Lawpath®

Protecting Customer Data

Lawpath

Contents

Chapter 1: Introduction

Chapter 2: If you're just starting out...

Chapter 3: How businesses can minimise risk

Chapter 4: When a breach occurs

Introduction

Changes to how customers view privacy

Customers have always prioritised their privacy. Before the online market took off, customers were mindful of giving out their personal address, using credit cards and handing over their phone number when making purchases at physical stores. It's no surprise then, that customers carry this same mentality when making purchases online. The difference is however, that customer information that is stored online is much more susceptible to exploitation. This is because there are many more ways for customer data to be accessed online, whether it's caused by malware or a hack.

Further, in recent years, customers have become more concerned than ever with how their information is handled online. This is because as technology which makes online shopping seamless has become more sophisticated, so too have the methods for stealing it. The information which customers provide has also become more sensitive, with cookies meaning that this information can be stored on a website eternally.

What is customer data?

Customer data is information that relates to a customer which is held by a business. This can extend from basic details such as someone's name and their recent purchases, to more sensitive information such as residential address and credit card information.

Customer data can also include:

- Email address
- Phone number
- Date of birth
- Location data
- Identity information
- Browsing data

Although this data can be extremely useful for businesses when devising marketing campaigns, customers want to know that their data is being handled responsibly and not put in a position where it can be misused.

Why and how businesses collect customer data

Businesses collect data not only so that customers can make purchases, but also so that businesses can make the experience better for their customers. Collecting data means that a customer will have a more personalised experience online. For example, a customer who is searching for a red phone case may see a red phone case appear on the homepage of the site they're visiting. Collecting customer data can also be highly convenient for customers, such as when a website a customer frequently purchases from remembers the customer's credit card details.

Why businesses need to protect Customer Data

There are multiple reasons why it's important to protect your customers' data. First and foremost, there are legal requirements to do so. In addition to this, protecting your customers' data adequately will instil trust in your customers. Alternatively, if you fail to do this, you may find that your business's reputation suffers.

How cookies work

The predominant way that online websites capture data is through the use of cookies. A cookie is a small data text file which downloads and stores information the first time a customer visits your website. When a customer visits your site for a second time (or any time after this), their computer remembers and uses the information from the cookie to tailor their experience. This is why when you fill out your details on a new website, the next time you return they are often auto-generated, or a store you've made purchases from before remembers the type of products you're on the lookout for.

If you're just starting out...

Getting ready to protect customer data

When starting a website for your business, one of the first things you should think about is how you will protect your customers' data. This will put you in a good position to become a trusted and widely-used brand in your industry. After formally registering your business and protecting your intellectual property, this is one of the first things you should think about.

Having the right documents

When it comes to online privacy, the most important document you should have is a privacy policy. In addition to this, having terms of use on your site will help you keep your site running smoothly. If you send emails to your customers, having a disclaimer in the footer of your emails will also protect you if anything goes wrong.

The Privacy Act 1988 (Cth)

In Australia, online privacy is governed by the Privacy Act 1988 (Cth). This Act outlines the obligations businesses and government agencies have when handling customer information. It also covers how information relating to tax and health should be handled. If you have any questions relating to your obligations when it comes to customer privacy, the Privacy Act should be your first port of call.

The Australian Privacy Principles (APP)

One of the key components of the Privacy Act are the 13 privacy principles which apply to 'APP entities'. An APP entity is:

- An agency (namely, a federal government entity or office holder)
- An organisation (which includes a body corporate, partnership, unincorporated association, or trust)
- A small business with a turnover of more than $3 million annually (or a business which is a subsidiary of a business with a turnover of more than $3 million annually)

An APP entity is not:

- A small business with an annual turnover of less than $3 million
- A registered political party A state or territory authority

The APPs provide guidance on the way you should handle customer information and are as follows:

1. Open and transparent management of personal information
2. Anonymity and pseudonymity
3. Collection of solicited personal information
4. Dealing with unsolicited personal information
5. Notification of the collection of personal information
6. Use or disclosure of personal information
7. Direct marketing
8. Cross-border disclosure of personal information
9. Adoption, use or disclosure of government related identifiers
10. Quality of personal information
11. Security of personal information
12. Access to personal information
13. Correction of personal information

Privacy Policies in Australia

Under the Privacy Act, only APP entities are legally required to have a privacy policy. Although this means that many small businesses are not legally obliged to have a privacy policy on their website, it is nonetheless strongly recommended that they do have one. This is because it will protect the business if anything happens, and will show that your business takes privacy matters seriously. Further, the global trend is towards making privacy policies mandatory for all businesses (such as in Europe) and means that Australia is likely to follow suit.

Why it's important to have a privacy policy

Even if your business isn't an APP entity according to the Privacy Act, you'll still need a privacy policy to conduct your business online. For example, if you want to promote your business on Facebook or Instagram, you will need a privacy policy. Further, many services Google offers requires businesses to have a privacy policy such as Google Ads, Maps/Google Earth, AdSense and Analytics. This means that to remarket your business on Google or even list your business's address will require you to have a privacy policy.

In any case, having a privacy policy is a necessity for most businesses, whether they're in Australia or not.

GDPR

The General Data Protection Regulation (GDPR), whilst only introduced in 2018 in the European Union (EU), meant new obligations for businesses operating both in and outside of the EU. The GDPR makes having a GDPR-compliant privacy policy compulsory for all businesses that operate in, or are connected with the EU. This applies to Australian businesses that have a presence in the EU or have customers who are citizens of an EU country.

