Introduction

Unless you live under a rock, in a subterranean cave, or on Mars, you’ll know that back in 2018 there were four letters which dramatically changed the relationship email marketers have with the data they collect, store, and use. These four letters were GDPR.

At the time, Jarrang (as email marketing experts) and Stephens Scown (as one of the UK’s leading law firms) teamed up to bring guidance and clarity to the new General Data Protection Regulation (GDPR). This helped businesses of all shapes and sizes prepare for the legislative changes in the best possible way.

This guide is the next step and helps answer the most pressing questions people still have regarding the use of their data and email marketing.

It’s important to always remember, we don’t live in a post-GDPR world; we now simply live in a world where GDPR is the norm and staying compliant with the new regulations means every business has to have their house in order. It’s not a case of adopting the mantra ‘set it and forget it,’ GDPR compliance requires constant work.

Businesses are especially worried after, in the summer of 2019, the ICO (Information Commissioner’s Office) handed out fines totalling nearly £300 million to British Airways and Marriott for data protection infringements.
Rather than create yet more fear mongering, both Jarrang and Stephens Scown want to address this issue head-on. We hope Jarrang’s knowledge, insight and expertise on all things email marketing, combined with the legal framework from the Data Protection Team at Stephens Scown, will give you clear, practical and useful advice on everything you need to do to stay compliant with GDPR.

In short, you need to think of GDPR in the same way as you do health and safety – it’s an essential component of running your business and prevention is better than cure. If you ignore GDPR, you do so at your peril and, if you fail to act, you’re sitting on a ticking time bomb, as British Airways and Marriott discovered.

Avoiding fines and reputational damage is relatively straightforward providing you take the necessary steps and work with experts like Jarrang and Stephens Scown to help safeguard your business and reduce your risk of being in breach of GDPR.

If you do have further questions, either on the legal aspects or the email marketing side of it, both the teams at Stephens Scown and Jarrang will be happy to help.

Yours,
Stafford Sumner & Robert Brooks
Jarrang Founder & CEO | Stephens Scown Privacy Officer
Part 1: Unpicking the threads of GDPR & Email Marketing

Let’s focus on the positives first; GDPR is something we’ve welcomed with open arms at Jarrang. It’s forced people to pay more consideration to the email marketing campaigns they send, make them create more engaging content and reduce the amount of unnecessary emails we all receive in our inboxes.

One of the wider benefits it’s brought with it, is forcing people to think harder and smarter about the data they collect for marketing purposes, how they use it and, most importantly from our point of view, why they send email marketing campaigns to their customers.

And getting this ‘why’ right is where we start with everything. Whenever we sit down with new clients we find out why they want to use email marketing, what they want it to achieve, and where they want to be, as a business, in terms of sales, growth or brand awareness.

It’s from here we’re able to help them figure out who their audience is and who buys from them, enabling us to provide better advice, support and strategy. Forcing people to think about this ‘why’ has been one of the biggest benefits to come out of the continued increase in popularity of email marketing.

What’s more, the general public are now much more aware of how and why their data is being used. When this comes complete with clear and transparent consent, it’s a win-win for everyone.

But unfortunately, and thanks in a large part to the maelstrom of noise surrounding GDPR, not everything was plain sailing. Without doubt, the biggest errors we saw were the profusion of ‘re-consent’ emails being sent out by businesses when, in a lot of instances, they weren’t necessary.
Poorly thought out re-consent emails saw customers lose, on average, up to 50% of their subscribers with the figure rising to 90% in the worst cases.

1. Unnecessary use of re-consent emails being sent to already consenting data subjects or data subjects that can be contacted under Legitimate Interests. This resulted in valuable contact lists shrinking in large numbers, when in many cases, they really didn’t need to.

2. Leaving it too long to start the GDPR work when given two years to complete it. Then rushing to create a veneer of compliance, which is unlikely to stand up to scrutiny if there are any issues in the future.

3. Making the consent process too complicated, which resulted in a significant drop-off in the number of subscribers to ongoing marketing communications.

