Clayden | Law

How to write a GDPR compliance 'white paper' as marketing collateral

What do we mean by a 'white paper'?

A white paper is an information document used by businesses to inform customers about an issue relevant to their business and present their perspective on that issue, with a view to encouraging customers and potential customers to learn more about and/or purchase their products and services.

As many businesses are (or should be!) assessing their current data processing practices and making any necessary changes to ensure they are compliant with the GDPR by 25 May 2018, and with cyberattacks and personal data security breaches increasingly in the news, the issue of your GDPR compliance, and in particular the security measures your business uses to protect personal data, is a fitting topic for a timely white paper.

Your customers will also have their own GDPR compliance in mind when deciding whether or not to buy your products and services, particularly where the provision of your products or services will involve you processing personal data on their behalf (i.e. where you are a "processor" on behalf of your customers, who are "controllers"). Under Art 28(1) GDPR, controllers must only use processors who sufficiently guarantee that they implement measures to ensure that processing complies with the GDPR; and under Art 82 GDPR, controllers can be held jointly liable with processors for damages arising from processing in certain circumstances. In short, controllers will be fully liable for any damage caused by non-compliant processing unless they can prove that they were not in any way responsible for the event giving rise to the damage. Savvy customers will therefore want to know as much as possible upfront about your data processing practices and GDPR compliance before deciding to buy.

If you're in the business of selling products or services that involve you processing personal data on behalf of your customers, a GDPR compliance white paper that informs your customers about that processing could be used as a sales and marketing tool.

We've been helping some of our clients write these documents, and explain in this article why and how to write them.

Why is it a good idea to prepare a GDPR compliance white paper?

There are several advantages in doing this:

It's good marketing collateral: A well-written GDPR white paper can be used to demonstrate to your customers and potential customers:

- that you are aware of and understand the GDPR's relevance and requirements for your business;
- that you have a strong handle on the type of personal data that are processed by your business and how and why it processes those personal data;
- how your processing of personal data and related technical and organisational practices comply with the GDPR's requirements, particularly in relation to your security measures and credentials;
- that by buying your products or services, their own GDPR compliance will not be effected negatively – or better still, that your products or services might even assist with their own GDPR compliance.

Usually customers don't know how businesses process personal data in connection with the provision of their products or services, or what data processing terms they offer, until they see the standard contract/terms and conditions for the first time – if indeed that document actually contains any suitable data processing provisions.

Customers also want to know whether they can trust businesses to protect the personal data processed on their behalf by implementing appropriate security measures (as required by the "integrity and confidentiality" principle and security provisions of the GDPR). A GDPR compliance white paper is an opportunity to demonstrate and even promote your information security practices and credentials, helping to build customer confidence in this area.

By making relevant information easily available to customers upfront, it will be easier to persuade customers that you are on top of your GDPR compliance and willing to be transparent about your processing, that they can trust you to process personal data lawfully and securely, and that it won't be an uphill struggle agreeing satisfactory data processing terms with you.

It could help you prepare your GDPR-compliant records: In order to write a GDPR compliance white paper, first you'll need to understand how your business collects, stores, uses and transfers personal data on behalf of its customers. Unless your business has already gathered all this information and conveniently documented it in one place, this is likely to involve carrying out a 'data mapping exercise' to discover and record it. As discussed in our previous blog http://www.claydenlaw.co.uk/site/library/clayden-law-news/getting-ready-for-gdpr, the outputs from a data mapping exercise should enable you to build up the records of your processing activities required under Art 30 GDPR. By doing what's necessary to prepare a GDPR compliance white paper, you might also find you've got everything you need to prepare your GDPR-compliant records.

And if you already have all the relevant information to hand and put your GDPR-compliant records together, producing a GDPR compliance white paper is an opportunity to capitalise on the work you've already done by turning it into something that has marketing value.

