GDPR will affect us all

YOUR ESSENTIAL GUIDE TO THE GDPR

INC HOUSE

INDEX

Content in this guide was written by Alistair Bell from Inc House. Inc House is a creative service in Rutland helping businesses and groups to spread their message using graphic design, web design, brand design and print. You are welcome to share the information within this guide as I believe it will be useful to many businesses.

www.inchouse.co.uk

INC HOUSE

Disclaimer: This guide is not legal advice. I'm not lawyer.

GDPR

THE LAW IS CHANGING

GDPR will affect your business and it doesn't matter if you are a small one man band or a large corporation.

You need to make sure you are ready. This information will provide you with the tools you need to protect yourself from potential fines resulting from non compliance with the new regulations.

WILL THIS AFFECT ME?

Simply put, yes. If you use any tracking tools like google analytics, if you have a contact form on your website, do email marketing, make sales calls, send out marketing literature or store information about clients and potential clients then this very much affects you.

Penalties are likely to include fines of up to 4% of annual revenue or £20 million, whichever is higher.

From **25th May 2018**, General Data Protection Regulations or GDPR come into force and some things you might do today will no longer be permitted.

You may have heard that this new law is enforced by the EU and that we are leaving the EU so why should we be concerned. Unfortunately, the legislation will come into effect before we leave the European Union, and even when we do leave, the UK government is unlikely to remove it.

DON'T WAIT UNTIL MAY

You may think that May 2018 is a long time away but if you start to take some of the simple steps in this guide now then you will save yourself a lot of trouble when the time comes.

This guide will not cover all of the new law as there is so much to know but it will cover some of the basics which will help you to start getting things in order.

DATA SUBJECT'S RIGHT TO BE INFORMED

Users have to be informed by means of a Privacy Policy about what information you may store and how that data may be used within your business including tracking data and IP Address (Transmission Control Protocol/Internet Protocol) information.

Don't have a Privacy Policy? You need to get one and it needs to be good!

GET PERMISSION FROM THE DATA SUBJECT

If you are using an email marketing tool like Mailchimp then you are probably aware that they are quite strict on who you can send email campaigns to. They require compliance with a rule that you must receive permission before you can start sending marketing emails to your list. Well the same applies to GDPR rules. The data subject must opt in to your marketing list and that means that they have to have ticked that box at the end of your contact form saying they give permission rather than it being pre-ticked. You may have got away with this in the past but that will change.

This applies to data that you have already so you should check that you have received permission from your existing contacts and if you don't, either seek it or delete those contacts.

Start getting consent now. Don't wait for the deadline.

If you don't have the function to ask permission with the forms on your website then I can help to put those in place. Please email alistair@inchouse.co.uk to find out how I can help you.

JUST GETTING PERMISSION ISN'T ENOUGH

Its not just a case of your contacts ticking the box and giving you permission, you also need to have a record of when and how you gained that permission. You also need to have evidence of the options they were given when they did opt in.

Is it starting to sound like a lot? This is why I'm pushing people to start taking action now and there is more.

There are different ways to record this information including creating a database on your website that securely stores form data. Again, if you would like help with this please contact me alistair@inchouse.co.uk.

THE RIGHT TO OPT OUT

The data subject must have a clear and simple way of changing their mind so that they can opt out of your marketing or have their data completely removed from your system / database at any time. If they do opt out then their data must be removed within a reasonably short space of time.

There are simple ways of doing this. For example you might give them the facility to send an email with the subject "unsubscribe" or you might provide a link to a page with an unsubscribe form.

Likewise, if you send printed marketing material, you have to provide details explaining how they can request that their data is removed so they don't receive further marketing, for example a telephone number or email address.

Keep the list of those that have opted out safe. If someone has asked to be removed from your data and they subsequently receive something, you are at high risk of being reported and facing fines.

Ask about building an opt out page and form for your site. alistair@inchouse.co.uk

CALLING THE DATA SUBJECT

Telephone marketing is a common annoyance for most businesses and I myself receive quite a number of calls about accidents I am supposed to have been involved in and other claims I could be making. Occasionally I receive more relevant calls regarding services I would be interested in but I have taken steps to stop such sales calls using a service called TPS (Telephone Preference Service). You may already use TPS for your business and, like me, it may not stop the calls but simply saying "TPS" to a sales person usually ends the conversation very quickly.