4. Not carrying out a data mapping exercise, and therefore not having a detailed record of data processing, which apart from being best practice, will be essential in the event of a data privacy issue needing resolution.

5. Approaching the GDPR as a standalone entity or box ticking exercise, and not truly understanding the details, therefore leaving the business open to unnecessary risk or fines in the event of a data breach.

6. Stating ‘Legitimate Interests’ as a legal basis for processing without carrying out the written test to evidence ‘why’ certain processing is taking place.

7. Not updating Privacy Notices on websites, which is the first place data subjects are likely to go in relation to a privacy complaint.
If any of this sounds familiar, and there are points mentioned above that you and your business haven’t actioned, then we can’t stress enough the importance of doing so as soon as possible.

On a more positive note, we’ve seen the quality of databases improve (with higher levels of engagement) thanks to GDPR. However, that doesn’t mean GDPR is ‘done.’ The reality is, once businesses have shaken their GDPR hangover, they need to realise staying compliant with GDPR requires constant work and due diligence to be undertaken.

THINK OF THE GDPR IN THE SAME WAY AS YOU DO HEALTH AND SAFETY – IT’S AN ESSENTIAL COMPONENT OF RUNNING YOUR BUSINESS AND PREVENTION IS BETTER THAN CURE.

“"’We’ve seen the quality of databases improve (with higher levels of engagement) thanks to GDPR.

- Jarrang
So where do we start when it comes to data compliance?

The first step is to audit all of the data you hold on the subscribers to your email marketing lists. This means finding out where it’s stored, where it came from, what you use it for and how you use it.

Whether that’s sign ups from your website, transactions from your ecommerce store or email addresses you’ve collected at a trade show, make sure you know what you’ve got and where it came from.

Here’s some guidance to help you:

What data do you hold? This will vary hugely from business to business. It might be you only hold an email address or, equally, you might have detailed profiles for each of your contacts. When you audit your data, make sure you know what data you hold, why you have that data and why you use it. If you hold data you don’t need or is superfluous to requirements, delete it.

Where does this data come from? You should also know where each subscriber to your list comes from and when they joined. Have they signed up through your website? Are they a customer? Did they enter a competition you were running? Did they give you a business card at a trade show or networking event? It’s important you map out every source of your data - and if you’re following best practice guidelines for email marketing you will already know this.

How often do you send emails to your database? Again, for best practice, you should know how frequently you send emails and who they are being sent to.

How engaged is your database? An engaged subscriber is someone who is opening or clicking on your emails, although as a rule of thumb, subscribers who click on links in your emails are more engaged than those who just open them. As best practice, you shouldn’t be sending emails to people who aren’t engaging with you, that’s why at Jarrang we only send to an ‘engaged’ segment - for example to someone who has opened or clicked on an email in a 12 month period and has been a subscriber for longer than 3 months. How this engagement segment is defined will vary from business to business.

For example, if a hotel had a guest two years ago and they stayed once, and their email data was collected legitimately for email marketing purposes and they have been sending to them regularly in that time, but they haven’t opened a single email, they should probably delete them from their database.
The same goes for data they collected over two years ago who haven’t been sent a single email - there’s no way a regular sending pattern can be proved, let alone engagement, and the chances are they won’t be interested anyway.

Robert Brooks, Data Privacy Officer at Stephens Scown, adds: “There is no set time frame under GDPR for removing a contact from your database. Once you have carried out a data audit you can then decide on a series of compliant policies relating to how long you hold customer Personally Identifiable Information (PII). To arrive at this you can look at the transactional history of current customers and measure their purchasing lifecycle. This fits into something called the Privacy by Design concept and the need under GDPR for accurate records of processing.”

How do you manage your lists, including **unsubscribes** and **bounces**? We’ve worked with hundreds of businesses and have seen it all when it comes to list management. Typically, businesses tend to have multiple lists in many different places. You need to know how these lists are managed and how you manage your unsubscribes and bounces in order to be compliant with GDPR. Again, if you already follow best practice guidelines, you should already be doing this.

