GDPR - Tidying up your data

A reflection on some of the points I have been considering while working on my and my client's data protection compliance

Sayers Solutions

May 2018

Contents

GDPR and what it means for small businesses

If you're a business owner or work for a business that handles any kind of customer data, then you've probably heard the term GDPR floating around recently. But what exactly is GDPR and what will it mean for your business when it's introduced from 25th May 2018?

As a business owner myself, GDPR has been on my radar (and my ever-growing to-do list) for the past year. I know first-hand how hard it is to dedicate time – valuable time that could be spent serving my clients or finding new ones – to keep up-to-date with this stuff. But it is important. That's why, as I've been learning about GDPR and understanding what it means for Sayers Solutions, I've collected my learnings and thoughts to share in this whitepaper.

I have always been mindful of the ethical collection and storage of data, and with GDPR being the biggest change to the data protection law in over 20 years, I was keen to get to grips with it. To date I have organised two seminar sessions and attended several others. I've written this whitepaper after reflecting on these sessions as well as my experience of implementing audits and data mapping with clients and for Sayers Solutions.

I hope the information helps you to manage your data compliance without hindering the day-to-day running of your business, as well as offering some useful recommendations for you to implement.

This whitepaper is by no means a complete review of GDPR nor an inclusive recommendation on how a business would become compliant. That information is available on the Information Commissioner's Office website (www.ico.org.uk). Instead it is intended as a conversation starter and a prompt of the main points you need to consider to help you prepare for the introduction of GDPR.

So, let's get started.

What is GDPR?

GDPR stands for General Data Protection Regulation and will replace our current data protection laws from 25th May 2018 to strengthen citizens' privacy rights within the EU. It is the biggest change to our data protection laws for over 20 years and penalties for not complying can be severe.

As a business you will need to evidence compliance and have procedures in place to show that you have considered and been careful with the data you hold. You will need to consider:

- where the data came from
- the reason for processing the data
- how long you want to keep the data.

However, you will also need to manage a 'do not contact' list and consider the notion of 'do no harm'.

In this paper, I hope to expand on these points by covering:

- what is meant by the ‘lead source’
- valid lawful reasons for processing data
- why you need to consider how long to keep data for
- the benefits of managing a ‘do not contact’ list
- and the notion of ‘do no harm’.

GDPR - lead source and evidence

Lead source

To manage your data in line with GDPR, 'lead source' should be a field in your database to focus on. It should indicate where you got that data from or how that contact became known to you. For example; subscribed to your mailing list, has bought your products/services, met at networking event etc. I recommend that this field is multi-field, as you generally come into contact with a number of people from the same organisation and perhaps have a variety of different initial interactions.

Evidence

It is also good practice to keep evidence of how that contact became known to you (i.e. business card, email, public record etc).

So, it's always a good idea to:

- take a digital copy of contacts' business cards after networking events
- save a copy of the email showing they wish to be added to your mailing list
- record the conversation
    - not necessarily a voice recording but add notes to the conversation history in your CRM system, providing that normal and truthful records are kept up-to-date. This should not be abused to override the system and good habits should always be applied.
- keep diary entries showing events and meetings attended with perhaps the delegate list.

If you don't currently use a CRM (customer relationship management) system, think about the other data your business keeps. For example, bookkeeping systems, spreadsheets, phone book etc, and implement a way of recording the lead source in those systems. No matter what system, the lead source of your data should always be noted and updated. Especially when moving it from one system to another – potentially including the date in the title, if not controlled by its own field.

GDPR – valid reasons for processing data

Valid reasons for processing data

In short, GDPR is being introduced to increase protection of personal data – any information that identifies a person. However, it also demands that you have a valid reason for processing that personal data in the first place.

The Information Commissioner's Office website states, "You must have a valid lawful basis in order to process personal data", and goes onto explain what the six lawful bases for processing personal data are:

- Consent
- Contract
- Legal obligation
- Vital interests
- Public tasks
- Legitimate interests

I'm not going to talk about each term here but I thoroughly recommend you check out the ICO website which offers an excellent 'At a Glance' section for each legal basis. Visit: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/

But let's take a closer look at 'Consent'. We've all heard about consent. You tick a box and give permission blah blah blah. But do you ever wonder what exactly you are giving permission for? With GDPR, organisations now need to make sure 'permission' is transparent and granular.

This means:

- making your request for consent prominent and separate from your terms and conditions
- asking people to positively opt in and not using pre-ticked boxes
- using clear, plain language that is easy to understand
- specifying why you want the data and what you will do with it
- clearly naming your organisation and any third-party controllers who will be relying on the consent
- reassuring individuals they can withdraw their consent
- not making consent a precondition of a service
- and offering separate sign-up to separate offerings (vague and blanket catch-all is not acceptable).

