STAY COMPLIANT WHEN COLLECTING CLIENT DATA

NAVIGATING GDPR, PRIVACY AND ANTI MONEY LAUNDERING LAWS

fileinvite

Stay Compliant When Collecting Client Data

Navigating GDPR, Privacy and Anti Money Laundering Laws

fileinvite

COLLATED BY FILEINVITE - THE **SIMPLEST** MOST **SECURE** WAY TO GET INFORMATION TO **PROFESSIONALS**

CONTENTS

A quick guide to staying on the right side of privacy, GDPR and anti money-laundering laws

If you collect client data, you're subject to a range of legal requirements. While not onerous, they are important as flouting them can cost you both financially and in terms of your reputation.

Read on to get an understanding of your obligations under GDPR, Privacy and Anti Money Laundering Laws.

1 //
Privacy Act

In most countries, businesses are responsible for protecting their customers' personal information from:

- theft
- misuse
- interference
- loss
- unauthorised access
- modification
- disclosure.

Most countries do not have one piece of legislation that protects personal information, but instead have a variety of sector-specific laws that offer some protection. In many countries, the relevant legislation often goes by the name of the Privacy Act or something similar.

The European Union has controlling legislation for how companies that do business there must handle and manage the personal information they collect. This law, called the General Data Protection Regulation, or GDPR for short, contains several regulations that businesses must follow when they collect customers' information. If your company does business in the EU, you must comply with this law or face substantial fines.

Even if you don't do business in the EU, these regulations are worth being aware of and complying with. Doing so will go a long way to ensuring you act in a customer-friendly way and protect your reputation as an ethical business.

2 //

GDPR – it's about protecting customers' privacy

The GDPR, which took effect in May 2018, is designed to prevent companies from mishandling and abusing the personal information they collect from consumers. It is also intended to streamline the various information protection laws in EU countries and provide consumers with greater privacy over their personal information.

These regulations apply in the UK until Brexit is completed, and the UK has stated it will implement an equivalent law after that.

Companies outside the EU that collect information from people who live in an EU country must also comply with the law. This makes it important for many companies to understand the requirements, regardless of where they might be located. For example, companies that have mobile apps and websites collect information such as IP addresses that are considered to be personal information and must comply with the law.

3 //

What the directive covers

The directive covers any information that could be used to identify someone. This means that the following types of information are covered (note that it doesn't matter what form the information is in):

- Addresses, names, bank information, and GPS location
- IP addresses, posts, email addresses, and social media posts
- Raw user IDs or anonymised information when it is possible to trace backward from the information to identify a person.

In other jurisdictions, personal information might include customers':

- Signature
- Telephone number
- Date of birth
- Medical records
- Bank account details
- Place of work
- Photos
- Videos
- Information about their opinions.

4 //

Complying with the directive

The GDPR is complex, but it can be broken down into some general requirements. Here is a review of the major requirements of this directive.

1 // Have a valid justification for collecting personal information

Companies are only allowed to collect personal information from Europeans if they have valid reasons for doing so. According to the EU, there are specific legal reasons that companies can use to collect information, including:

- Company obtains express consent from the user to collect information
- The information is necessary to fulfill contractual obligations under the contract with the user
- The information is necessary to comply with a different law
- A public authority needs the information to follow its responsibilities
- The company has a legitimate interest in the information.

That last point is designed to prevent companies eliciting customer information that's not needed for the task at hand – you must have actual business needs for the information you collect and are expected to document your reasons for needing it.

What's more, you must define those needs before collecting the information and not after. You must also inform users why they need the information at the time that they ask for it.

You may not resell the information you collect to third parties. For example, a company may not tell users that they need their shipping addresses to send products to them and subsequently sell the address information to advertisers.

There are specific rules that apply to each of the allowed justifications for collecting personal information. For example, there are very specific rules about obtaining express consent from users for collecting their information.

If a company works with certain types of sensitive information such as religion, race, sexual orientation, health information, political party, or biometrics, additional rules apply.

4 // Complying with the directive *continued*

2 // Users control their information

After a company collects information from a customer, the customer must be granted control over the information. The seven rights that users retain over their information are:

1. People must be told why their information is being collected, what you will do with the information, and how long the information will be retained.
2. They must be provided copies of all of the information that has been collected from them if they ask for it.
3. Information must be corrected if a customer tells you it is inaccurate.
4. Customers have the right to have companies delete the information about them.
5. They can ask for companies to stop processing their information.
6. They have the right to transfer their information from one company to another in a digital format.
7. Customers can object to their information being used for specific purposes such as direct marketing.

Companies that collect personal information for profiling or automated decision-making will have to explain how their models work, have a system for appeals in place, and comply with other requirements.

When a customer asserts any of these rights and makes a request, companies must usually process the request within a month. If companies structure their operations to support all of the user rights, they should be compliant with the directive.

4 // Complying with the directive *continued*

3 // Maintain the security of customer information

This law requires companies to maintain the security of the customer information they collect and to conduct regular tests of their security measures. Security measures should be a part of the design process to make them more effective and should not be weak measures that are added on retroactively.

Companies are expected to monitor for breaches and, within 72 hours, report to regulators any that are discovered. They should also maintain records of all breaches.

4 // Maintain accountability, documentation and governance

A large component of complying with the directive is maintaining governance, documentation and accountability. Companies must document their compliance in all aspects.