**IN SUMMARY**

- Carry out an audit on all your data
- Gather all your different ‘pots’ of data into one place
- Establish what data you have and where it comes from
- Confirm the engagement rates of your database
- Have a plan in place for cleaning your data and updating your privacy policies
One common trait we’ve definitely noticed since GDPR came into effect are the number of questions coming from businesses of all shapes and sizes.

Barely a week goes by without a client asking us a question about their data, compliance, and what they should do if things go wrong. Seeing as you’re reading this guide you’re probably no different!

Firstly, you’ll want to know if you’re compliant with GDPR. Secondly, you’ll want to know what you have to do to stay compliant and, thirdly, you’ll want to know how to keep your email marketing effective and delivering results.

With the help of the Data Protection Team at Stephens Scown, we’ve compiled the answers to some of the most common questions we’ve been asked since GDPR became law.

You can find the answers in the following pages but if you do have further questions, either on the legal aspect or the email marketing side of it, both the teams at Stephens Scown and Jarrang will be happy to help.
GDPR COMPLIANCE

WHAT SHOULD BUSINESSES BE DOING IF THEY DIDN’T MAKE “THE DEADLINE”?  

Keep going and don’t let up, May 25th 2018 was the starting line not the finishing post!

WE LOST A LOT OF DATA DURING “RE-CONSENT”. WHAT CAN WE DO TO FIX THAT?  

Short of buying a DeLorean, there isn’t a huge amount you can do.

Consider this though - if they weren’t active clients or customers and they didn’t engage with your content, are they really worth fighting for?

Moving forward, look to build on solid foundations and consider a strong engagement process, making it clear and transparent as to what you intend to do with the data at the point of collection.

Many businesses sent re-consent emails when they did not need to do so, if you received poor advice, you may have a claim against your adviser.
You need to be aware that you can only rely on the “Legitimate Interests” ground under GDPR if you have carried out a written balancing exercise between your legitimate interests as a business and the rights and freedoms of the people you are emailing.

So what this means is, essentially, you can continue sending emails to your existing database and your legacy data, providing:

- You can prove that someone has been a customer in the past (for example you have a transaction date, booking reference or date of last check-out);
- You have been sending to them regularly with an evidenced sending pattern (e.g. once per month);
- They have engaged with your emails or organisation ‘recently’ (eg within the last 2 years);
- You continue to clean your list by removing unsubscribers immediately, regularly removing hard-bounces and contacts who haven’t engaged within a predetermined period of time e.g. 2 years.
- You have carried out a written balancing exercise between your interest and the rights of the people you are emailing, and their rights do not outweigh yours.

For example, take a customer who purchased something from you two years ago. During that transaction you collected their email address, and you have since emailed them once a month, with the last email they opened being two months ago. In this case it’s fine for you to continue emailing them. However, Legitimate Interest isn’t as simple as thinking “this is totally reasonable; therefore it is totally legitimate.”

We saved most of our database using Legitimate Interest, but we didn’t do a balancing test. What is this and how do we do it?
You’re required to **carry out an assessment** and it would be prudent to document it. A Legitimate Interest Assessment comprises a 3-stage test:

1. **Identify** your Legitimate Interest. For example, you could say: “We believe it is a legitimate interest to send marketing material via email to previous customers about the same product or service to encourage them to buy with us again in the future.”

2. Carry out a **Necessity Test** – consider whether the processing of Personal Data is “necessary” for the pursuit of your objectives. For example, your reasoning could be: “It is necessary for us to do this as a business in order to make repeat sales.”

3. Carry out a **Balancing Test** – you can only rely on Legitimate Interest where the rights and freedoms of the individual whose Personal Data will be processed have been evaluated AND these interests do not override the Controllers’ Legitimate Interest. For example: “We made it clear that the data subject will receive regular marketing from us at the point of capture, we only send communications about similar products or services, and we will unsubscribe them immediately if they ask us to do so. With this in mind, we think this is an equally balanced decision.”