It could be helpful in contract negotiations: Once a customer has decided to buy your products or services, getting to the point of contract signing can still be a protracted and difficult process. The data processing provisions of a contract can be subject to particular scrutiny, particularly where the customer (or their lawyers!) are data protection law-savvy. If Customers have access to a GDPR compliance white paper, they will already have an idea of what your processing terms will/should cover and understand those terms in light of the 'bigger picture' of your processing and related technical and organisational practices. The information included in the white paper should also help you write suitable data processing terms into your standard contract/terms and conditions that accurately reflect your practices and are likely to be more readily accepted by your clients.

What information should a GDPR compliance white paper include?

The type of information to include in a GDPR compliance white paper will vary depending on the type of products and services you sell and the nature and scope of the processing you carry out on behalf of your customers in connection with them. However, you could include information about:

- types of personal data that you process: think about this in wide terms as in the GDPR – not just names, email addresses and dates of birth, but things like photographs, ID numbers, location data, physical data, online identifiers (e.g. IP addresses/cookie identifiers), genetic information and information about a person's economic, social and cultural identity. Then consider whether any of it falls within the "special categories" under the GDPR (known as "sensitive personal data" under current law) – such as data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic and biometric data processed for the purpose of identifying people, data concerning a person's health, sex life or sexual orientation.
- Purposes of your processing: the general purpose will usually be to provide the products or services requested by your customers, but different types of personal data might be processed for different purposes.
- Practicalities of processing: what do you do with it in factual terms? To what extent is it automated or manual?
- Storage: where you store it geographically and whether anyone else is involved – such as cloud hosting / server providers.
- Deletion: how long you store personal data for, any automatic deletion/archive procedures, whether customers can choose/direct deletion periods.
- Subcontracting: who you engage to carry out various elements of the processing – e.g. hosting/infrastructure providers, process outsourcing providers, other group companies, consultants.

- Access: who accesses the personal data (e.g. your staff, subcontractors and group companies' staff); in what circumstances (e.g. only for troubleshooting or on customers' request?); whether the extent of that access is varied or restricted. Also, in respect of those staff members who do have such access, what privacy training have they undergone and can you demonstrate this?
- Transfers outside the EEA/EU: does personal data leave the EEA/EU as a result of what you do with it – e.g. does it go to your non-EEA/EU-based group companies / offices or to international organisations; is it stored/backed up in servers outside the EEA/EU, do your staff access it remotely from outside the EEA/EU? If it does, what GDPR-compliant mechanisms or safeguards do you have in place in respect of those transfers – e.g. standard contractual clauses, binding corporate rules?
- Anonymisation/pseudonymisation: if you carry out anonymisation it's worth mentioning this, as truly anonymised data is not personal data and therefore not subject to the GDPR requirements; if you carry out pseudonymisation it's also worth pointing that out, as the GDPR specifically recognises that this can reduce risks to individuals and help comply with data protection obligations.
- Information security measures: the technical and organisational measures you implement to protect personal data – e.g. staff training, vetting and confidentiality obligations, physical security controls to your premises, paper records and computer systems, due diligence/minimum standards/contractual commitments imposed on your suppliers and subcontractors, cybersecurity measures (firewalls, penetration testing etc.). This can be an opportunity to show off your security awareness and credentials such as any ISO certifications or industry awards.
- Data processing terms: you could mention that your standard contract/terms and conditions include suitable data processing provisions, demonstrating that you understand the need for these and offer them as standard.
- Data protection officer ("DPO"): you could set out your views on whether you are required to appoint a DPO under the GDPR, and if you do have a DPO, and provide their contact details.
- Contact: whether or not you have a DPO, it's worth providing contact details for any customer queries or complaints relating to your processing of personal data.

Finally, aim to make it readable, jargon-free and to the point, explaining technical points in language that the uninitiated can understand.

Do contact us if you would like to investigate preparing a white paper for your own organisation or if you otherwise have any GDPR compliance questions.