If you make a sales call to someone who's on the TPS list, you will be breaking the law, and you're liable to be fined. Previously it was Ofcom who punished offending businesses. Now it's the ICO who are much more strict.

If you are actively making sales calls to potential clients you need to check if they are registered with TPS.

You can sign up your business or personal number to the list or check if the person you are about to sell to with a phone call is on the TPS list at www.tpsonline.org.uk

HOW SECURE IS YOUR WEBSITE?

I'm guessing that by now you have heard of SSL (Secure Sockets Layer) certificates or have seen the little padlock symbol in the address bar when you are browsing a website. Well SSL helps your website to stay secure by encrypting data shared between your site and the user.

Use of SSL has risen from 2% in 2011 to 42% in 2017 and is climbing rapidly.

The reason for the ongoing rise in use is that Google now considers website security a very important matter. If you don't have a SSL certificate on your website google is likely to warn users that your site is not secure and in some cases will not display the site to the user.

If you have a contact form or any kind of form on your website you absolutely must ensure you have a SSL certificate.

Unfortunately, like a lot of the security changes we are talking about in this guide applying the certificate is not easy and although there is a lot of advice on how to apply it the process can be quite complex. If you would like some help applying SSL to your website drop me an email alistair@inchouse.co.uk.

WHAT ABOUT DIRECT MAIL?

By now you may be forgiven for wondering how you are going to continue with effective marketing without considerable time and effort.

I have some good news springing from the world of traditional marketing!

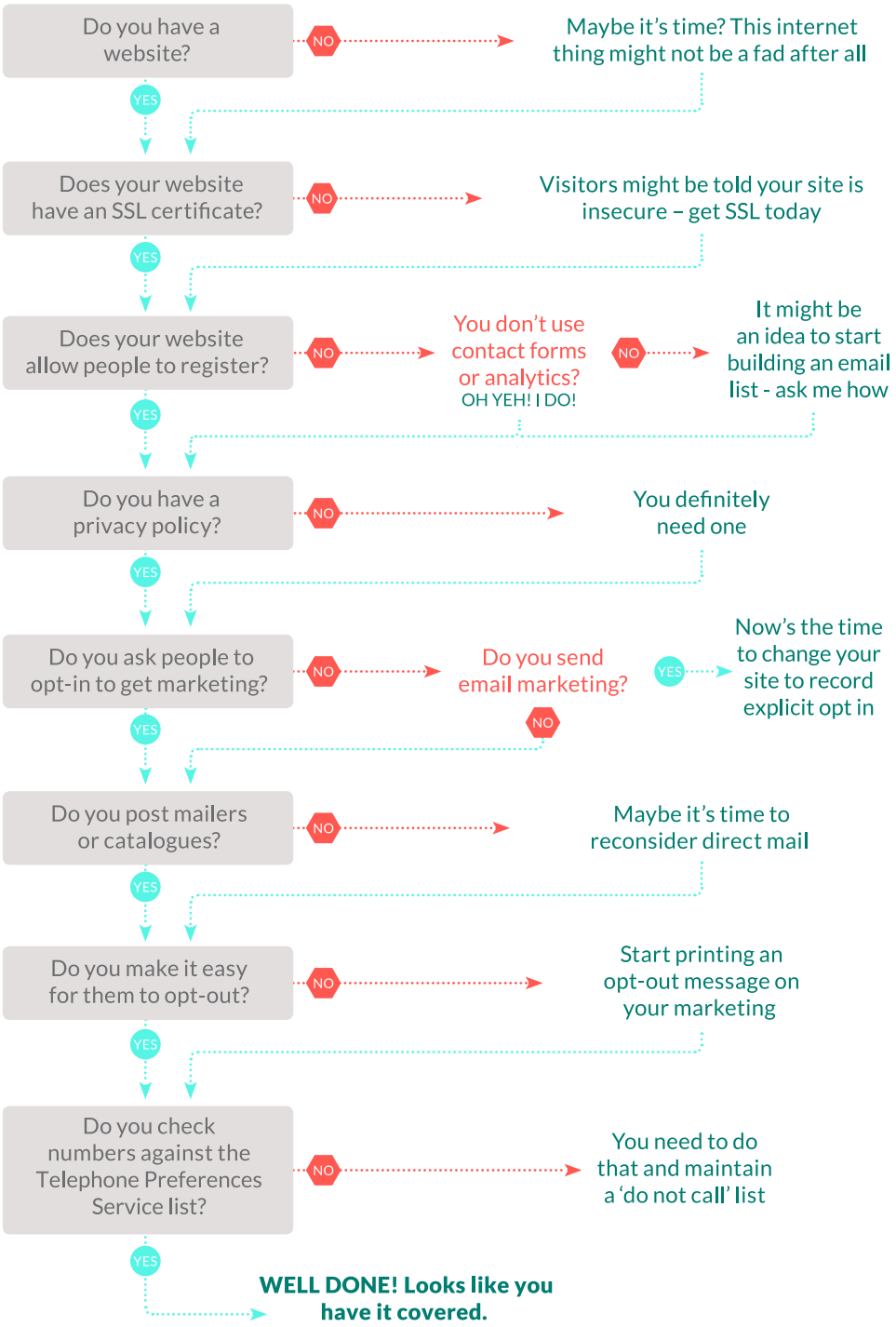
The compliance regime for direct mailing is slightly different. You must make sure that what you post out is relevant and you absolutely must make sure you give clear details on the mailer how the recipient can opt out of your mailing list using a phone number or a simple link to a page on your website with an opt out form.

