ampersand STUDIO

T: +44 (0)1295 533544
E: enquiries@ampersandstudio.uk
W: ampersandstudio.uk

GDPR Compliance

GDPR is the biggest change to privacy laws in the last 20 years and will replace the 1998 Data Protection Act. The digitalisation of our lives since 1998 has brought about the requirement to update the 1998 Act. So what does it all mean?

What is GDPR?

GDPR stands for General Data Protection Regulation and will be coming into force on 25th May 2018. Detailed information can be found on the EU GDPR website. Let me start by saying this is a good thing! Yes, it will require some time and effort to ensure you comply but as a citizen, business owner, manager or employee, this is being introduced to protect your personal data in the ever increasing digital world we live. The current Data Protection Act was introduced in 1998 and a lot has changed in those 20 years! There was no such thing as an iPhone back in 1998, for example. Reviewing your data systems should be carried out on a regular basis anyway so see this as an opportunity to house keep your data collection and management methods.

How do I Comply with GDPR?

This is where it can get a bit complicated and we advise you get advice from your legal representative or GDPR specialist as every case will be different. You may also wish to study the EU GDPR website and work through it yourself. That being said we have broken down the major parts for you, allowing you to make a good start. You may also wish to take a look at the GDPR FAQs, in this document, for answers to some of the common questions and we have also put together a glossary of some of the terms you will read, as some may not be self explanatory.

The ICO (Information Commissioner's Office) will be responsible for ensuring compliance in the UK and so they also provide useful information on their website, for both public and organisations. Our summary of advice, below, is taken from the 'For Organisations' section of the ICO website, using their 12 step plan for preparing for GDPR.

ampersand STUDIO

T: +44 (0)1295 533544
E: enquiries@ampersandstudio.uk
W: ampersandstudio.uk

GDPR Compliance Steps

Last updated: 26/3/2018

Step 1: Awareness

Make sure all key decision makers in your organisation are aware there are changes coming and ask them to consider the impact of these changes. This applies whether you are a sole trader or employee in a large organisation.

Step 2: Information You Hold

Create an audit of all the personal information you hold. This includes data held on and offline, in cloud space or filing cabinets. You must ensure you know what is held, where it is held, what it is used for and where it came from. This information will form part of your privacy policy.

Step 3: Communicating Privacy Information

If you haven't already done so, you should create a privacy policy that details the information you have sourced from step 2. The policy needs to be publicly available and understandable to read, no legal talk, just plain English.

Step 4: Individual's Rights

Personal information should be considered to be the ownership of the individual who the data is about. You must be able to provide a legitimate claim for holding the data as well as having a plan in place for being able to remove data, should the request be made. You must also be able to provide an electronic copy of all data you hold on an individual, should it be requested.

Step 5: Subject Access Requests

A subject access request (SAR) is a request from an individual to have a copy of all the data you hold on them. If a subject access right is made you will not be able to make a charge for the request and must be able to comply within one month. Refusal or charging for a request is possible but the grounds for both must be detailed to the individual, for which they have the right to appeal. In most standard cases a charge is unlikely to be acceptable.

T: +44 (0)1295 533544
E: enquiries@ampersandstudio.uk
W: ampersandstudio.uk

Step 6: Lawful Basis for Processing Personal Data

Do you know what the lawful basis for holding personal data is? In most cases it's likely that you have requested consent, at some point, but this needs to be documented in your privacy policy. If consent is the lawful basis for holding personal data then an individual has the right for that data to be deleted.

Step 7: Consent

You must review the basis for which you seek, record and manage consent. If you can't provide evidence of data having been sought using methods that comply with GPPR consent rules then you will have to request consent again in order to continue holding the data. A detailed guidance on consent can be found here and you should use this to review your current procedures. A key point is that consent must be via an opt-in process and may not be included as part of other terms and conditions. For example, a condition of creating a new account, may not be that the new registration is automatically added to a mailing list.

Step 8: Children

For the first time an individuals age may be of consideration when collecting data. There will be new protective rights for children's personal data and you should consider if your arrangements need to gain parental consent and / or verification of age. An individual may not consent until the age of 16, although this may be reduced to 13 in the UK.

Step 9: Data Breaches

Would you be able to detect if a data breach has taken place? If not you must update your systems to ensure you can detect, report and investigate a data breach. It is likely that a data breach will require you, by law, to notify the individual(s) as well as the ICO. By reviewing this step you can document when and where any possible data breach needs to be recorded.

