LAWPATH
We've made legal easy

Does My Business Need a GDPR Compliant Privacy Policy?

If you run an online business in Australia,
it's likely that you will have to comply with the GDPR.
Read about what that means here.

2ND NOVEMBER 2018

In April 2016, the European Parliament passed the General Data Protection Regulation (GDPR). Although this applies to the 28 member-states of the European Union (EU), Australian businesses are also likely to be affected.

It is likely that as a business owner, you also run a website for it. Having a website has many advantages. Not only can your customers purchase products and find information easily, your brand has an added level of exposure.

In this guide, we'll discuss what new privacy laws mean for you and how to know when you have to comply with international regulations.

Collecting customer data

In the normal course of operating a business, it is likely that the business will gather the personal information of users. Prior to the advent of online business and eCommerce, businesses collected customer information, albeit in different forms. For example, businesses who had a shop would likely have the records of transactions made and even more personal information.

In some ways, business websites are the same. They collect information from customers such as their name and contact details, activity on the site and their financial information. However, the internet also has added risks of data exploitation through hacks and malware. To protect the privacy of consumers, jurisdictions around the world have enacted legislation directed towards regulating how businesses deal with data.

A new model for privacy?

The recent enactment of the General Data Protection Regulations (GDPR) has captured the attention of countries all around the world. This is partially because as it has expanded the scope of entities which need to be GDPR compliant. However, the most significant thing about the GDPR is that it requires all businesses to have a privacy policy. Indeed, the GDPR may represent the beginning of a global push towards making privacy policies compulsory.

Who does it apply to?

The GDPR applies to data controllers (businesses), data processors (businesses who process data) and data subjects (citizens). For the purposes of this article, we're most interested in the requirements for the data subjects. The data subjects are people living or based in the EU – and this is where Australian businesses need to be careful. If your customers count as a 'data subject' under the GDPR, then you will want to keep reading.

What do business's have to do?

Businesses need to inform data subjects that their data is being collected. In addition to this, businesses have to also provide their contact details and the purposes for collecting the data. This information, in addition to other details, is ordinarily found in a privacy policy. Privacy policies differ in what they cover, but business's subject to the GDPR need to make sure they comply with all the provisions of the GDPR.

Australian obligations

The Privacy Act 1988 (Cth) regulates privacy law in Australia. The Act imposes an obligation on certain entities to create a **privacy policy** indicating how they will deal with the information collected about their users. These entities include:

- Australian or Norfolk Island Government agencies;
- Businesses or not-for-profits generating an annual turnover of at least $3 million;
- Private health service providers; and
- Businesses or not-for-profits generating an annual turnover less than $3 million who fall within one of the small business exceptions.

Unsure if you fit the bill? The Privacy Act details who is required to have a privacy policy. Yet, even if your business is not required to have one legally, it is still recommended that you do. A privacy policy will protect both your customers and your business. There are online platforms which offer an easily customisable **privacy policy**. Australian privacy policies are designed to comply with Australian law. The same goes for business's that have a presence in the GDPR jurisdiction.

Example

Robert owns and runs an online phone accessories store, where he uses drop shipping to get his products to customers. Robert has recently started accepting orders from Germany, as a brand he carries is immensely popular there. He has been processing German orders for 3 months but only has an Australian-compliant privacy policy on his website.

Because 'data subjects' are providing information to Robert's business, he is breaking the law by not having a GDPR compliant privacy policy. Fines for non-compliance vary, however fines can be issued that are as high as €10 million. However, member states also have the discretion to determine penalties. In fact, there was a recent case in Germany where a social media company was fine €20,000 for failing to encrypt the data of their customers.

The International Sphere

On 25 May 2018, the General Data Protection Regulations **(GDPR)** came into effect. These regulations substantially altered the privacy obligations of entities operating in the European Union or collecting information about its citizens. It applies to the data processing activities of businesses that are data controllers or processes, subject to certain criteria. It seeks to monitor 'personal data' which is 'any information relating to an identified or identifiable natural person' under Article 4 of the Regulations.

How does this affect Australian businesses? Australian businesses are required to comply with the GDPR in some instances. This is if:

- If they have an establishment in the European Union; or
- If they offer goods or services, or monitor the behaviour of individuals in the EU.

If the GDPR applies to the Australian business, they will need to use a **GDPR compliant privacy policy**. Determining whether your business falls within the scope of the regulations can be tricky, depending on how much business you conduct in Europe. A **privacy lawyer** can assist you with understanding your privacy law obligations, both domestically and internationally.

Not only do customers value their privacy online, but legislation is increasingly reflecting this. Business's who fail to comply not only risk financial penalties, but also risk losing customer trust. If your business has a presence or serves customers overseas, it's important that you comply with privacy laws of those jurisdictions.

Unsure where to start? Contact a LawPath consultant on 1800 529 728 to learn more about customising legal documents and obtaining a fixed-fee quote from Australia's largest legal marketplace.