1. Introduction

The General Data Protection Regulation (GDPR) follows on from the current Data Protection Act. It gives individuals more say in how organisations use their data, making data protection regulations standardised throughout the EU. The Information Commissioner's Office (ICO) will be regulating the GDPR.

The data protection rules will apply to all businesses based in the EU and/or doing business in the EU. These organisations will have to comply with the new regulations if they collect any personal data from citizens residing in the EU. The new regulations will be much tougher, introducing fines for organisations not complying, with the hope that these new regulations help improve trust in the emerging digital economy.

2. What is the purpose of the GDPR?

The GDPR has been implemented in order to increase the levels of trust brought between an individual and an organisation. It allows an individual to know and understand what data is being collected by an organisation, and why it is being stored. Therefore by introducing the GDPR, it becomes easier for individuals to have more control over the data they have stored on them. Under this new legislation, it is now understood that an individual should be able to opt-out as easily as they were to opt-in.

3. Who is affected by the GDPR?

The new GDPR will apply to both 'controllers' and 'processors', meaning that those collecting personal data, and those processing the data will be affected.

For controllers, this means that you will need to ensure that all data being collected is compliant with the GDPR. As the data controllers make decisions regarding processing activities, they must ensure that there is sufficient purpose for the data to be collected. They must also have clear evidence that an individual gave them consent to store their data.

Processors, who are processing the data on behalf of the controller, will need to ensure that records of personal data and processing activities are all well documented. Evidence of all this must be maintained in order to comply with the new legislation.

The GDPR not only applies to any organisations that are operating from within the EU, but also those that are involved with trading goods or services to individuals residing in the EU.

4. Types of Data

There are two types of data that is important in GDPR: personal and sensitive.

Personal Data

This involves data that can directly or indirectly identify an individual, which could involve names, ID numbers, location data or even online identifiers. As a result of this, the technology used in everyday tasks and also the way in which organisations collect personal data will have to be adapted.

The GDPR is only applicable to living people, as personal data collected on the deceased does not fit within the legislation.

Sensitive Data

Sensitive data consists of any data that categorises an individual. This includes any data surrounding an individual's ethnicity, religion or political views. It also applies to genetic and biometric data that can specifically identify an individual.

Any individual data that is identified with criminal convictions and offenses are excluded from the GDPR as criminal law is outside of the EU's authority.

5. Penalties

If your organisation has a breach in data and it is not reported within the 72-hour deadline, there is a risk of being fined up to €20 million or 4% of your global annual turnover – the fine will be based on whichever one is greater.

If a breach in data "*is likely to result in a risk to the rights and freedoms of individuals*" it must be reported to the ICO. It should also be reported to the individuals whose data has been breached if it risks their '*rights and freedom*'.

In some organisations, particularly those with over 250 employees, it is recommended that a 'Data Protection Officer' is employed to help manage the GDPR compliance of the firm. Though this isn't a legal requirement, it can help reduce the possibility of any potential data breaches that could risk in a significant fine.

6. Individuals Rights

Individuals whose data you have collected now have the 'right to be forgotten'. If requested, their data must be completed erased. This would mean that the controller of the data is responsible for telling other organisations linked to them to delete all copies of the data stored on this individual.

If an individual does request access to their data, in most circumstances you will no longer be able to charge them a fee for complying with this request. As an organisation, you have 30 days to complete the request and disclose the information. However, in some circumstances, organisations can refuse or charge for requests from an individual that are unfounded or deemed excessive.

The GDPR allows individuals to have:

- The right to be informed
- The right to access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- The right to not be subject to automated decision

7. Preparing your Website for the GDPR

Form Submissions

The collection of data from the forms submitted through your organisations website is something that will need to be assessed. Almost all of the data collected will be classed as 'personal data', so this might include things like event registrations and enquiries etc. This data can only be stored for 60 days. After the 60 days are up, the data must be anonymised meaning that any identifying attributes must be removed.

It is also worth noting that the data can only be used for the purpose that the individual has consented to. This means that you cannot automatically add an individual to your mailing list after receiving a completed enquiry form from them.