Step 10: Data Protection by Design

Essentially this is ensuring that any new system is created with privacy at the centre of the design process. Considering the privacy implications after development of a new system will no longer be legal. When there is a possible privacy risk with new implementations a Data Protection Impact Assessment

T: +44 (0)1295 533544
E: enquiries@ampersandstudio.uk
W: ampersandstudio.uk

(DPIA) should be carried out. You should create a system for knowing what the assessment will include, who will carry it out and who else needs to be involved in the assessment. Further guidance for DPIAs can be found on the ICO website.

Step 11: Data Protection Officers

Public organisations and organisations that carry out large scale monitoring of data are formally required to employ a Data Protection Officer (DPO). A small organisation should still appoint someone to have a responsibility for data protection, even if it's not their primary or sole duty within the organisation. This can then be documented in a privacy policy making it clear who the point of contact should be.

Step 12: International

If your organisation has offices or working buildings within a number of EU member states then you should nominate a lead supervising authority. This should be the location that is responsible for the majority of your organisations administration or where decisions can be made.

ampersand STUDIO

T: +44 (0)1295 533544
E: enquiries@ampersandstudio.uk
W: ampersandstudio.uk

When do I have to comply by?

GDPR will be coming into force on May 25th 2018

What is Personal Data?

Personal data is anything that can be used to identify someone. This could but is not exclusive to; a name, email address, phone number, photo, social media posts and even an IP address

I'm a sole trader / small business, does this apply to me?

Yes.

As this is an EU directive will I still need to comply after Brexit?

Yes. The British Government have stated this will be adopted after Brexit and apply to UK residents as well as EU residents. Even if this wasn't the case, if you are engaging with EU citizens and collecting their data you would still have to comply even if your company is not within the EU.

Does this mean I can't send any email to a customer without consent?

No. Transactional emails, such as those stating an order has been received, or emails that are fundamental to operations may still be sent, however, all marketing emails must have specifically been opted in to. This could include emails inviting customers to visit a social media account, so care should be taken regarding the language used and whether the intent is to market the organisation.

Does this just apply to online records?

No. All records held, whether online, in the cloud or locally in a document are considered to be covered. If you collect business cards and store these they are also included and you should ensure customers, colleagues and clients are aware that you hold this information and what it's intended use is. Being given a business card is not confirmation or opting in to marketing either. This must be a recorded opt in process as it could be claimed you simply found the business card and weren't handed the business card.

Does this just apply to customers?

No. Employee data must also be held in a compliant manner. For example a company that holds an employees personal data would be considered the data controller. If that company outsources the payroll service to another company then the payroll company would be the data processor

How do I make my email system compliant?

T: +44 (0)1295 533544
E: enquiries@ampersandstudio.uk
W: ampersandstudio.uk

A great question and a very grey area! Receiving an email, by its very nature, will include personal data from the sender. As a minimum you will have, and be storing, their email address but without explicit consent to do so. At this stage my advise would be that it's reasonable to assume that the mere fact someone has sent you an email is also acknowledging that you will maintain that personal data within your email system. The key is to ensure you manage that data properly so it is not passed on or sold or added to a mailing list without explicit instruction to do so. You must also ensure that your email system is secure and that you publicly acknowledge where email data will be stored and backed up to.

T: +44 (0)1295 533544
E: enquiries@ampersandstudio.uk
W: ampersandstudio.uk

GDPR Glossary

There are a number of terms that you will here being used when discussing GDPR so we have created a list of some of the most common terms and what they mean:

Data Processor: Processes data at the instruction of the controller.

Data Controller: The collector of the data and person who makes decisions about the use of the data.

Consent: You may not use indecipherable terms and conditions filled with legalese. It must also be as easy to withdraw consent as it is to give consent.

Breach Notification: You must report the event of a data breach within 72 hours. This is not 72 business hours and the notification must be sent to data controllers and customers.

Right To Access: Customers have the right to obtain confirmation from data controllers of whether their data is being processed. An electronic copy of the data should be provided free of charge if requested.

Right to be Forgotten: If the data is no longer relevant to it's original purpose customers can ask the data controller to erase their personal data. There are cases where this would not be practical, for example, in order to keep a product warranty valid for the full term of the warranty or if the data could be used as part of any investigation.

Privacy by Design: Data protection must be considered from the beginning of the design process for any new systems.

Data Protection Officers: DPOs must be appointed in public authorities or large organisations (>250 employees) that monitor or process personal data.

Subject Access Request: A subject access request is when an individual requests a copy of the information that is held on them. This must be able to be provided electronically within one month.

Data Protection Impact Assessment: A data protection impact assessment (DPIA) is an assessment that should be carried out to evaluate the risk to data protection on new technologies or systems that will be introduced. As part of the privacy by design requirement, data protection assessment must be carried out prior to a new technology or system being introduced.