AVOIDING FINES UNDER THE UK GDPR — 5 TOP TIPS FOR BUSINESS OWNERS

SHOREDONS&CO. LEGAL

INTRODUCTION

IF YOU'RE UNSURE WHETHER YOUR BUSINESS IS COMPLIANT WITH THE UK GDPR - IT PROBABLY ISN'T!

All businesses in the UK must comply with the General Data Protection Regulation, as implemented in the UK (we call this the UK GDPR). Failing to comply can lead to fines of up to £17.5m, or 4% of annual global turnover (whichever is greater).

Ensuring your business is compliant with the UK GDPR can be complicated, time-consuming and confusing - but failing to take action will create a serious risk within your business.

It's your role as a business owner to reduce risk across your business. That includes ensuring you're complying with any necessary laws (including the UK GDPR).

There is no 'one-size-fits-all' approach to complying with the UK GDPR. Instead, businesses must consider the different types of personal data they collect, and adopt contracts, documentation, policies, systems and security, appropriate to the specific risks they face.

A business collecting large amounts of highly sensitive data (for example, health data) will clearly need to take a different approach to a business collecting first names and email addresses only.

This report sets out 5 practical tips that you, as a business owner, can implement to reduce the risk of fines under the UK GDPR.

You should note that these tips are not exhaustive. The UK GDPR lays down a whole range of obligations that businesses need to comply with. Whilst these tips won't necessarily ensure your business is compliant, they do address most of the key issues. They also help create momentum - something most businesses struggle with.

If you'd like a free UK GDPR consultation, call us now on 0203 7292 388. In that consultation, we'll help you understand whether your business is compliant, we'll identify the risk of fines, and we'll work with you to map out a plan for avoiding them.

TIP #1 - REGISTER ONLINE WITH THE ICO AS A DATA CONTROLLER

This first tip is a quick win for most businesses. It should take no longer than 10 minutes.

If your business acts as a data controller, you'll need to register with the ICO and pay the annual fee.

If you're unsure as to whether your business acts as a data controller, call us now on 0203 7292 388.

"ALMOST ALL BUSINESSES ARE DATA CONTROLLERS.

ALL DATA CONTROLLERS MUST REGISTER WITH THE INFORMATION COMMISSIONER'S OFFICE (THE ICO) AND PAY AN ANNUAL FEE."

TIP #2 - IMPLEMENT YOUR KEY UK GDPR DOCUMENTATION

"THE DOCUMENTATION YOU'LL NEED WILL VARY DEPENDING ON THE DATA YOU COLLECT."

As a minimum, you should consider:

a. A Record of Processing Activities

The UK GDPR requires businesses to document their processing activities. This is usually the starting point, as it will give you a good understanding of the data you collect, and what you do with it.

Your Record of Processing Activities must contain certain information. Such as:

- details of the personal data being collected;
- the purposes for which that personal data is being collected;
- the individuals to which that personal data relates;
- details of any third parties that personal data will be transferred to (along with where they're located); and
- any technical and organisational security measures implemented around that personal data.

Preparing a Record of Processing Activities is not straightforward. Make sure you're including all of the information the UK GDPR requires you to include. Failing to include that information could open your business up to fines.

(continued on next page...)

b. Privacy Notices

Privacy Notices should be used to explain to individuals how your business collects, uses and stores any personal data relating to them.

You'll need two separate Privacy Notices:

- One for your staff; and
- One for other third parties, such as customers and suppliers.

Your Privacy Notices must include certain mandatory information laid down by the UK GDPR, so make sure they're drafted by a specialist to ensure they're compliant. Simply downloading a Privacy Notice from the internet will not be sufficient, as it needs to be tailored to reflect the way in which your business operates.

Your Privacy Notices must be brought to the attention of individuals at the time of collecting their personal data. You may, for example, need to ask your staff to sign a copy of your Staff Privacy Notice on the day their employment begins. You might also need to upload Privacy Notices to your website (and any other places where you collect personal data), and include tick boxes to properly bring your notices to the attention of your visitors.

Many businesses fail to properly implement their Privacy Notices. Don't take that risk, as it will open your business up to potential fines.

c. A Data Protection Policy

A Data Protection Policy is an internal document explaining the rules that your staff will need to comply with under the UK GDPR.

