Assentive Ltd
Your partner for business solutions

25/7/2018

BECOMING GDPR COMPLIANT

The steps any organization needs to go through

mailto:info@assentive.uk

Author: Assentive Ltd

Assentive Ltd
Your partner for business solutions

BECOMING GDPR COMPLIANT

The steps any organization needs to go through

This guide aims to provide a sensible and practical approach to meeting the requirements of GDPR for any organization be it a commercial enterprise, a school, a government organization or a local club or charity. Any organization that collects, handles and uses (or, as the GDPR likes to call it, "processes") personal data needs to follow these steps to ensure it is compliant and can remain compliant with the regulation.

It is not meant to be and does not purport to offer a thorough or detailed alternative to getting legal advice on the GDPR and how it affects your specific business. Its aim is to enable business leaders to gain an overview of the key matters they need to know and to help them identify some of the areas where they may need more advice, information or help. For readers wishing a more comprehensive document on the GDPR the ICO has produced a 241 page guide (see www.ico.org.uk) with a further guide on children and the GDPR!

We, in contrast, have adopted a "brevity over comprehensiveness" approach which we hope our readers will appreciate.

Assentive Ltd
Your partner for business solutions

Brief overview of the GDPR

For those readers who have been living in isolation and have remained blissfully ignorant of the events of the past 12 months here is a synopsis of what we are talking about.

The GDPR (General Data Protection Regulation) is an EU-wide regulation which came into force on 25th May 2018 and provides enhanced data rights for individuals as well as greater responsibilities (and penalties) for organizations which handle personal data. This is defined as any data which can be used to identify a person such as their name & address, email address, etc.

If you maintain lists of people – customers, potential customers, club members, staff, pupils or similar – then the GDPR affects you. This pretty much captures any business, government department or charity and many others. It doesn't affect us as individuals if we keep lists of our friends' emails unless the plan is to start sending them unsolicited marketing emails.

There are plenty of expansive guides to the GDPR and what it does but, in summary, the key things to note are:

1. You can no longer treat people's personal data as if it were simply an asset of your business – it must be treated with respect by you and all your staff and, in effect, it is loaned to you and not owned by you;
2. Anyone can ask you to send them the data you have on them (free of charge) or to delete it if they wish. Unless you can demonstrate a good reason to be keeping it you will have to comply;
3. You need every data subject's permission to use their data in specific ways. This means you can no longer ask for blanket consent to use their data, you have to specify HOW you plan to use it;
4. There are certain special types of personal data which are classed as more sensitive and requiring greater security. These will probably surprise few of you – sexual orientation, genetic data, health records, race, politics, ethnicity and trade union membership;
5. Compliance is now a direct responsibility of the data controller – what the GDPR calls accountability;
6. If you do have a data breach the sanctions can be serious. In truth, we would not expect many businesses to be hit with the full wrath of the GDPR penalty regime unless the breach was large scale and/or due to willful negligence. However, it pays to make sure you have done everything you can to avoid this happening;
7. Data security needs to be "designed in" to your systems and your organization and not managed as an afterthought.

Most businesses will be able to audit their own systems and make the necessary changes without too much stress but the one thing not to do is be complacent about this. If the regulator (Information Commissioner's Office) is going to be harsh with anyone it will be those that have ignored the regulation or been blasé about the implications, especially if they go on to have a major data breach.

Assentive Ltd
Your partner for business solutions

Getting outside help

In many cases organizations will be able to achieve compliance without the need for expensive consultancy advisors, new software tools or other costly additions. However, it is worth bearing in mind that that the Information Commissioner's Office (ICO) is entitled to ask you for evidence of the processes you followed and the decisions you made as part of its review of your compliance. This will mean that many organizations will find a benefit in having some external input and guidance on their process so that the decisions are fully documented.

Also, do not underestimate the considerable time and resource that this exercise could demand in your organization. If you do not already have suitably qualified in-house resource then the time needed for someone to become adequately competent may itself be quite costly. Sometimes a relatively modest investment now can be a saving in the long run but analyze carefully your own organization and its needs before you commit too much to 3rd parties as they will not know your business half as well as you do.

Whatever you do please ensure you do not rely on someone else entirely and do not buy software in the hope it will answer all your needs. Data protection needs to become second nature to everyone in your organization from the highest levels down and there can be no substitute for having a proper appreciation of the regulation. If you do feel the need to appoint a Data Protection Officer (DPO) for your business (whether as a full-time employee or an outsourced provider) then you will need to accept that they cannot be restricted in how they go about performing the duties that are expected of someone in that position which may mean them having access to people, data and meetings that are important in the fulfillment of their duties.

