5 GDPR Essentials for Small Businesses

GDPR compliance for small businesses can seem like a maze – but with a solid foundational understanding and a plan in place, it's a maze you can easily navigate.

In this blog, we'll run through 5 essential considerations, from awareness to policy reviews, to help simplify GDPR compliance.

1. Be data-aware

The first step to data compliance is knowing your data.

Conduct a full and thorough audit of your business to find out exactly what data you process and who has access to it. Companies larger than 250 employees – or those whose data is considered 'higher risk' – will need to keep a list of their processing activities and be prepared to show it to a regulator on demand.

Companies with less than 250 employees should also assess their data to make GDPR compliance easier.

Be sure to think about the Why, What, Who, How, and When:

- **Why** – Why are you processing this data? Do you have legal justification?
- **What** – What is the nature of the data you are processing?
- **Who** – Who in your business has access to this data? Are you transparent about your privacy policy with those whose information it is?
- **How** – How are you keeping the data safe and secure?
- **When** – Will you be deleting the data at some point? Is it easy for a customer to ask you to delete their data?

2. Be secure

Data security is vital for GDPR compliance.

You should use encryption or pseudonymisation wherever possible and ensure that processing systems are regularly tested for integrity and effectiveness.

Data security spans beyond the technical, however – your business's staff must be aware of processes in place so that operational errors don't lead to compromises.

This is where policy comes in. Your employees should have guidance on passwords, email security, two-factor authentication, encryption, and VPNs. Further to this, anyone with access to data should know the correct way to handle it.
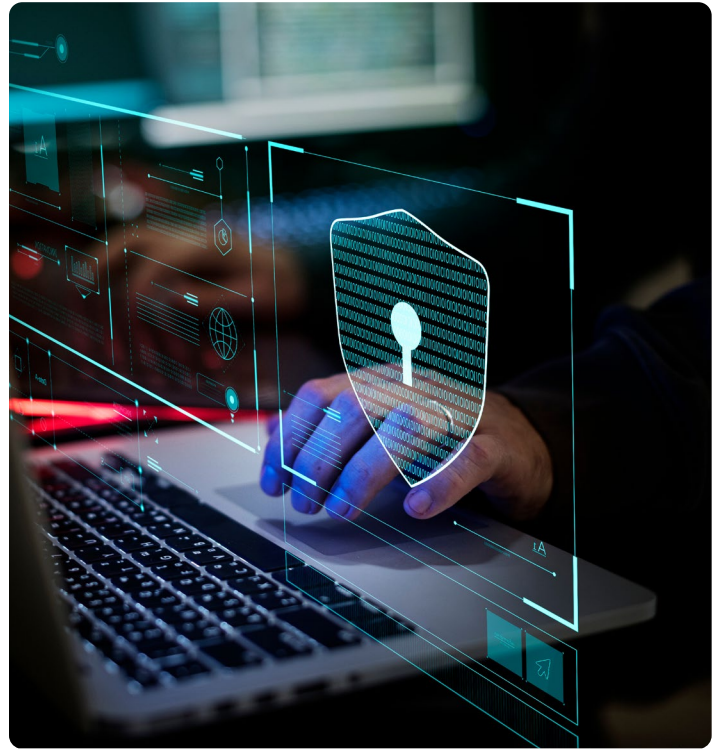
3. Conduct Training

Businesses have a responsibility to ensure their employees – especially employees who handle data – are trained in GDPR.

As a small business, you might have a better opportunity to be hands-on with this training, making sure everyone has what they need. But on the other hand, having multiple staff members out on training as a small business can be detrimental – so plan wisely.

Within the training, set measurable goals – like a target of 0 successful phishing attempts, for example. Be sure to set both short and long-term goals, basing longer-term goals on current threats once you've assessed those.

Having a dedicated GDPR person or team of people will prove useful for continuity here.
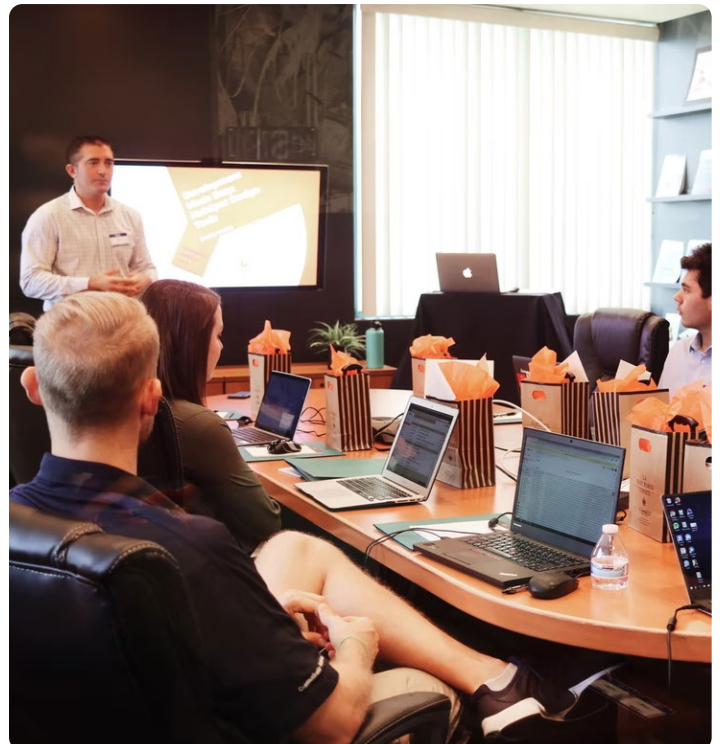
4. Check throughout the chain

Don't let there be a weak link in the chain by making sure you sign agreements between your business and any third party that processes data on your behalf.

You should ensure you use reliable third parties and check their data processing agreements (many have standard ones on their website). Email services, cloud servers, software, and more – these are all potential points of vulnerability when it comes to data, so keep these third-party services in mind too.

5. Regular policy reviews

When it comes to GDPR compliance, you can't simply 'set it and forget it'!

Regularly reviewing policies and security is crucial to your GDPR strategy, especially as your business evolves, processes change, and data requirements shift.

Personal data should be up to date and accurate and the customer should be aware of how their data will be used. Therefore, information should be reviewed regularly, alongside policy, to be fully compliant.

If your business starts processing data on a large scale or you begin processing particularly sensitive data, you might consider appointing a Data Protection Officer. Think about and predict this ahead of time so you don't have to scramble to hire when the demand strikes!

Get data smart!

If you're a small business looking for more information on GDPR, take a look at this GDPR Checklist and read the official guidance in its entirety here.

Here at Vinters, we take pride in the security of our solutions, be it with our dedicated servers or our private cloud options; your data protection is our priority.

Get in touch with us if you'd like to find out more about how we work!