This information has been taken from the ICO website which provides a checklist to use when you are asking for consent. It's a great resource for ensuring you are compliant. Check it out at: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/consent/

Consent is an important legal basis for me. As a small business owner, I am keen to nurture the contacts and relationships I have made through keeping in touch by email. But what will GDPR mean for email marketing?

As a marketer, you should be aware of the PECR and ePrivacy regulation. The Direct Marketing Association (DMA) explain how PECR/ePrivacy and DPA/GDPR work together for email marketing:

"Under PECR and ePrivacy you need consent or an existing customer relationship to send email marketing. If you want to make your emails more timely, targeted and tailored to the individual, you need data: Demographics, preference, purchases, browsing behaviour, location and device information. All this extra information can help make email more relevant and valuable but data protection regulations (DPA and GDPR) require you to have a legal basis for this. This is to ensure what you do is fair, transparent, not excessive, and to make sure you look after the data you collect, store and use. And for that you need consent or "legitimate interest."

Source: https://dma.org.uk/article/gdpr-consent-or-legitimate-interest-email-marketers-need-both

We've covered consent but what is meant by the lawful basis 'legitimate interest'?

Legitimate interest could be interpreted as a catch-all basis for data processing. As explained by the ICO website, it "is the most flexible lawful basis for processing, but you cannot assume it will always be the most appropriate".

It goes onto explain:

"It is likely to be most appropriate where you use people's data in ways they would reasonably expect and which have a minimal privacy impact, or where there is a compelling justification for the processing.

If you choose to rely on legitimate interests, you are taking on extra responsibility for considering and protecting people's rights and interests."

Source: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/legitimate-interests/

As the most flexible of the lawful bases for processing data, legitimate interests could be seen as the general fall-back option. However, the introduction of GDPR means it is now relevant to flip and focus on the data subject. It is their rights that GDPR is helping us protect. If I think about my personal data and how I'd like it to be safe and also have the right to request erasure, then GDPR is certainly something to celebrate.

GDPR – how long to keep data for

How long should you keep data for?

So far, I have covered documenting and evidencing where your data came from and making sure you have a valid reason for processing data. But you also need to think about how long you keep the data for.

So how long should you keep personal data? To answer simply – as long as you met a valid lawful basis for processing the data – you should keep it for only as long as it is still beneficial to both your business and the data subject. A clean database of people that connect and interact with your business, as in life, is much more productive than 'throwing up' on them on a regular basis. Also, GDPR requires you to keep the data you store secure. You'll probably agree that it is not efficient to spend time and resource on securing data that is of no use to you. Better to delete it and maintain a cleaner and more useful database.

At Sayers Solutions, I advise my clients to regularly audit the data they have processed. This is fairly easy to do by using, or adding, the "date created" field in their CRM system and having another field automatically populate a future date to prompt them to review the data. To review the data, it should be assessed alongside information in the "lead source" and "reason for processing" fields to determine if the data is still relevant to either their business or the data subject. If the answer is no – my advice is to delete it to maintain a clean and relevant database of contacts.

GDPR and managing a 'do not contact' list

What is a 'do not contact' list?

Before making business communications you should always refer to your 'do not contact' list. A 'do not contact list' contains people that opted not to be contacted by you or unsubscribed from your mailing list, as well as people you have opted not to contact (for example clients you don't wish to work with again, people that have failed credit checks or perhaps someone with a conflict of interest).

I find that the 'do not contact' list is one of the trickier parts of compliance. The risk of having records on your system noted 'do not contact', increases the risk of accidental human error – I am sure we've all taken that phone call or seen an email list after the campaign has gone out and noticed someone you didn't want to connect with.

As a business owner, you also need to think about the consequence of a disgruntled employee taking a copy of the list for themselves. Or any of your data for that matter … but that's another subject I don't intend to tackle here.

