Protection Act 1998, but this will be superseded by the new legislation. GDPR introduces tougher fines for non-compliance and breaches, and gives more people say over what organisations can do with their data.

Why was the GDPR drafted?

The drivers behind GDPR are twofold. Firstly, the EU wants to give people more control over how their personal data is used. The current legislation was enacted before wide use of the internet and platforms like Facebook discovered the value of using their users' personal data. Secondly, the EU wants to give organisation a simpler, clearer legal environment in which to operate, making data protection law identical throughout the single market.

When will the GDPR apply?

The GDPR will apply in all EU member states from 25 May 2018.

Who does the GDPR apply to?

'Controllers' and 'processors' of data need to abide by the GDPR. A data controller states how and why personal data is processed, while a processor is the party doing the actual processing of the data. The controller can be any organisation, from a private company, to a government department or a charity. A processor could be an IT firm doing the actual data processing.

How do I obtain consent under the GDPR?

Consent is one possible lawful basis for processing but is not the only one. Consent must be an active, affirmative action by an individual user, rather than the passive acceptance under some current models that allow for pre-ticked boxes or opt-outs.

Controllers must keep a record of how and when an individual gave consent, and that individual may withdraw their consent whenever they want.

When can people access the data an organisation stores on them?

People have the right to access any information an organisation holds on them,

and the right to know why that data is being processed, how long it's stored for, and who gets to see it.

People can ask for access at "reasonable intervals", and controllers must generally respond within one month. GDPR requires that controllers and processors must be transparent about how they collect data, what they do with it, and how they process it; they must be clear in explaining these things to people.

What's the 'right to be forgotten'?

Individuals also have the right to request that their data is deleted if it's no longer necessary to the purpose for which it was collected. This is known as the 'right to be forgotten'. Under this rule, they can also request that their data is erased if they've withdrawn their consent for their data to be collected, or object to the way it is being processed.

What happens if your organisation suffers a data breach?

If your organisation suffers a data breach it's your organisation's responsibility to inform the Information Commissioner's Office (ICO) of any data breach that risks people's rights and freedoms within 72 hours of your organisation becoming aware of it.

The deadline is tight and means that you probably won't know every detail of a breach after discovering it. However, your initial contact with the ICO should outline the nature of the data that is affected, roughly how many people are affected and what the consequences could mean for them. You should inform the ICO of the measures you've already taken or what actions you intend to take.

However, even before calling the ICO, you should tell the people affected by the data breach. Those who fail to meet the 72-hour deadline could face a penalty of up to 2% of their annual worldwide revenue, or 10 million Euros, whichever is higher.

If you don't follow the basic principles for processing data, such as having a legal basis for doing so or ignore individuals' rights over their data, you risk facing even higher fines of up to 20 million Euros or 4% of your annual turnover, whichever is greater.

However, it's important to note that fines must remain "proportionate" to the breach. If you demonstrate that you worked hard to ensure your organisation is compliant with GDPR, the ICO is unlikely to issue such high fines in the event of a breach.

What about Brexit?

The GDPR will apply in all EU member states from 25 May 2018 and GDPR has effect and will continue to apply to the UK post Brexit.

Do organisations need a data protection officer?

Any public body carrying out data processing needs to employ a data protection officer, as do organisations whose core activities involve data processing that requires they regularly monitor individuals "on a large scale".

The data protection officer's job is to inform and advise the organisation about meeting GDPR requirements, and monitoring compliance. They'll also act as the ICO's primary point of contact, and will be expected to cooperate with the authority.

Practical Tips for Compliance

Privacy by design

Privacy by design means building data protection into all your new projects and services. It has always been good practice, but GDPR makes privacy by design an express legal recruitment. To achieve this, data protection impact assessments should be undertaken where new technology is being deployed, where profiling may significantly affect individuals or sensitive categories of data will be processed on a large scale. Clarify who will be responsible for carrying out impact assessments, when you will use them and how you will record them.

The Information Commissioners Office (ICO) has guidance on privacy by design and data protection impact assessments.

Get ready to detect, report and investigate personal data breaches

A data breach is a breach of security leading to 'accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data'. You will need to have the right procedures in place to detect, investigate and report a personal data breach. GDPR introduces a duty to report certain types of data breaches to the ICO and in some cases to individuals concerned.

You need to be able to demonstrate you have appropriate technical and organisational measures in place to protect against a data breach.

Build in extra protection for children

Many charities support children and young people and GDPR brings in special protection for children's personal data. GDPR says that children under 16 cannot give consent (although this may be reduced to 13 in the UK) so you may have to seek consent from a parent or guardian. You will need to be able to verify that person giving consent on behalf of a child is allowed to do so and any privacy statements will need to be written in a language that children can understand.

Review how you get consent to use personal data

If you rely on consent as your lawful basis for processing personal data, then you need to review how you seek and manage consent. Under GDPR consent must be freely given, specific and easily withdrawn. You can't rely on pre-ticked boxes, silence or inactivity to gain consent instead people must positively opt-in.

Know how you deal with 'subject access requests'

Individuals have the right to know what data you hold on them, why the data is being processed and whether it will be given to any third party. They have the right to be given this information in a permanent form (hard copy). This is known as a subject access request. Your organisation needs to be able to identify a subject access request, find all the relevant data and comply within one month of receipt of the request.

Check your processes meet individuals' new rights

GDPR will give people more rights over their data. For example, GDPR gives someone the right to request to have their personal data deleted.

Would you be able to find the relevant data and who would be responsible for making

sure that happened? Get to know the eight rights and have the systems in place to be able to deliver one each of them.

Identify and document your 'lawful basis' for processing data

To legally process data under GDPR you must have a 'lawful basis' to do so. For example it is a lawful basis to process personal data to deliver a contract you have with an individual. There are a number of different criteria that give you lawful basis to process and crucially, different lawful basis give different right to individuals. For example if you rely on consent as a lawful basis, individuals have stronger rights to have their data deleted.

Update your privacy notices

You must always tell people in a concise, easy to understand way how you intend to use their data. Privacy notices are the most common way to do this. You may already have privacy notices on your website for example but they will need to be updated. Under GDPR privacy notices must give additional information such as how long you will keep data for and what lawful basis you have to process data.

Identify what data you hold and where the data came from

If you don't know what personal data you hold and where it came from you will need to organise an audit of your different systems and departments to find out. This means all personal data including employees and volunteers, service users, members, donors and supporters and more. You should document your findings as GDPR means you must keep records of your processing activities. You should also record if you share data with any third parties.

Contact details for organisations mentioned in this information sheet

Information Commissioners Office
https://ico.org.uk/
ICO helpline: 0303 123 1113

Civil Society Guide https://www.civilsociety.co.uk/news/free-gdpr-guide-published.html

Newcastle CVS
Higham House
Higham Place
Newcastle upon Tyne
NE1 8AF

Contact us: 0191 235 7037
information@cvsnewcastle.org.uk
www.cvsnewcastle.org.uk

Newcastle Council for Voluntary Service is a registered charity (number 1125877) and company limited by guarantee (number 6681475) registered in England and Wales | Our registered office is as above