DO GDPR & EPRIVACY AFFECT YOUR CUSTOMER DATABASE?

General Data Protection Regulation

GDPR

All businesses probably have a database of customers that they rely on for marketing. That all changes next year and we will cover this in the ePrivacy article later.

This GDPR section is about the effect of Privacy Notices on the processing of customer information after 25th May 2018 and is just as important for business survival as having marketing consents.

This is about privacy notices and consent

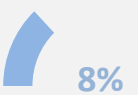
Privacy Notices should currently tell customers everything about where information is collected, who from, why, what is done with it, who it is shared with, what else is generated or analysed from it, if it is used for research or statistical analysis, obtain their consent where necessary and inform them of their rights. ***It is the most crucial document of business rights.***

If no contact is made with the customer after 25th May 2018 then there is no problem, unless the business wants to share information with anyone else.

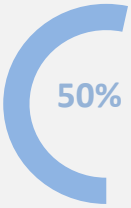
If they do want to be in contact with their customer after 25th May, they cannot rely on their existing Privacy Notice, and that will be problematic.

You may not be able to get your customer to allow you to do what you need to do after May 2018

Number of UK businesses



Number of businesses registered with Information Commissioner



Percentage of UK businesses that suffered a data breach last year according to UK Government

Why business cannot rely on an existing Privacy Notice after 25th May 2018

First of all it is important to realise why the Privacy Notice is such a big deal. It is because this is the most critical document in this area.

The Privacy Notice is what gives lawful authority to do everything the business needs, wants or has to do in relation to the personal information they collect and use.

After 25th May 2018 a new form of Privacy Notice has to be given, and the extent of consents needed changes, so any business could find they cannot do things that they currently do as their customer may not give their consent. This includes B2B customers as well.

The question is, if your customer will not give the new consents required under the new rules both in terms of collecting and using new data for new deals with them, or indeed for holding on to the personal information already held about them, where does that leave business?

Will the business have to destroy data if the individual will not consent to the business continuing to have it or use it? The answer to that question is yes.

Why would that happen?

The reality of Privacy Notices is that few businesses have any idea what IS in it

The reality of Privacy Notices is that few businesses have any idea what HAS to be in it

The reality of Privacy Notices is NEARLY everyone copies somebody else's

The reality of Privacy Notices is that few create and use a data flow map first

The reality of a Privacy Notice is that few really capture what business actually does with data

The main issue to note is the last point, that the Privacy Notice does not capture what is actually done with personal information, which in turn means there is no lawful authority to use it for those reasons. That also means there is no right to have it or keep it at all.

Why does it matter now?

Obviously it will matter a lot more after 25th May 2018, because if a customer finds out the business is continuing to use their personal information for reasons not disclosed to them in the Privacy Notices, the individual may lodge a Privacy Claim and, should they complain to the ICO, to fines up to £20 million because not getting your Privacy Notice right is one of the specific reasons for the ICO imposing the biggest fines.

However, not having a correct Privacy Notice right now is the starting point of these problems. Not devoting sufficient resource, time and attention to data flows and uses, and not concentrating on accurate Privacy Notices and collection of data is the position of 95% of all UK businesses.

Examples of Privacy Notices that do not work

The following are a few examples of current practices which do not work to protect business against data destruction, Privacy Compensation Claims and ICO fines.

These are all real examples.

EXAMPLE	WHY IT IS A PROBLEM
We collect and use your information in accordance with the Data Protection Act.	Unless the reader actually knows the Data Protection Act inside out, would they have any idea what it means?
US Limited is part of an international Group of companies owned by World plc and registered as a data user under the Data Protection Act. Any member of this Group may keep and use your personal details for the purposes of providing services to you. In addition we may need to disclose your details to organisations working on our behalf anywhere in the world (for example, credit reference agencies, mailing houses and call centres).	It gives names but does not identify which company is the data controller. It does not get the required consent to allow other companies to have the person's information. It does not obtain the consent needed for sending data out of the EU/UK. The reference to "providing other services" means they are marketing without consent. It lacks disclosure or transparency as to what they are going to do with the data.
The members of this Group never sell, rent, or give away information that personally identifies customers …	This is an example of someone lifting their privacy notice from somebody else's and getting it wrong. This company then sold on customer details for £13,000, and was fined £120,000 by the ICO. Although the ICO fine is about emarketing and therefore falls under the ePrivacy/PECR rules, it shows where companies have been burying these marketing issues, wrongfully, in their Privacy Notices

The issue is that there are many ways to think the process is followed, when in fact it does not achieve the requirement of giving notice to the individual properly. Privacy Notices that are not layered, or which do not get seen or do not require positive affirmation are worthless.