This is called the 'legitimate interests' rule and it may result in the resurrection of the printed mailer. In a time when nearly all marketing is done on line and through email and social media we receive much less printed marketing than we once did. This is actually an opportunity to be exploited. At a time when most people's inboxes are overloaded with marketing material that is never read, why not provide the only bit of posted marketing your potential client receives today - and get noticed.

Done well it can have a lot of impact so why not give it a go? If you would like some information regarding mailers and possible print options then drop me an email to alistair@inchouse.co.uk

A study by MarketReach revealed some startling insights…
87% of people said they were influenced to make an online purchase as a result of receiving direct mail and **four out of five people said they'd connected with a business after getting direct mail.**

Did you know the average mailer hangs around the home for 17 days? **29% of people said they're shared with someone else? 72% of people get less than three pieces of mail a day. Yet 70% agreed they get too many emails.** Is it time to look again at direct mail?


Do you have a website?
NO
Maybe it's time? This internet thing might not be a fad after all
YES
Does your website have an SSL certificate?
NO
Visitors might be told your site is insecure – get SSL today
YES
Does your website allow people to register?
NO
You don't use contact forms or analytics?
OH YEH! I DO!
NO
It might be an idea to start building an email list - ask me how
YES
Do you have a privacy policy?
NO
You definitely need one
YES
Do you ask people to opt-in to get marketing?
NO
Do you send email marketing?
YES
Now's the time to change your site to record explicit opt in
NO
YES
Do you post mailers or catalogues?
NO
Maybe it's time to reconsider direct mail
YES
Do you make it easy for them to opt-out?
NO
Start printing an opt-out message on your marketing
YES
Do you check numbers against the Telephone Preferences Service list?
NO
You need to do that and maintain a 'do not call' list
YES
WELL DONE! Looks like you have it covered.

WHERE TO GET STARTED?

Take a look at the flow chart on the previous page which covers every step you need to consider now.

GDPR does not just apply to personal data it also applies to company data so GDPR most probably applies to you.

I hope you found this guide useful and can identify the things you now need to protect yourself and your business. There is a lot more information available to read on the **Information Commissioner's Office website www.ico.org.uk**. This is the body upholding the law and issuing fines. Download extensive guides and read their latest guidance.

There is a highly useful checklist tool and a 12 step guide which you can access by going to the ICO website and clicking on the GDPR link in the 'For Organisations' section.

12 STEPS TO TAKE NOW

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.

2. Communicating privacy information
You should review your current privacy notices and put a plan in place for making any necessary changes in time for GDPR implementation.

3. 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.

4. Subject access requests
You should update your procedures and plan how you will handle requests within the new timescales and provide any additional information.

5. 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.

6. 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.

7. 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.

8. Data breaches
You should make sure you have the right procedures in place to detect, report and investigate a personal data breach.

9. 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.

10. 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.

11. 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.

This information was taken directly from ICO guide 'Preparing for the General Data Protection Regulation (GDPR) 12 steps to take now'. Please review the full guide on the ICO website.

If you would like assistance with implementing anything in this guide, then please get in touch to discuss how I can help.

Email
alistair@inchouse.co.uk

INC HOUSE

www.inchouse.co.uk