The GDPR guide for small businesses

Our easy guide on making your business data compliant.

Cyber Accelerator Alumni

in association with National Cyber Security Centre

CYBER ESSENTIALS

naq.

GDPR:
What is it and how does it affect my business

The GDPR applies to all businesses that collect or store sensitive information, regardless of company size.

Coming into effect in May 2018, the GDPR requires organisations to not only be transparent in their reasons for collecting user data but also ensure that is stored securely and responsibly.

What counts as sensitive customer data?

- A customers name and surname
- A customer's home address
- A customer's email address
- An identification number, such as a passport or National Insurance number.
- Data about your customer's location
- A user's advertising identifier.

If your organisation holds any of the pieces of information about its customers, **it is required to adhere to the GDPR or face a potential fine.**

But the UK is no longer in the EU?

The UK has now implemented the UK-GDPR which follows the same set of policies outlined by the EU-GDPR. If your organisation processes information from EU customers, it is now bound by both sets of regulation.

1 Understand your legal basis

In order to be GDPR compliant, your business must adhere to one of six legal bases. These legal bases outline your reasons for collecting, processing and storing sensitive information.

One of the bases you may already be familiar with is **consent.** While this may seem the easiest option, maintaining consent can prove difficult, in addition to requiring strict record-keeping and giving users the ability to withdraw information at any point.

It is advisable then, to review all of the lawful bases and decide which one applies best to your business:

- **Consent:** A user has given explicit consent for their data to be collected, processed and stored.
- **Contractual obligations:** The sensitive data is essential to fulfilling your contractual obligations. or to provide something like a quote or a brief.
- **Legal obligations:** If the processing of sensitive data is required to comply with common law.
- **Vital Interests:** The processing of sensitive data is necessary to protect someone's life.
- **Public Interest:** The processing of sensitive data is necessary to perform tasks in the public interest, including the administration of justice.
- **Legitimate Interest:** This is the most flexible out of all the six bases, yet the most difficult to interpret. Legitimate interest includes, but is not limited to:

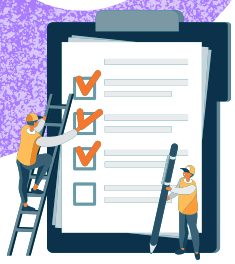
Processing client or employee data
Processing data for marketing purposes
Processing for IT security purposes

The ICO has published a three-part test you can take to determine whether there is a legitimate interest in processing this sensitive data.

To summarise, it is important to review each of these bases in detail to determine which one applies best to your business. Additionally, take note of what record-keeping practices you'll need to implement to remain compliant.

2

Keep a processing registry



Keeping track of your processing activities is an essential part of GDPR compliance for small businesses and large enterprises alike. It also enables your business to demonstrate its compliance effort to customers, ensuring them that their data is being processed responsibly.

Companies should keep a **"processing registry"** which essentially **details your business' legal basis, what personal data is being processed, how, why, for how long it's kept and what security measures are in place to prevent a potential breach.**

Begin by identifying what personal data is collected across your business. Appoint one member of staff to be responsible for GDPR compliance so you also have a single point of contact should any external GDPR questions arise.

3

Write your GDPR policies

In addition to your processing registry, there are a few other policies you'll need to write and have in place. You can read our detailed blog on **7 GDPR policies small businesses need to have**, but for now, we'll touch on two of the most crucial policies to implement., **the cookie and the privacy policy.**

The cookie and privacy policies tells users on your website what data is being collected as they browse through your site. This is crucial if you use cookie data for marketing purposes. Additionally, it should highlight that users have the right to withdraw their consent to data collection, firstly through opting-out directly on your website and secondly by sending you a direct request.

These policies must be clearly outlined on your website and kept up to date whenever you implement additional tracking activities such as new advertising tools.

4

Website consent management: Keep track of those cookies.

As we mentioned earlier, in order to remain GDPR compliant, you'll need a comprehensive cookie policy highlighting how data from users visiting your site is collected and how it's used.

Additionally, you'll also need to give users the ability to opt-out of this tracking activity through the use of a cookie banner. This allows users to say no to collecting any non-anonymised cookie information, leaving just those which allow your website to run.

As part of our service, all of our customers have access to a tailored, easy to implement cookie policy for their websites.

Keep personal data safe

5

Keeping your customer's data is safe is an integral part of remaining GDPR compliant, but just how do you go about it? Let us take you on a whistle-stop tour of **what is known as privacy by design.**

Privacy by design is a GDPR principle which states that you must incorporate privacy not just into your data processing activities, but also into your business practices. This simply means taking privacy into account in everything that you do, from building your website through to daily tasks such as emailing.

But how do you go about incorporating this? For emails, it could be something as simple as avoiding sharing any personal information in the form of attachments, using instead a secure cloud platform such as Google Drive. It could be implementing two-factor authentication across any accounts containing sensitive information.

|For this step, [you'll need to take stock of what apps, accounts and software currently contains personal or sensitive information and ensuring these are kept secure.

In addition to complete GDPR compliance, Naq also takes care of all your business cybersecurity, baking privacy by design right in to your business.

6

Implement an incident response strategy

As if you didn't have enough to do already, the GDPR requires that your business has a good incident response plan in place. Before you do, it's important that you know the difference between an **incident** and a **data breach.**

An **incident** is an event that impacts your information processing systems but hasn't impacted any personal data. This could be a malware attack on one of your office devices.

If any personal data is compromised, this then escalates to a **data breach** and includes but is not limited to; hackers getting access to your sensitive business data or this data being published online.

In order to be GDPR compliant, your business needs to include the following steps in its incident response:

- **Keep detailed records of all the events leading up to the data breach,** how it was discovered, what measures have been taken to resolve the data breach and what steps have been taken to ensure this doesn't happen again in the future.

- Even if you don't have all the details on the event, you must **notify the data protection authorities within 72 hours of discovering the breach.**

- If the data breach is likely to result in a high risk of adversely affecting an individual's rights and freedoms, you must **inform the data subjects immediately.**

7

Help data subjects exercise their rights

Individuals have the right to be informed about the collection and use of their personal data. As a business, you must provide them with this information, through your cookie consent banner and privacy policy.

Additionally, individuals to get access to all of their information through a **Subject Acess Request.** Your business must comply with these requests without the delay and in most cases within one month.

About Naq

Naq provides SMEs with a complete cyber security, GDPR compliance and staff training solution at an affordable monthly cost. Through our exclusive easy to use platform businesses can review their security actions, improve their organisation's security score and ensure their staff are trained on the most common cyber threats. **All delivered for as little as €99 a month.**

GDPR & DPA Compliance

We provide businesses with complete and bespoke data compliance policies ensuring their data and marketing efforts remain compliant.

Cyber security & Monitoring

24/7 monitoring, web scanning & easy to implement actions to protect your business' valuable data.

Staff Training & Phishing Tests

Training courses & phishing tests to empower your team to remain compliant & secure

Incident Response

if your business falls victim to an attack, we'll be there to help with data recovery and legal advice.

Ready to begin protecting your business?

Take a look at our pricing page here. Alternatively, reach out to us on info@naqcyber.com and a member of our team will be in touch.

Cyber Accelerator Alumni

in association with National Cyber Security Centre

CYBER ESSENTIALS

naq.