You should also have a policy detailing when and how a **Legitimate Interest** test should be run.

**Stephens Scown** can provide guidance and templates to assist with this process.
WHAT IS A GDPR FILE? WHAT SHOULD IT HAVE IN IT? WE HAVE NOTHING.

This goes by many names; it simply means a single location where all of your decision making records and compliance documents are stored. Your GDPR file should contain explicit provisions about documenting your processing activities, including processing purposes, and data sharing.

It can be as simple as a folder with a different sheet of paper for each topic, signed and dated as to when the decision was made and why. In the event of an issue, the ICO who police GDPR will want to see this.

I'M A LEGITIMATE BUSINESS AND DON'T INTEND DOING ANYTHING UNTOWARD WITH MY CLIENTS' DATA. WHAT'S THE WORST THAT IS LIKELY TO HAPPEN TO ME IF I HAVE A BREACH OR A COMPLAINT?

Providing you have put in the time and effort needed to have policies and processes in place to deal with these issues – and still make errors (all human) – you will be able to mitigate some of the repercussions from the ICO. If you cannot show that this work has been done, then you run a high risk of meeting the full force of the commissioner. The worst might be a large fine and loss of good name.

HOW OFTEN DO I NEED TO SEND CAMPAIGNS FOR IT TO CLASS AS A 'REGULAR SENDING PATTERN'?

This will depend on your business. Some send emails to their database once a week, others every day, and some only once a month. The key here is having a regular sending pattern, planned and documented in an email marketing schedule, so you can prove you’re using the data you store in the way you said you would and giving your customers the best opportunities to engage with you.

WHAT IF SOMEONE ASKS TO BE REMOVED FROM MY DATABASE, WHAT STEPS DO I NEED TO TAKE?

Firstly, understand on what basis you are processing the data, if the basis is Consent or Legitimate Interests then you must act on the request.

The ICO states that - If a valid erasure request is received and no exemption applies then you will have to take steps to ensure erasure from backup systems as well as live systems. Those steps will depend on your particular circumstances, your retention schedule (particularly in the context of its backups), and the technical mechanisms that are available to you.

You must be absolutely clear with individuals as to what will happen to their data when their erasure request is fulfilled, including in respect of backup systems.

It may be that the erasure request can be instantly fulfilled in respect of live systems, but that the data will remain within the backup environment for a certain period of time until it is overwritten.

You may also have to inform others that you have shared data with.

If they simply want to opt-out of emails (instead of requesting a full erasure of their data) and haven’t used the link in your marketing, do this for them quickly and efficiently, and confirm that they have been permanently unsubscribed from your email marketing database.
IS IT IMPORTANT THAT I KNOW WHERE MY SERVERS THAT HOLD MY EMAIL DATABASES ARE LOCATED? BE IT IN OUR OUTSIDE OF THE EEA?

Yes, very important. You will be in breach of the Act if you do not know where your databases are, especially if they turn out to be outside the EEA, or in a country that does not have a legal agreement with the UK for the equivalent data privacy rights. You should look at your email marketing platform, such as Mailchimp, as well as cloud based locations where you might store other databases or back ups, such as Google Drive or Amazon Web Services. Write them down, check their compliance and put it in your file.

IF AN EMAIL RECIPIENT TELLS ME THEY HAVE THE ‘RIGHT TO BE FORGOTTEN’ WHAT DO I SAY/DO?

First, establish on what grounds the individual is being contacted on. If you are relying on Consent or Legitimate Interests (and there is no overriding legitimate interest to continue - as is sometimes the case in medical professions), or if you are processing for direct marketing and the subject has objected to this, then you must delete their data.

You will also need to take steps to ensure the data is removed from your backup systems as well as your live systems. You must inform the data subject making the request what will happen to their data when the request is completed. You have up to one month to complete this action. Again, it’s best to have a form and process pre-prepared in your file so you can act swiftly if this were to happen.
WHAT DO I NEED TO CONSIDER WHEN COLLECTING DATA AND REBUILDING MY LIST MOVING FORWARDS?