Again, this should be professionally drafted to ensure it addresses the specific types of personal data your business collects. It also needs to be in sufficient detail to cover the various rules you'll need to adopt under the UK GDPR.

d. A Data Retention Policy

The UK GDPR states that your business must retain personal data for no longer than needed. A Data Retention Policy will set out the rules your staff need to comply with to address this requirement.

This document should be professionally drafted and tailored to ensure that you're properly deleting the specific types of personal data that your business collects. Failing to have this policy in place will probably mean you're not deleting personal data properly. That issue will open your business up to potential fines.

(continued on next page...)

e. An IT and Communications Systems Policy

An IT and Communications Systems Policy sets out the rules your staff will need to comply with when using information technology. It should include rules around passwords, downloading software, accessing emails, using the internet and monitoring. This policy will not only lay down rules for your staff, but it will help reduce the risk of data breaches and data leaks - as it will help ring-fence (and provide security) around the personal data you're collecting.

This document must be detailed and tailored to your business. Make sure you have it professionally drafted. A half-baked policy will not provide the protection you need.

f. Data Processing Agreements

Whenever a business transfers personal data to a third party (or provides a third party with access to personal data), the UK GDPR requires you to have a written contract in place with that third party.

That written contract must contain certain mandatory data processing provisions, so it's important to have it properly drafted. If it does not contain those mandatory provisions, it will not be compliant with the UK GDPR - so your business may be open to potential fines.

CAUTION!

Implementing this documentation is a large part of compliance. However, documentation that either (i) does not include the mandatory information laid down by the UK GDPR, or (ii) does not properly reflect how your business operates, will not address compliance – it's the content of those documents that's important.

We see many businesses downloading templates online, and in some cases, taking documentation from a competitors' website. In most cases, that approach will not address compliance. In fact, it can make matters worse. Not only will that documentation fail to reflect how your business operates in practice, but you may not have the rights to use it (so you might find you have an infringement claim against you!).

Make sure you take advice from a specialist.

TIP #3 - MAKE SURE YOU'RE ABLE TO PROVIDE INDIVIDUALS WITH THE RIGHTS LAID DOWN BY THE UK GDPR

The UK GDPR provides individuals with:

1. A right to be informed about the processing you'll carry out.

This is usually addressed with Privacy Notices. If you've implemented Privacy Notices in accordance with the UK GDPR, it's likely you've addressed this.

2. A right to access their personal data.

You must be able to provide copies of any personal data you collect upon request. You'll have around a month to provide copies of this personal data, so it's important you're prepared.

Personal data can be stored electronically (in emails and on CRM systems) and in hard copy (in filing cabinets). It's important that you're able to provide copies of all sets of data on request.

3. A right to rectification and data quality.

You must have a way of correcting any personal data that is incorrect. This might be fairly straightforward for personal data stored on a CRM system, but it might be more difficult for personal data stored on other platforms – particularly if those platforms are controlled by third parties.

Again, strict timeframes will apply when correcting any data, so makes sure you're able to provide this right.

(continued on next page...)

4. A right to erase any personal data you're storing about them.

This is known as the 'right to be forgotten'. You'll need to delete any personal data you hold about individuals that request it.

You'll have strict timeframes to comply with here. There are circumstances where you can refuse to comply with this type of request - but that will depend on the circumstances at the time. For now, it's important that you have the ability to quickly delete any personal data you collect.

5. A right to restrict processing.

If an individual asks you to restrict the processing his/her personal data, you must comply with that request. Again, there may be exemptions you can rely on to refuse this type of request, but that will depend on the circumstances at the time.

For now, make sure you're able to provide this right.

6. A right to data portability.

You must allow individuals to reuse the personal data you've collected about them if they wish to do so.

To address this, you'll need to ensure you're able to provide this personal data in a structured, commonly used and machine-readable format.

7. A right to object.

If an individual requests that you stop processing his/her personal data, you must comply with that request. You'll have one month to respond to this, so make sure you're prepared.

CAUTION!

Ensuring that individuals are provided with these rights is critical for compliance. Any procedures you adopt for providing these rights should be documented – for example, in your Data Protection Policy.

TIP #4 - MAKE SURE THE PERSONAL DATA YOU COLLECT IS SECURE

"THE UK GDPR PLACES AN OBLIGATION ON ALL BUSINESSES TO ENSURE THEY ARE PROCESSING PERSONAL DATA WITH APPROPRIATE SECURITY IN PLACE.