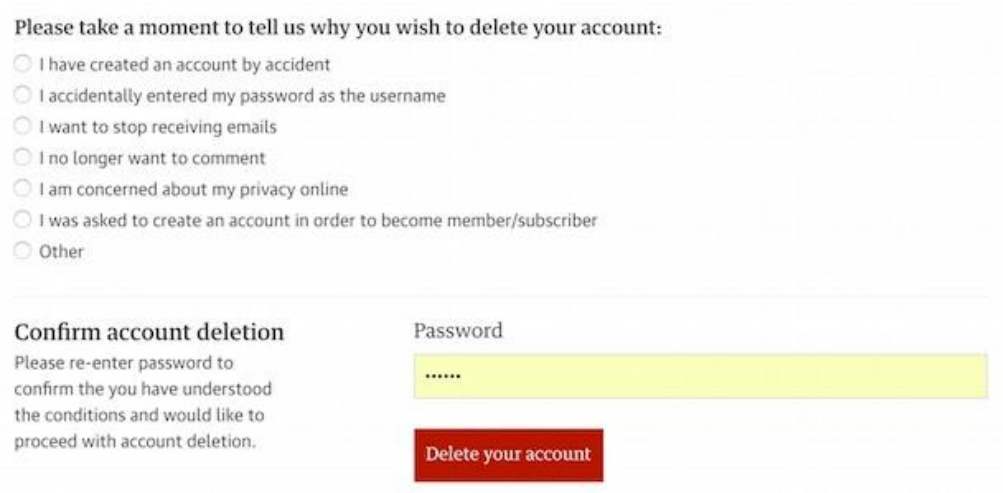
But to ensure that you do not repeatedly contact people that do not want to be contacted, and to comply with GDPR, it is recommended that you manage a 'do not contact' list.

Under GDPR, it will now be necessary for the reason the organisation is processing data to be transparent and granular. This means letting the data subject know exactly what they are subscribing to and getting specific consent for specific things (vague or blanket consent will now not be enough).

Email marketing services, like Mailchimp, manage your email lists and do not let communications be sent to those who have unsubscribed from your mailing list. Also, email services like this do not let you send emails out without the 'unsubscribe' link included. If someone clicks this link, they will be unsubscribed from your mailing list, and future emails through that email service will not be sent to them.

However, it would be ideal to also offer 'unsubscribers' the ability to review their preferences for how their data is processed by your company. When someone unsubscribes from your mailing list it might not mean they don't want to 'buy' from you in the future or don't want you to contact them again. They might just want to vary the frequency or types of communication. It's therefore a good idea to outline what unsubscribing means and offer a way of updating their preferences and choose what they do want to continue to receive from you.

A good example was noted in the article on eConsultancy (2017) that demonstrated the Guardian's efforts to allow users the right to erasure: "When you do this from within your account settings, there's lots of clear information about how it will affect everything from the comments you have made to any paid subscriptions you have in place."



Further to unsubscribing, there is the request for erasure, where the data subject can request for their data to be deleted. And this is the tricky bit – well at least in my head at the moment – you must also have a record of the deleted record.

Of course, when there is a contractual obligation, the data subject does not always have the right of erasure. If you think you want to give this further thought, I would suggest you check your contract and seek legal guidance.

Email marketing services also have the ability to bulk unsubscribe individuals as well as subscribe. Before sending a mailshot, the 'do not contact' list should be uploaded, which will remove contacts that don't want to be contacted from your mailing list, before the email campaign is sent.

Another way that businesses can keep their data tidy is to securely delete unnecessary data, including those spreadsheets that are exported from systems; to be filtered and drilled for information and reports, potentially imported into other systems, but then go out of date. At Sayers Solutions I recommend to clients that they at least make sure they delete the personal identifiable data elements that are not necessary.

To enable you to do this, I suggest that when you export and save files, make sure you add or change the date of the file, i.e. 01042018. Similarly, I would recommend you date stamp business cards and other permission slips. At Sayers Solutions, I suggest that you write on the card when and where you met the person – maybe marking whether and why you might want to contact them – and then mark where you have uploaded the data to.

GDPR and do no harm

So far, I have talked about lead source, valid reasons for processing data and how long to keep data, and the benefits of managing a do not contact list. Another interesting topic when thinking about GDPR, is the element of 'do no harm'. Which I guess is what prosecution will depend on. Are you doing harm to the individual by keeping or acting on the information that you keep?

The interesting element here is that this includes receiving nuisance phone calls and emails. Are you harming someone by potentially wasting their time by making them answer calls and delete emails? This is an aspect that I think small businesses need to be most mindful of.

"As the Data Protection Network points out, 'organisations will still need to ensure they can establish necessity and balance their interests with the interests of those receiving the direct marketing communications'.

That means a post every week could be hard to justify, but quarterly mail to let users know about charity work may seem to be more balanced."

