TECHNOLOGY

Making Sure You Are Compliant With Consumer Privacy Acts in 2022

by Natalie Redman

Image Credit | Glenn Carstens-Peters

It's important to ensure your company is compliant with ever-increasing privacy laws.

☑ **INSIGHT** | **FRONTIER**   25 Apr 2022

There has been a lot of change over the years regarding our privacy. The internet led to individuals sharing more of their information and that's where a lack of control over our data, began.

The problem was a lot of these laws and regulations weren't as well enforced as they are now. Many organizations have had to quickly adapt and make changes to their processes in order to abide by these rules to avoid hefty fines and further prosecution.

In this article, you'll get all the information you require to ensure you're compliant with the many consumer privacy acts that have popped up over the years.

The rise of data privacy laws

The rise of data privacy laws has rocketed over the years and it's only a matter of time before most of the world's population is protected. Gartner found that by 2023, **65% of the world's population** will have its personal data covered under some form of privacy regulations.

However not all these regulations are exactly the same and there are certain data privacy laws that are more stringent than the next.

Consumers around the world are getting more say over what is done with their data, whether that's through the EU's recent General Data Protection Regulation (*GDPR*) to the California Consumer Privacy Act (*CCPA*)

What are consumer privacy acts?

Consumer privacy acts are in place to help protect the privacy of every individual who falls into the territory that the individual privacy act covers. For example, GDPR is intended for all those who hold data from customers in the EU, whilst the CCPA is specifically for the customers of California.

The CPRA is the newest of consumer privacy acts to come in and will replace the historic **California Consumer Privacy Act** of 2018. Yes, 2018 has been considered too outdated when it comes to data privacy online!

There are a number of measures that a consumer privacy act covers which include any of the following:

- Passwords and various authorization measures
- 'Do not call' lists
- Limiting the amount of data saved on individuals - such as credit card numbers, social security numbers, browsing history, etc.
- Transactions verified by either email or telephone.
- Encryption and decryption of any data that are transmitted electronically.

Why do we need consumer privacy acts in 2022?

In this modern age where a lot of consumers are online, it's harder to police the actions of others on the internet. There's also been a rise in data breaches, meaning there's an increased need for more consumers across the world to be protected with an appropriate consumer privacy law in place.

How to be compliant with consumer privacy acts

There can be a lot of difficulties faced when trying to remain compliant with consumer privacy acts, especially as they seem to be changing so frequently.

Consider each privacy act's wants and needs

Each and every privacy act that comes into effect is different from the next. Some are more outdated than others and some have complexities that mean more time and resources are required.

Businesses can't be ignorant of the privacy laws in place because quite frankly, the repercussions are seriously damaging. For example, the California Consumer Privacy Act gives every company **30 days to comply** with the law, once the violation has been discovered and regulators have notified them. It's a similar case for GDPR too.

If the issue isn't resolved, then a fine of up to **$7,500 per record** can be dished out. These potentially multiple fines could ruin businesses, particularly those that don't have deep pockets.

Know what data is required

When it comes to the data you're collecting, businesses need to think about what data they require. Less data held by a business can help mitigate the risks, should a data breach occur.

With these privacy laws in place, it's helped a lot of businesses fine-tune their databases and to help reduce the volume of data being held. With the average company **holding 534,465 files** containing sensitive data, there's a lot of damage that could occur from cyber attacks.

Understand what threats exist

Cyberattacks are rife at the moment online and the more that any business can do to help protect their **consumer's data**, the better.

Understanding the threats that are online and the newest methods that these cybercriminals are using to steal or hack data is important. It can help you provide the right level of training for your employees who may hold a lot of responsibility for keeping that data safe.

There's a lot of helpful information out on the internet already when it comes to threats online and being seen to look out for these will hopefully give you a fairer reaction if you're notified of a violation by the consumer privacy act in question.

Limit the data

Limiting the data that you hold onto as a business is going to cause you fewer problems. If you're only holding onto so much, then you're hopefully putting a small target on your back as a result.

Take a look at what data is available to you and what you require from your customers. Only take what you require, rather than taking anything unnecessary.

Protect the data

How you protect your data is really important, especially if you get a violation for breaching data or the rules laid out by the privacy act in question. When you protect your data properly, you help your future self out, should anything happen to your business and its hold of customer data.

There are plenty of security measures that you can take in order to help keep your data safe. From anti-ware software to doing something as simple as strengthening your passwords. The more you can do to protect the data, the better.

It's clear that customers are concerned about their data with **48% indicated** that they'd already switched companies or providers due to data policies or data sharing practices in place. Listen to your customers and see what more can be done to improve data protection.

The benefits of data privacy law

There are some great benefits of having data privacy laws in place. Whilst they can be a pain for businesses that haven't adapted to such stringent measures, in the long run, it helps protect everyone and their data. What are some of the benefits of data privacy laws?

Stay ahead of the competition

Whilst most places around the globe now have some sort of data privacy law in place, not all of them do. It means that your level of data protection could help you stay ahead of your competitors not just nationally but internationally.

By being proactive with your own business's efforts for data privacy, you'll increase the confidence of your customers and any investors or partnerships that you may be looking to secure this year or in the future.

Invest in the relevant and up-to-date software required to protect your data. With stringent data policies in place, it's good to help strengthen customer relationships and to protect valuable information from threats or attacks.

By staying ahead of the competition, you're more likely to attract some of their customers over to your business.

Reduced costs for development

When you install the relevant security and update your data policies, it ends up saving a lot of costs that you may have to spend in the future to help prevent last-minute dangers to your data. You reduce the chances of data loss by having those strong security measures in place from the very beginning.

If you've got basic security and you're able to upgrade or improve it, but don't - that's where you could get into trouble. Insecure software and a lack of data policies in place can cost you a lot of money and time.

Protection against hackers

Data protection is difficult for hackers when you've got the very best software and data policy practices in place. When it comes to accessing sensitive information, you want to make it as challenging as possible for anyone to hack into your data systems.

By actively safeguarding important and confidential data, you can help make yourself less of a threat, especially if you're known widely for providing great data protection.

Better business management

Sticking to the best practices when it comes to adhering to data privacy acts is good for your business management. Being more organized and switched on to what needs changing or improving is going to help improve working relationships too.

It'll keep everyone on the same page when it comes to protecting data whether that's your receptionist to your executive-level employees. Not everyone is well informed when it comes to data protection, so focusing on it as an organization, can certainly help the business as a whole.

There are other consumer privacy acts coming in, like the CPRA in 2023. It's better to act quickly when it comes to adopting your business to comply with these privacy laws in place. There are no exceptions when it comes to data privacy acts, so make sure to prioritize it to the top of your list!

Natalie Redman

Freelance writer for many clients across multiple industries. Natalie has two years of copywriting experience. Natalie has a wide range of experience copywriting for web pages for businesses across many industries. She's also an owner of two blog websites and a Youtube content creator.