YOU'LL NEED TO CONSIDER THE TYPES OF PERSONAL DATA YOU'RE COLLECTING, AND BUILD APPROPRIATE SECURITY AROUND IT."

If you only collect email addresses, then your security may be more relaxed than if you were collecting criminal convictions data. Likewise, if you're storing your data in the UK only, then you might take a more relaxed approach than you would if you were transferring personal data to another country.

CAUTION!

This may require specialist advice, so speak with your IT team (or your IT provider) if you're unsure. You will also need to document the security you have in place, so make sure you take legal advice from a specialist on the best way of documenting that security.

TIP #5 - DELEGATE RESPONSIBILITY AND ARRANGE TRAINING (FOR YOU AND YOUR STAFF)

"WE ADVISE MANY BUSINESSES ON COMPLIANCE WITH THE UK GDPR.

BUSINESSES TEND TO STRUGGLE ADDRESSING COMPLIANCE WHEN THE BUSINESS OWNER HAS OTHER ISSUES TO DEAL WITH.

THIS IS A COMMON PROBLEM."

Whilst it is important to have senior management buy-in with UK GDPR compliance, responsibility does not necessarily need to sit with the business owner. It can (and often should) be delegated.

Appointing someone within your business to take ownership of UK GDPR compliance is great way of encouraging progress. Once an individual takes responsibility for it, progress generally comes shortly after.

When delegating responsibility, you should arrange training for that individual (either in person or online). You should also set milestones and deadlines for that individual to work towards, and monitor progress over time. Regular check-ins will also help encourage progress.

(continued on next page...)

The UK GDPR places an obligation on all businesses to arrange data protection training for all staff that handle personal data. If you're arranging training for one individual, select a provider that can train you and all of your staff at the same time. Not only will this address one of your regulatory requirements, but it will help raise awareness across the business. It will also provide your staff with the knowledge they need to pick up on risks and issues when they arise. This will, in turn, reduce risk across your business.

Data protection training will raise questions. Make sure that any training provider you select is able to hold a Q&A session at the end. That will help ensure your staff properly understand the content.

CAUTION!

When selecting an individual to take responsibility for UK GDPR compliance, make sure they have the necessary support to handle that project. UK GDPR is complicated, so ensure they have an external data protection specialist that can help guide them through the more complicated parts. Working with a specialist will help speed up the process. It will also ensure that any documentation is properly drafted. Remember - it's the contents of your documentation that's important (not the document itself).

WE HOPE YOU FIND THESE TIPS USEFUL.

IF YOU'D LIKE A FREE UK GDPR CONSULTATION WITH ONE OF OUR SOLICITORS, CALL US ON 0203 7292 388. IN THAT CONSULTATION, WE'LL HELP YOU UNDERSTAND WHETHER YOUR BUSINESS IS AT RISK OF FINES UNDER THE UK GDPR, AND WE'LL WORK WITH YOU TO MAP OUT A PLAN FOR AVOIDING THOSE FINES.

WE'RE HERE TO HELP.

ABOUT THE AUTHOR

This report was published by Matt Turner, the founder of Shoredons & Co Legal.

Matt is a solicitor with extensive experience in advising organisations on the UK GDPR. He also advises on how to avoid the fines.

He offers bespoke advice on certain queries, but he also carries out compliance audits to identify areas of non-compliance. He then provides the documentation, advice and training needed to ensure compliance.

When working with Matt and his team, they'll bring the experience you need to address compliance quickly and efficiently.

If you'd like to speak with Matt or one of our other team members, call us now on 0203 7292 388.

THE UK GDPR IS COMPLICATED. ALL BUSINESSES LOOKING TO COMPLY SHOULD TAKE EXPERT ADVICE FROM A SPECIALIST SOLICITOR, WHO UNDERSTANDS THE INTRICACIES AND DIFFICULTIES OF THE UK GDPR.

APPOINTING A SPECIALIST WILL SAVE YOU TIME AND MONEY.

This document (and the contents within in) does not constitute legal advice. Your use of this document will not give rise to a solicitor and client relationship. This document is provided for informational purposes only. You must not take, or refrain from taking, any particular action based on this document. Instead, specialist legal advice should be taken from us. That advice will be tailored to your specific circumstances. It's also important to note that data protection laws change, so some of the information contained in this document may be out of date. We disclaim all liability arising from any reliance placed on the contents of this document.

Publication date – October 2022.