This is a big question and one lots of you have asked us about so we’ve broken it into a number of parts for you.

You must approach this scenario from the starting point that privacy is paramount from the outset and that any process decided upon is done so having first completed something called a Privacy Impact Assessment (PIA).

The PIA will help you prove that the data has been collected in a way that is fair. This means that you are then unlikely to have processed the data in a way that is unduly detrimental, unexpected or misleading to the individuals concerned. This of course assumes that you have made your decisions appropriately, in accordance with the GDPR.

If you’re generating the list content through your own website, events or checkout system, the data collection must be transparent and fair, with links to your compliant Privacy Information. You should make it clear that you intend to use their details for marketing purposes. The best way to get clear consent for your marketing is to provide opt-in boxes that specify the type of messages you plan to send, however you may be able to use the legal basis of Legitimate Interest for customers (see next question about customers).

SO WHAT DOES THIS MEAN FOR PRIZE DRAWS & COMPETITION?

If running prize draws or competitions, providing free content to download, or wifi access in return for data that will be used for marketing purposes (as many businesses have done before), you will need to ask for Consent before you do so.

The ICO frowns upon automatic submission to marketing databases and believes data subjects should have the right to access any material being offered, without having to give their data in return.

If you’re running a joint competition with an affinity marketing partner for example, you must use a tick box to get consent for each party involved who wants to use the data for their own marketing purposes. Joint consent covering multiple parties is not acceptable.

HOW DOES IT IMPACT WEBSITE SIGN UPS TO ENews?

With regards to enews subscription boxes on the website, it’s acceptable to simply ask the data subject to enter their email address and click submit, as this passes the ICO requirement that a ‘positive action’ needs to be taken to give Consent (and they wouldn’t enter their own email address in the box unless they wanted to hear from you). For added peace of mind, make it clear at this point what they will receive and how frequently.
CAN WE USE ‘FORWARD TO A FRIEND’ AS A WAY OF REBUILDING OUR DATABASE?

To clarify, using the frowned upon “Forward to a Friend” mechanism as a way to get your subscribers to build your database by adding the names of their friends to your data capture platform in return for them being in with a chance to gain some kind of incentive is not a compliant method for database gathering. Consent should be given by the data subject themselves and it should be clear what will happen as a result of sharing their own data with you.

CAN WE STILL BUY IN DATA?

It is neither best practice, nor likely to be legally compliant to purchase databases for email marketing purposes, be that for B2B or B2C purposes. Build your databases organically and get the necessary permissions to market to them directly, not via a generic list building company who sells their data to multiple businesses like yours.

WHAT OTHER WAYS ARE THERE FOR US TO GROW OUR DATABASE?

Build your database by using data capture forms and optimised landing pages to gather information from people who are interested in hearing from you. You can drive traffic to these pages from different sources such as social media, paid search advertisements or offline advertising.

Once the data has been captured and the necessary consents given, capitalise on this moment by sending them an automatic, branded email at point of submission, and consider sending a series of ‘welcome’ emails as part of an automated journey to ‘nurture’ your new found prospect and encourage them to engage with you further. Remember, it’s quality not quantity when it comes down to the new era of email marketing in a GDPR world.
Data collection

CAN WE AUTOMATICALLY COLLECT ANY CUSTOMERS’ DATA FOR EMAIL MARKETING PURPOSES WHEN PURCHASING/BOOKING?

Yes, but the following conditions must be met:

- You have obtained the contact details in the course of a sale (or negotiations of a sale) of a product or service;
- You are only marketing your own similar products and services;
- You provided a simple opportunity to refuse or opt-out of the marketing, when you first collected the contact details and in every subsequent communication.

This exemption from consent is known as “soft opt-in”. You must provide links to your Privacy Notice and details of how to opt-out.

DO WE NEED A TICK-BOX FOR CONSENT FOR EVERY BUYER IN OUR ECOMMERCE STORE?

