The General Data Protection Regulation (GDPR)

What is it and what can you do to prepare for it?

GDPR will replace the UK Data Protection Act 1998 (DPA) from 25th May 2018. GDPR will apply across Europe, regardless of the UK's decision to leave the EU.

The new regulation strengthens the rights of individuals to access and amend their personal data; places greater emphasis on an organisation's accountability; and introduces more serious consequences for non-compliance, including fines.

Personal Data means any data which relates to a living individual who can be identified from the data, or from the data and other information that is in, or likely to come into the, possession of the data controller.

12 Steps to take now

https://ico.org.uk/media/1624219/preparing-for-the-gdpr-12-steps.pdf

Guidance Steps

1. **Awareness**
   You should make sure that decision makers and key people in your organisation are aware that the law is changing to the GDPR. They need to appreciate the impact this is likely to have.

2. **Information you hold**
   You should document what personal data you hold, where it came from and who you share it with. You may need to organise an information audit. ***(see attached template)***

3. **Communicating privacy information**
   You should review your current privacy notices and put a plan in place for making any necessary changes.

4. **Individuals' rights**
   You should check your procedures to ensure they cover all the rights individuals have, including how you would delete personal data or provide data electronically and in a commonly used format.

5. **Subject access requests**
   You should update your procedures and plan how you will handle requests within the new timescale of one month, and provide any additional information. You will not be able to charge for complying with a request.

6. **Lawful basis for processing personal data**
   You should identify the lawful basis for your processing activity in the GDPR, document it and update your privacy notice to explain it.

7. **Consent**
   You should review how you seek, record and manage consent and whether you need to make any changes. Refresh existing consents now if they don't meet the GDPR standard.
   https://ico.org.uk/media/about-the-ico/consultations/2013551/draft-gdpr-consent-guidance-for-consultation-201703.pdf

8. **Children**
   You should start thinking now about whether you need to put systems in place to verify individuals' ages and to obtain parental or guardian consent for any data processing activity.

9. **Data breaches**
   You should make sure you have the right procedures in place to detect, report and investigate a personal data breach.
   https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/

10. **Data Protection by Design and Data Protection Impact Assessments**
    You should familiarise yourself now with the ICO's code of practice on Privacy Impact Assessments as well as the latest guidance from the Article 29 Working Party, and work out how and when to implement them in your organisation.

11. **Data Protection Officers**
    You should designate someone to take responsibility for data protection compliance and assess where this role will sit within your organisation's structure and governance arrangements. You should consider whether you are required to formally designate a Data Protection Officer.
    https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-officers/

12. **International**
    If your organisation operates in more than one EU member state (ie you carry out cross-border processing), you should determine your lead data protection supervisory authority. Article 29 Working Party guidelines will help you do this.
    https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/international-transfers/

As a small charity what do I have to do to ensure we comply with GDPR?

You can find the latest guidance on the new legislation in the ICO's Guide to the GDPR. It will be updated regularly and you can check it for the latest position.

They have also created a package of tools aimed at small and micro organisations, including charities:

- Getting ready for the GDPR – a practical self-assessment tool
- 12 steps to take now checklist (as above)
- A dedicated advice line for small organisations

The GDPR is an evolution of the existing law. If you are already complying with the terms of the Data Protection Act 1998, and have an effective data governance programme in place, then you are already well on the way to being ready for the GDPR.

Privacy Notices

To cover all these elements you will need to consider the following issues when planning a privacy notice:

1. What information is being collected?
2. Who is collecting it?
3. How is it collected?
4. Why is it being collected?
5. How will it be used?
6. Who will it be shared with?
7. What will be the effect of this on the individuals concerned?
8. Is the intended use likely to cause individuals to object or complain?

It is also important to recognise that the ways in which data is collected are changing.

Traditionally, data was collected directly from individuals, for example when they filled in a form. Increasingly, organisations use data that has not been consciously provided by individuals in this way. It may be:

1. **observed**, by tracking people online or by smart devices;
2. **derived** from combining other data sets; or
3. **inferred** by using algorithms to analyse a variety of data, such as social media, location data and records of purchases in order to profile people for example in terms of their credit risk, state of health or suitability for a job.

In these cases you are acquiring and processing personal data about individuals, and the requirement to be fair and transparent still arises. These new situations can make it more challenging to provide privacy information, and new approaches may be required. A good way to approach these issues is to carry out a privacy impact assessment (PIA). This is a methodology for assessing and mitigating the privacy risks in a project involving personal data.

ICO Information re Data Consent and Privacy Statements

Give individuals appropriate control and choice

Where you need consent from an individual in order to process their information you need to explain what you are asking them to agree to and why. This will often go hand in hand with providing privacy notices. Therefore the code also includes information about obtaining consent.

It is important to make sure that where people do have a choice, they are given a genuine opportunity to exercise it. This means that it must be freely given, specific and fully informed. Consent must also be revocable (ie people must be able to withdraw their consent) and you should have procedures in place to action and record it when this happens.

You should always be honest with the public and not lead them to believe that they can exercise choice over the collection and use of their personal information when in reality they cannot.

There are some cases in which consent is not relevant, for example if individuals are required by law to provide their personal details. Giving people control and choice over how their personal data will be processed will not always be applicable in other situations, for example in an employer/employee relationship.

In all of these cases it is still important to be fair and transparent. Ensuring you have effective privacy notices can help you to achieve this.

Decide what to include by working out:

- what personal information you hold;
- what you do with it and what you are planning to do with it;
- what you actually need;
- whether you are collecting the information you need;
- whether you are creating new personal information; and
- whether there are multiple data controllers.

If you are relying on consent, you should:

- display it clearly and prominently;

- ask individuals to positively opt-in;
- give them sufficient information to make a choice;
- explain the different ways you will use their information, is there more than one purpose;
- provide a clear and simple way for them to indicate they agree to different types of processing;
- include a separate unticked opt-in box for direct marketing.

Also consider including:

- the links between different types of data you collect and the purposes that you use each type of data for;
- the consequences of not providing information;
- what you are doing to ensure the security of personal information;
- information about people's right of access to their data; and
- what you will not do with their data.

ICO Information re Data Breech

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/

GDPR introduces a duty on all organisations to report certain types of personal data breach to the relevant supervisory authority. You must do this within 72 hours of becoming aware of the breach, where feasible.

If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, you must also inform those individuals without undue delay.

You should ensure you have robust breach detection, investigation and internal reporting procedures in place. This will facilitate decision-making about whether or not you need to notify the relevant supervisory authority and the affected individuals.

You must also keep a record of any personal data breaches, regardless of whether you are required to notify.

Checklist

Preparing for a personal data breach:

- Know how to recognise a personal data breach.
- Understand that a personal data breach isn't only about loss or theft of personal data.
- Prepare a response plan for addressing any personal data breaches that occur.
- Allocate responsibility for managing breaches to a dedicated person or team.
- Ensure staff know how to escalate a security incident to the appropriate person or team in their organisation to determine whether a breach has occurred.