Other global attitudes towards online privacy

Global attitudes towards online privacy tend to be following the EU train of thought, in making privacy policies mandatory for businesses. For example, some States (such as California) in the United States have made privacy policies compulsory and New York is currently debating a bill which will introduce this. Closer to home in Asia, Japan has implemented legislation which closely resembles the GDPR, making privacy policies mandatory for businesses.

How businesses can minimise risk

Why prevention is better than cure

Data breaches can be hugely detrimental to businesses. In addition to potentially facing fines for failing to comply with legal requirements, businesses may have to deal with reputational damage and customer fallout. In fact, a survey conducted by RSA on data and privacy found that when a data breach occurs, more than 50% of customers blame the company (as opposed to the hacker themselves). A salient example of this is Facebook, which in the wake of the Cambridge Analytica scandal saw 1 in 4 Americans delete or deactivate their accounts. It can also be said that Facebook's reputation has never quite recovered from this - as users are still highly sceptical of how their data is handled on the site.

What can be taken from this is that preventing a data breach is always a better option than dealing with the fallout if it happens. Further, even if you have all the right legal documents in place, there are further measures you can take to lower the likelihood that your business will become the victim of a hack.

Don't sell data

It is becoming increasingly common for companies to sell data on to third parties, known as data mining. Although this may sound unethical to consumers, businesses do it for a myriad of reasons, with one of these being that the data can assist with tailoring certain products to different demographics of people. Businesses who sell this data also stand to make a lot of money. Legally speaking, businesses which purchase or sell data are considered an APP entity under the Privacy Act, and this applies whether or not they have an annual turnover of more than $3 million. This means that they need to have a privacy policy explaining that what they do with customer data on their website. However, if your business does engage in data mining, the risk that this data will be compromised is greater. Further, if a breach occurs at an agency of which you sold data to, it's still likely to be traced back to your business.

Monitoring your security systems

Businesses need to be diligent in monitoring their security systems. This extends to monitoring your site and how it's operating, your software and the methods you use to keep information secure.

This can mean something as small as changing your business's passwords regularly, or even using NDAs to keep sensitive information (which may or may not relate to customers) within your business. Further, you should always check that the software or plugins your business uses are up to date, as those that aren't can leave your business vulnerable.

Phishing and pharming

Phishing and pharming are both common practices which hackers use to 'steal' information from customers. These businesses normally contact customers pretending to be the business in question, and obtain information they can then exploit or they can direct customers to impersonator websites that are in fact, viruses. However, there are ways you can lower the risk of your customer's information being exposed this way. For example, you can notify customers if there are any scams occurring in your industry, or you can address your emails in a way which is unique to your business. Phishing scams normally address their emails in a generic way, such as 'Dear User', with the content of the email often being poorly written. To distinguish your business from phishing scams, you may want to address your customers in your emails by using their full name and using another identifying factor. You can also inform your customers of this and provide them with tips on how to identify whether an email is the source of a scam or actually from your business.

Malware and other viruses

Malware can affect your customers' information if a link or document purporting to be from your business is sent to customers or the data you hold is stolen. A lot of data breaches are caused by malware, so it's important to understand how your business can avoid it. Some key ways your business can avoid it is by using sophisticated anti-virus software, securing your hardware and encrypting your data. Further, it is worth training your staff in the dangers of malware and making them aware of the danger signs to look out for.

When a breach occurs

How to respond

It's never ideal if a breach occurs and you find that your customers' data has been compromised. However, what's most important at this time is how you respond. Firstly, you should try and identify the source of the breach. Was it a hacker? Or were systems in place that made your business susceptible to malware or other viruses? If you find that the breach was caused by a particular piece of software you're using, you may want to look at finding an alternative software to use. If you catch the breach early on, you may also be able to intercept it and prevent the breach from causing more damage.

The Notifiable Data Breaches Scheme (NDBS)

The Notifiable Data Breaches Scheme (NDBS) came into effect in 2017. Businesses which are subject to the Privacy Act must notify customers that a breach has occurred where:

- There is unauthorised access to or disclosure of personal information held by an entity (or information is lost in circumstances where unauthorised access or disclosure is likely to occur)
- This is likely to result in serious harm to any of the individuals to whom the information relates
- The entity has been unable to prevent the likely risk of serious harm with remedial action

Even if your business is not legally required to notify customers about breaches under the NDBS, it is still a good idea to do so.

Repairing any reputational damage

Depending on the extent of the breach, your business may suffer significant reputational damage, especially if it is found that your business didn't take adequate measures to protect your customers' data. A good cautionary tale can be seen in the Uber data breach. In 2016, the accounts of 57 million Uber customers was exposed, along with those of 600,000 drivers. Uber did not notify the public (or affected users for that matter) at the time, but rather paid the perpetrators to delete the data. When the breach was announced the following year, Uber was met with harsh criticism. Uber at the time was in negotiations with softbank to sell some of its shares. Before knowledge of the breach became public, Uber was valued at $68 billion. After this, its value dropped to $48 billion. Many put down this drop in value to the significant reputational damage Uber suffered for its handling of the data breach.

If we're to learn anything from Uber's example, some tips on bouncing back from a data breach include:

- Being honest with customers about what happened
- Implementing measures to lessen the likelihood that it will happen again
- Informing customers what measures you've taken to better secure their data

Minimising risk in the future

There are many things you can do to lower the risk of your customers' data being compromised. This can begin with having the right legal policies in place, seeking the appropriate legal advice, and promoting a workplace culture that handles customer data sensitively. Beyond this, you can create a management plan which will help you deal with any security incidents which occur in the future. Customer data is one part of your business where you need to be proactive in protecting your customers' interests, because this directly affects how your business will be seen by customers.

Lawpath®

Have any questions?

Call and speak to Lawpath consultants on

1800 529 728

Find out more