In the case of a buyer, you may be able to rely on Legitimate Interests for contacting the customers post-purchase but it must be for related purposes and you must provide the usual opt-outs. And the written test mentioned earlier must be recorded.

If it is not for a buyer, or you need to use the legal basis of Consent. This requires clear and positive action – tick-box is best but, as in the answer above, in the case of an enews subscription box on a website, entry of the email address and a ‘positive action’ for submission will suffice.

Pre-ticked boxes or non-action to get Consent (which is different to Legitimate Interest) is frowned upon.

WHAT WORDING DO WE NEED TO HAVE ON OUR DATA COLLECTION CARDS OR IPAD LANDING PAGES WHEN AT A SHOW, EXHIBITION OR ON THE SHOP-FLOOR?

It’s all about transparency. As long as the data subject understands why the data is being collected and has a clear idea about what it is going to be used for.

An example of this could be:

“I would love Jarrang to keep in touch with me and understand that I’ll get an email roughly once a month with news, views and insights about email marketing”

Always provide the address or link to your privacy notice.
WHAT IF WE CAPTURED DATA AT A TRADE SHOW, AND THE DATA IS FROM A COMPANY, CAN WE STILL USE IT?

Yes, as long as the information you provided to the data subject at the time was clear regarding the future use of this data.

Remember, when marketing electronically to sole traders, partnerships, unincorporated trusts, partnerships and foundations and their staff members they have the same protections as a consumer under both GDPR and the regulations of PECR* and therefore you may need consent.

Marketing to staff members of limited companies, public limited companies, incorporated partnerships, trusts and foundations, local authority and government institutions is exempt from these protections (PECR) but subject to GDPR, for these you may be able to use Legitimate Interest as the legal basis for electronic marketing because PECR does not apply. We must carry out the written tests and balancing tests as described earlier which will help you to decide if it’s possible to email them without specific Consent.

*PECR - Privacy and Electronic Communications Regulations.
WHAT SHOULD WE DO IF THINGS GO WRONG?

The first thing to do is not to panic! It’s incredibly important to have processes and procedures in place to follow if something goes wrong - like accidentally sending an email marketing campaign to people who you don’t have permission to contact.

Robert Brooks, Data Protection Specialist and Privacy Officer from Stephens Scown, says: “Where we’ve assisted clients and notified the ICO of potential issues, and the client has the right systems and procedures in place - especially where we act as their virtual data protection officer - because they’ve done the training and reacted in a swift manner, there’s nothing the ICO could really do apart from say it came down to human error and they’re not in the business of lining people up against the wall.”

“So far they’ve been taking a fairly pragmatic view of it. Where correct elements have been in place there’s been no prosecutions and very little has come of it other than a few action points to take.”
IN SUMMARY...

If you haven’t done so already, you should carry out an audit of all your data so you know what information you hold, where it comes from and how you use it.

Make sure you have a GDPR ‘file’ and, if you’re using Legitimate Interests as your basis for communicating with people, make sure you have carried out a Legitimate Interests Assessment (LIA) and documented it.

If you have done the above, you can continue to email existing contacts in your database providing they have been a previous customer, you have been sending emails to them regularly with a regular pattern, they have been given a clear opportunity to opt-out and they have engaged with your emails within the last two years.

Your website should ideally include data capture points where consent for you to communicate with the data subject is given with a clear and positive action.

In a Business-To-Business setting, suspects or expired prospects should be removed from your database and you should no longer communicate with them through email marketing until such a time as they give you consent to do so through new communications initiated by them. People who you have met and collected their data in the course of that meeting, and you’ve been communicating with since, can still be contacted in most cases.

Your email marketing focus should be on creating quality email marketing campaigns and programmes rather than on the size of your list and the number of emails you send.
As far as the future goes, email marketing is stronger than ever and, when it’s done right, it can be one of the most powerful marketing channels out there to deliver results.

As noted by Adobe in their 2018 Email Stats: “Since email continues to reign as one of the most important communications investments a brand can make, it pays to get it right. You can’t just avoid the sins, you also have to deliver. According to the survey, top wishes amongst the survey takers are emails that are less promotional and more informational (a priority for 37%) and emails that are personalised to the recipient’s interests (a must for 27%).”