Assentive Ltd
Your partner for business solutions

The first steps

Know what you've got

Before you can even begin to see how close or distant your organization is from compliance you will need to audit the data you currently hold. For some this may be simple but do not be deceived... it is a multi-dimensional issue:

What data?	How obtained?	How held?
Customer data	With consent? Or not? What consents?	Electronic databases – how many?
Staff data	Bought-in lists?	Filing cabinets?
Business contacts	Ex employees? Pensioners?	Address books?
Supplier data	Downloaded from LinkedIn?	External agencies?
Any sensitive data? On children? Sexual orientation? Race? etc	Copied from an email someone once sent?	Other software tools. E.g. accounting software

The table above is hardly an all-inclusive list but it should begin to give you a flavour of what you need to be looking for, where to look for it and where some ruthless purging might be worthwhile. Every member of your team needs to be involved in this since any data they hold (that spreadsheet each salesman has that he guards jealously on his computer's C-drive or, worse, on a data stick he carries everywhere he goes!) has to be included in this. A data breach is a data breach, regardless of who within your team was responsible or where the data had been held.

We would recommend establishing a committee with representatives from the main departments in your business so that there is buy-in from all and everybody understands that compliance overrides any other considerations they may previously have had as regards data, its acquisition, storage, sharing and use (or "processing").

Centralize as much as you can

Once you have identified the data you have and where it came from it would be wise, as far as you are able, to pull it all together into one place and discard any datasets you can do without. This will make it easier to manage going forwards, will enable you to respond to requests from data subjects asking what you hold of theirs and should ensure you can archive or delete records as required.

Once you have the data in one place you need to prevent staff from reverting to previous bad habits and creating their own databases. Your data protection policy should enshrine this rule but any practical measures you can take to encourage sharing and discourage hoarding of data will help. Conduct regular audits of the data people are retaining and run update talks for staff so that they become aware of the dangers of personal contact lists.

Document policies and procedures

There is little point collating all the information on what data you hold and where it resides if you do not set up systems to control how data is collected and stored in the future. You will almost certainly need new policies and procedures but these need to be dynamic and adaptive. More legislation is on the way (the ePrivacy Regulation is not far away, for example) and your staff need to be educated in the ethos of data protection so that they can quickly assimilate and put into practice all new laws and regulations as they arrive.

Train your people

Educate your staff to understand what data privacy is all about and how your organization plans to meet and exceed the standards required. Get them to change their behaviour in ways that reflect not merely the cost of failure to comply but the very real benefit you can get from leading the market in data security standards. Customers need to trust your organization if they are to permit it to retain their data so make sure you are and remain above reproach in this. We believe there will be tangible competitive advantages to be had from being ahead of the crowd in data security and data protection.

Do not rush to buy software

If you plan to buy software to help you with data security then do so once you have completed your audit and documented your policies and procedures. To seek a software solution prior to this runs the risk of ending up with an unsuitable product because you were not best placed to specify accurately what your organization actually required.

Systems considerations

Whilst we have counseled against rushing into software purchases you will need to ensure your current systems – computerized and manual – can cope with the reporting requirements laid out by the GDPR and likely to follow with new legislation too.

Subject Access Request ("SAR")

Data subjects (that's you and me and every other natural person still alive) have the right under the GDPR to request any organization for copies of all data that organization holds on them. This request has to be fulfilled within one month and at no cost to the data subject. The request does not have to be in writing or to specifically mention that it is an SAR – verbal requests made to a member of your staff for the data you hold on the data subject is sufficient.

You need to make sure your organization and all relevant staff are trained to recognize each SAR howsoever made and to respond fully and compliantly within the stipulated one month. If you are holding data in different systems, locations or ledgers this may become a challenge and that is why we recommended on page 4 that you consider pulling as much of it into one place as you possibly can to make life easier when you receive an SAR.

Data Protection Impact Assessment ("DPIA")

You need to have systems and controls to identify when an intended action with the data you are holding may represent risk to that data and the people behind the data– e.g. the change of storage location, a plan to process the data in some new way or combine data from different sources. In such circumstances you will need to carry out a risk assessment or DPIA in the GDPR terminology.

Make sure your staff are trained and qualified to carry out these assessments competently and that each DPIA is thoroughly documented – you are guaranteed to need to evidence this should anything go wrong.

Breach recognition, reporting and recording

Set up systems now to record any breaches of personal data from your organization, no matter how small the breach. Not only is this a requirement but it will help to train your staff to recognize what constitutes a breach so that you can identify those that are serious enough to require you to report them to the ICO and, where applicable, the affected data subjects.

Breaches do not only occur where electronic data is sent or carried outside your organization and falls into the wrong hands. They can be accidental disclosure of personal data on the telephone or even a tube train; sending emails to the wrong people; allowing the visiting plumber to see and even copy data in a written format. Anything, in other words, which could affect the Confidentiality, Integrity or Availability ("CIA") of personal data which may have a detrimental effect on the persons whose data is compromised in this way.

Closing remarks

As stated on page 1 this guide is only intended to be a brief overview and each business will have specific measures it needs to adopt in respect of the data it holds and processes. Many businesses will already be compliant or will have systems and policies which need few changes to adapt them to the GDPR regime but, as at the time of writing this, many commentators are saying that as many as 60% - 70% of businesses are still lacking adequate compliance with the regulation.

If your business needs help getting up to speed then please get in touch – info@assentive.uk. The process needn't be painful but failure to go through the checks and necessary changes could well lead to a painful outcome in due course.