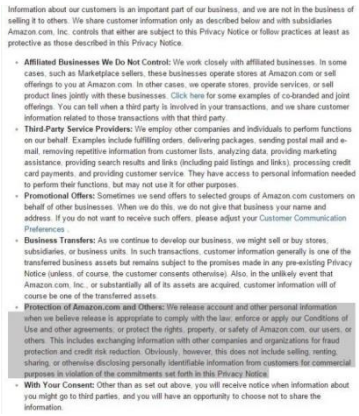
THE IMPORTANCE OF PRIVACY NOTICE PRACTICES FOR KEEPING DATA

Strangely, the easiest way of illustrating this is to look at what might happen when a customer takes their business elsewhere.

When they fail to renew a licence, subscription, insurance or membership or account the losing business will have to look at what personal information it may legally then keep, as the losing business has no ongoing relationship with that individual.

What has it got to do with keeping hold of data?

This all then comes down to what was put into the Privacy Notice(s) at the very beginning of the customer relationship journey. This is where the critical nature of these Privacy Notices becomes very self-evident and the processes that have to be thought through before the Privacy Notice even starts to be written. That is a series of articles in itself, but for the purpose of this we will keep it brief.



Information about our customers is an important part of our business, and we are not in the business of selling it to others. We share customer information only as described below and with subsidiaries Amazon.com, Inc. controls that either are subject to this Privacy Notice or follow practices at least as protective as those described in this Privacy Notice.

- **Affiliated Businesses We Do Not Control:** We work closely with affiliated businesses. In some cases, such as Marketplace sellers, these businesses operate stores at Amazon.com or sell offerings to you at Amazon.com. In other cases, we operate stores, provide services, or sell product lines jointly with these businesses. Click here for some examples of co-branded and joint offerings. You can tell when a third party is involved in your transactions, and we share customer information related to those transactions with that third party.
- **Third-Party Service Providers:** We employ other companies and individuals to perform functions on our behalf. Examples include fulfilling orders, delivering packages, sending postal mail and e-mail, removing repetitive information from customer lists, analyzing data, providing marketing assistance, providing search results and links (including paid listings and links), processing credit card payments, and providing customer service. They have access to personal information needed to perform their functions, but may not use it for other purposes.
- **Promotional Offers:** Sometimes we send offers to selected groups of Amazon.com customers on behalf of other businesses. When we do this, we do not give that business your name and address. If you do not want to receive such offers, please adjust your Customer Communication Preferences.
- **Business Transfers:** As we continue to develop our business, we might sell or buy stores, subsidiaries, or business units. In such transactions, customer information generally is one of the transferred business assets but remains subject to the promises made in any pre-existing Privacy Notice (unless, of course, the customer consents otherwise). Also, in the unlikely event that Amazon.com, Inc., or substantially all of its assets are acquired, customer information will of course be one of the transferred assets.
- **Protection of Amazon.com and Others:** We release account and other personal information when we believe release is appropriate to comply with the law; enforce or apply our Conditions of Use and other agreements; or protect the rights, property, or safety of Amazon.com, our users, or others. This includes exchanging information with other companies and organizations for fraud protection and credit risk reduction. Obviously, however, this does not include selling, renting, sharing, or otherwise disclosing personally identifiable information from customers for commercial purposes in violation of the commitments set forth in this Privacy Notice.
- **With Your Consent:** Other than as set out above, you will receive notice when information about you might go to third parties, and you will have an opportunity to choose not to share the information.

MAIN AREAS OF PRIVACY NOTICES			
What is collected	Who and where it is collected from	Who it is shared with and why	Other
AND EACH ITEM OF INFORMATION COLLECTED OR GENERATED OR SHARED HAS TO BE MAPPED INTO ONE OF THESE THREE AREAS	What is needed to perform the contract		
	What is used for a legitimate business interest		
	What needs consent (the rest)		

It is critical to know into which category the data falls

Why is it important to know?

The reason is that obviously at the outset business needs to be able to prove (should the Regulator or indeed the individual or their Claims Management representative make enquiry) WHY that information was needed, what was done with it and who it was shared with and why.