The good news is this goes hand in hand with GDPR forcing all of us to send better emails. Our databases now should be full of people who we know want to hear from us or are previous customers.

On the whole, databases have got smaller after the data-cleansing triggered by GDPR and this has made organisations think about the best ways to use them, rather than relying on the volume of emails they send.

Attention is now turning to retention of databases and the use of the promotional or re-engagement style emails are more important now than ever before to keep subscribers engaged and interested in our products and services.

These refreshed, cleansed and profiled databases can now be used to serve up more targeted messaging to subscribers. For example, the targeting of several different groups by displaying different content that’s most relevant to them and most likely to get them engaging with you in the future.

Additionally, in relation to the smaller databases we’re seeing since May 25th 2018, there is the continued re-education we at Jarrang play a part in, where we help people to understand a higher quality, smaller database of engaged recipients is more valuable than a larger database of inactive non-openers.

This message is starting to get through as businesses start to see improved open and click through rates on campaigns since the GDPR cleansing, using their more engaged databases continually. This is likely to lead to a re-assessing of what a ‘good open rate’ is and what metrics we really care about when measuring the impact of an email marketing campaign.
IF YOU’RE NOT DOING SO ALREADY YOU SHOULD

• Use a master list (rather than lots of different, smaller lists) to manage all your email marketing data, making sure you are suppressing unsubscribed and non-compliant contacts, and tagging the different groups to which they might belong for future targeted messaging.

• Only collect data from your contacts that will help you send better email marketing campaigns to them. Cut your risk in the event of a data breach by collecting only the fields you need to execute the email marketing. Do you really need their full name and date of birth?

• Remove contacts from your database who aren’t engaging with your content. Set yourself a policy and stick to it. For example, if someone hasn’t engaged with you (bought something or opened an email) for the last two years, is it worth keeping them and is it legally compliant? If not, set a process to automatically delete them.

In short, email is in a position of great strength and these are exciting times for the industry. However, there is still that ticking time bomb to consider for those who haven’t acted yet. Those who ignore GDPR do so at their peril because, once the ICO have caught up with their workload, the fines will inevitably follow.
Thankfully, avoiding them is relatively straightforward providing you take the necessary steps. So what are the 6 things you NEED to know to avoid prosecution in a GDPR world?

HERE’S WHAT STEPHENS SCOWN SAY:

1. The personal information that makes up your data belongs to the data subject, it belongs to them, treat it with respect.
2. Have the correct policies and procedures in place and ensure all employees and suppliers have understood them.
3. Test your reporting process in the event of a problem (e.g. internal breach escalation and subject access requests).
4. Understand when you need to report matters to the ICO.
5. Make sure your security is sufficient and tested.
6. Train your staff to understand and identify data risks.

This concludes our guide to ensuring your email marketing stays compliant with GDPR. Our Mission is to help you send better email marketing campaigns and to make sure they are a catalyst for fuelling the growth of your business.

NEXT STEPS

This guide is only looking at GDPR in relation to email marketing and does not set out to look at the wider reaches of the law, if you want specific legal advice for your own circumstances, or you would like to find out more about their Virtual DPO services, you should contact Stephens Scown at ip.it@stephens-scown.co.uk to talk to their Data Protection Team.

If you would like support with your email marketing programme or to find out more about our database management services and how to implement the policies described above, please get in touch with Jarrang at hello@jarrang.com and our team will be happy to help.
Jarrang has been deploying email marketing programmes for businesses around the world since 2003. With expertise in email marketing design, code, content, database management and analysis, it makes them true experts in their field.

jarrang.com
hello@jarrang.com
0203 597 4975

With 270 staff and 50 partners across three offices in Exeter, Truro and St Austell, Stephens Scown is a law firm with a regional focus but all the benefits of a big city rival.

stephens-scown.co.uk
enquiries@stephens-scown.co.uk
0345 450 5558