The rest of the data collected such as the data and time the form was submitted can be held onto so that the performance of the forms can be continually monitored by the marketing team.

Newsletters

The GDPR has made it clear that email newsletters need to be as easy to opt-out of as they were to opt-in. MailChimp are one of the services that has already put into action the easy opt-out process for their email templates.

They also specify that when users are filling out a form that gives them the option to subscribe to a newsletter, the form can no longer automatically opt for "yes". It should default to "no", then giving the user the option to amend.

Online payment

If your website uses a payment gateway to for example collect payment for events or pay invoices, then there may need to be some changes in the way the data is processed. Each online payment system will vary in the technology used as some will push the payment towards an external site, while others will use an API to integrate the payment system into the website. Either way, it is worth checking if the personal data collected is stored.

For any personal data collected (names, addresses, etc), it will all need to be deleted after 60 days. This would just mean that any identifying factors such as names, email addresses will need to be removed from the system.

Registration

On areas that might require individuals to 'register' to view/access content, you need to be explicitly clear to them what will happen with their personal information that is collected during the registration process. The individual must agree to your Terms & Conditions of collecting the data, and it is also recommended that a double opt-in approach is used. E.g. the user registers, and then they get another email which allows them to confirm their registration.

Privacy Policy

A large part of the GDPR is clearly communicating to individuals how you're collecting their data and what your organisation tends to do with it. The language used in your websites privacy policy needs to be clear and concise. It needs to state how the data collected on individuals is going to be processed, and that if they have any problems with the way in which their data is being handled then they are able to contact the ICO.

Staff Profile Pages

In order to comply with the new regulations, you will need to gain permission from each staff member if you wish to display their photo, contact information and personal details on your website. This needs to be documented for your records, so it is essential that all staff members sign a copy of a document to show they have given consent for these details to be displayed on the website.

The document would also need to give information on how staff members may proceed on the occasion that they do not want these details displayed or removed from the website.

Case Studies/Testimonials

If there are any case studies or testimonials that reveal an individual's name or any other identifying factors, then you need to gain permission from that individual to display their data on the website. Similar to the way in which you gain consent from staff members for their profile pages, you would need to get permission from individuals providing testimonials.

On all occasions where data is being collected on an individual, there should always be a disclaimer to state what, where and why the data is being recorded. It needs to use clear and concise language that can be easily understood by the individual. They need to have a solid understanding of the purpose their data has for being stored.

A 'how to comply' checklist

This short checklist will help you comply with the Data Protection Act (the Act). Being able to answer 'yes' to every question does not guarantee compliance, but it should mean that you are heading in the right direction.

- ❑ Do I really need this information about an individual? Do I know what I'm going to use it for?
- ❑ Do the people whose information I hold know that I've got it, and are they likely to understand what it will be used for?
- ❑ Am I satisfied the information is being held securely, whether it's on paper or on computer? And what about my website? Is it secure?
- ❑ Am I sure the personal information is accurate and up to date?
- ❑ Do I delete/destroy personal information as soon as I have no more need for it?
- ❑ Is access to personal information limited only to those with a strict need to know?
- ❑ If I want to put staff details on our website have I consulted with them about this?
- ❑ If I use CCTV, is it covered by the Act? If so, am I displaying notices telling people why I have CCTV? Are the cameras in the right place, or do they intrude on anyone's privacy?
- ❑ If I want to monitor staff, for example by checking their use of email, have I told them about this and explained why?
- ❑ Have I trained my staff in their duties and responsibilities under the Act, and are they putting them into practice?
- ❑ If I'm asked to pass on personal information, am I and my staff clear when the Act allows me to do so?
- ❑ Would I know what to do if one of my employees or individual customers asks for a copy of information I hold about them?
- ❑ Do I have a policy for dealing with data protection issues? Do I need to notify the Information Commissioner?
- ❑ If I have already notified, is my notification up to date, or does it need removing or amending?

If you need any more information about this or any other aspect of data protection, please contact the Information Commissioner's Office : www.ico.org.uk