Knowing this means only actual, needed and used information is collected and that is efficient.

Then it has to be categorised into one of the 3 legal grounds above: contract, legitimate interest or consent…….***AND CONSENT CAN BE WITHDRAWN AT ANY TIME***.

But if any item of information cannot be put into one of the three legal grounds then it cannot be collected, used, generated or shared in any way let alone kept past the end of the contract.

USING THE RIGHT LEGAL GROUND PROTECTS BUSINESS

It is worth spending time to list all the types of personal information a business collects or generates and what it is used for, and then to work out which category applies, because if it seems to fall into the Consent category, what needs to be worked out is what it would mean if the customer withdrew that consent at any point in the relationship, the delivery of the services or the provision of goods or access to the deliverable item/service.

TO PERFORM THE CONTRACT

A LEGITIMATE BUSINESS USE

CONSENT

If it turns out that the business cannot deliver the service, access or goods required without being able to use something which has been categorised into the Consent category, then it actually belongs in the first category of, "required for the contract (to be performed)."

That means the customer cannot stop it being used. The question then is what happens when the goods have been delivered? Is that information still needed? If it was to enable the performance of the contract then it is likely it will continue to be needed to prove delivery, or acceptance or for legal or accounting reasons BUT IT ALL NEEDS TO BE DOCUMENTED AND UNDERSTOOD.

HOW DOES THIS APPLY TO ONGOING SERVICES?

In addition to the foregoing points about working out what is needed to start the service, it is also necessary to work out what is needed or will be created or shared during the delivery of the service, and to work out the effect of what would happen if that activity or information fell into the consent category and consent was withdrawn.

The bottom line is that the reality of the situation has to be addressed, so if it falls into the consent category then that is where it lies. It is not wise to push something into the wrong category.

WHAT HAPPENS IF THE CUSTOMER GOES ELSEWHERE?

This is actually an interesting point as it ties to the new right of ***Data Portability***.

What it means is for any business that provides a service, say for insurers but not necessarily, if the customer decides to go elsewhere during the period of insurance or service or on renewal they can ask the insurer or service provider to port over all the information they have about them to the new, or intended, provider.

Once the information has been ported over, the question is what information can actually be kept?

WHAT HAPPENS IF THE CUSTOMER GOES ELSEWHERE? Part 2

In this scenario the customer does NOT ask for their information to be ported to a new provider.

The same questions apply:

What has to be kept by the business and for what purpose? There is no ongoing provision BUT what needs to keep to be part of the corporate records, tax records, accounting information, legal defence information (in case a claim arrives).

All of this then turns on what was put into the Privacy Notice at the outset.

Again, this means having to think about the uses to which data is put, and for which it is needed not just at the start of the relationship with the customer, but during it and after it is over.

FOR EXAMPLE, if you think the customer might come back in the future, would you need to have kept some of the information even on a pseudonomised basis in order to underwrite them for the new insurance or service or access? If so that would need to go into the Privacy Notice at the outset.

If consent was needed in order to do that, then what would the consequence be of not being able to use that previous information? Would the price be higher? If so say so and ask for consent on the basis that it would be used in the future for better pricing.

EXAMPLES OF THE THREE GROUNDS

To perform the Contract	A legitimate business use	Consent
Name, Address	Credit reference searches	Anything not falling under the other two headings
Contact details	Electoral role search	
Payment details	Sharing with delivery company	
	Sharing with debt collectors	
	Statistical analysis	

Legitimate business use is something that you can justify as having to be done either to enable performance (because you don't have to use a delivery company, that is your choice as a business) or something deriving from it (such as collecting the debt if there is non-payment)

THE SUMMARY

On the basis that the vast majority of businesses have not paid any, or any due, attention to their Privacy Notices we can only suggest they do the following:

1. Sit down and review the Privacy Notices used to date
2. Analyse if they are accurate
3. Issue a new one which is accurate*
4. Do not seek marketing consents of any kind.

When the GDPR arrives it will be necessary to create a whole new Privacy Notice, but in our view it is not worth taking that pain until you have to do so.

DataGuardsman Limited

August 2017

[* for many this is a work in itself. DataGuardsman has a Privacy Notice section where a business can build one that fits its business]

DISCLAIMER: THIS ARTICLE IS NOT LEGAL ADVICE NOR IS IT INTENDED TO BE NOR IS IT INTENDED THAT BUSINESS WILL RELY ON IT.