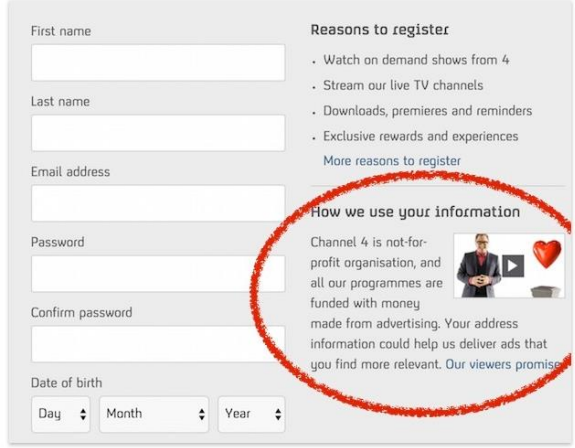
(Econsultancy, July 2017)

Source: https://www.econsultancy.com/blog/69253-gdpr-10-examples-of-best-practice-ux-for-obtaining-marketing-consent

This reinforces my point that it is important to be interacting with an engaged following.

The eConsultancy (2017) article also uses Channel 4 as a best practise example for providing clarity for subscribers on what they are signing up to. In 2012, the broadcaster used a video campaign to prepare viewers for compulsory registration.

"When registering for a Channel 4 account on the All 4 website, you can see Alan Carr featured on the right hand side and a link to the video ('Our viewers promise'). There's a clear heading – 'how we use your information' – and the text mentions tailored advertising, and sits underneath copy detailing 'reasons to register'." (eConsultancy, 2017)



To help manage your engaged subscribers and tidy your databases, at Sayers Solutions I recommend to clients to have an automatically generated date, based on the "created" date, "reason for processing" and further engagement for the gradual deletion of data for direct marketing.

It is good practice to review and take into account whether people are opening your emails and identify those who have not done so in the last year, per say. Sayers Solutions recommends sending them an email asking if they still want to be on your mailing list and offer the chance to "re-subscribe" to stay in touch.

Sayers Solutions then recommends moving 'those that do not re-subscribe' from the "prospect" to "not opened in one-year" list.

You might want to go further and look at those on your mailing list who have, say, not 'clicked' in the last three months. The frequency of the reviews completely depends on your company, as well as the type and frequency of the communications that are sent, as well as industry standards.

Sayers Solutions recommends that you then reduce the frequency of the emails sent to these lists, with only critical or extremely interesting information being sent, along with an annual reminder email; letting them know they can re-subscribe to your more regular communications.

Sayers Solutions also recommends setting a time limit, maybe three years, for them to re-subscribe to your newsletter, after which you can finally make the decision to delete the data.

The theory goes, if they miss your messages, then they will re-subscribe, or they will find you through your other marketing techniques.

Updating your lists through this filtering process will help provide a more manageable way to control your data and will ensure that you are communicating with an engaged audience.

GDPR - Summary of best practice for small businesses

By writing this whitepaper, I'm aiming to help small businesses understand what the introduction of GDPR will mean for them and also share tips and advice I've found useful for my own business, Sayers Solutions.

I have written this paper to reflect on some of the areas that will impact businesses, offering tips and advice that will help to implement best practice when managing data, in particular when executing marketing activity.

The paper has covered:

- what is meant by the 'lead source'
- valid lawful reasons for processing data
- why you need to consider how long to keep data for
- the benefits of managing a 'do not contact' list
- and the notion of 'do no harm'.

I hope the information helps you to manage your data compliance without hindering the day-to-day running of your business, as well as offer some useful recommendations for you to implement.

The paper is by no means a complete review of GDPR nor an inclusive recommendation on how a business would become compliant. That information is available on the Information Commissioner's Office website (www.ico.org.uk). Instead they are intended as a conversation starter and a prompt of the main points you need to consider to help you prepare for the introduction of GDPR.

Useful resources to download

Checklist – Points to consider when approaching marketing data under GDPR
GDPR – Types of contacts

Want to know more?

If you would like to discuss your GDPR compliance, or any other marketing activity, then please get in touch. Sayers Solutions are well connected with experts on this matter and would love to help support your business.

If you want to arrange a conversation, we can chat over the phone or potentially skype. Give me a ring **(Merewyn Sayers – 07790705223)** during reasonable business hours (yours might be more generous than mine, so please don't ring too early! #SchoolRunMum).

If you are in the Huddersfield/Wakefield/Leeds area let's arrange to meet to discuss this or your marketing activity further.

Or email me through the website contact form http://www.sayerssolutions.co.uk/contact-me/

Like what you've seen?

If you've found this whitepaper useful and want to receive carefully crafted advice and support tailored to small businesses please join our mailing list: http://eepurl.com/dp5eQz