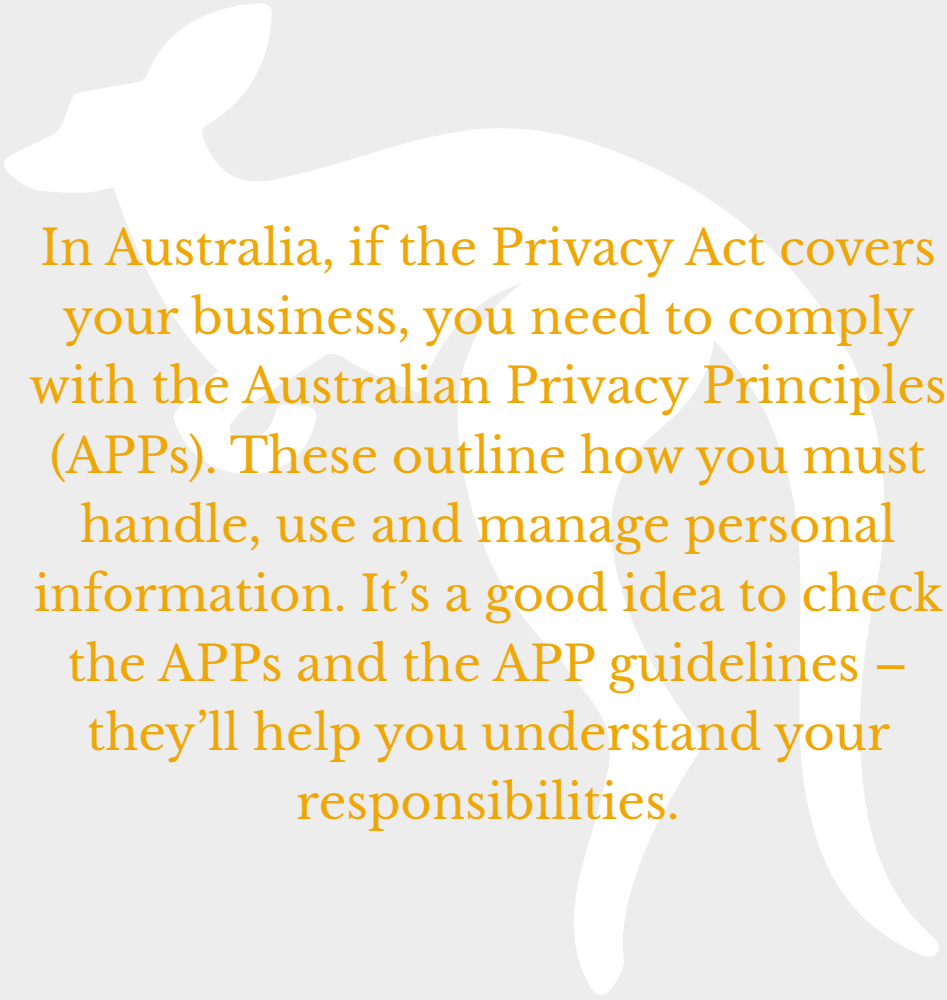
Companies must keep written documentation of their justifications for collecting information, their information retention policies, records of any time the information is shared, and their security policies. Companies that hire third parties for data processing must have written contracts that outline the privacy responsibilities that those parties must follow.

Companies with fewer than 250 employees that only occasionally process the information of EU residents have relaxed rules to follow. They will not have to keep written records except when they collect sensitive information. Large companies with more than 250 employees and those who collect sensitive information should take extra precautions. They will have to complete protection audits regularly and have designated protection officers or DPOs on staff.

5 //

Penalties

The penalties for failing to comply with the law are substantial. They will depend on the circumstances surrounding what occurred, and the regulators can choose to impose a corrective measure with or without fines. Companies that fail to comply with certain requirements may face from 2% to 4% of their total global yearly turnover or from €10m to €20m, whichever is greater. The goal of the regulations is to improve how information is handled rather than to enforce stiff penalties on companies for technical violations. Companies that do their best to follow the regulations will have a reduced risk of the assessment of fines.



In Australia, if the Privacy Act covers your business, you need to comply with the Australian Privacy Principles (APPs). These outline how you must handle, use and manage personal information. It's a good idea to check the APPs and the APP guidelines – they'll help you understand your responsibilities.

6 //

Anti-money laundering and countering financing of terrorism

Similar legislation has been passed across the globe in an effort to reduce money laundering and the financing of terrorism. You should check the specific requirements of your own country, but this section provides a useful guide to the intent behind the law changes in many jurisdictions.

Recent changes to New Zealand's Anti-Money Laundering and Countering Financing of Terrorism (AML/CFT) Act mean that more businesses are now covered by the legislation.

In New Zealand, businesses now covered by the law (who were previously not specifically covered) include real estate agents, conveyancers, many lawyers and accountants, and others.

6 //

Anti-money laundering and countering financing of terrorism *continued*

The AML/CFT Acts require companies to:

- meet specific reporting requirements
- meet specific requirements for identifying their customers
- keep good records.

Industries governed by the legislation differ by country, so ensure you review your local and international obligations. If the law applies to you, you should take steps to ensure you understand and are able to comply with it. A good way to do that is to:

- Appoint an AML compliance officer responsible for making sure you meet your obligations. That can be anyone with a direct reporting line to senior management.
- Identify risks and create a compliance programme, and make it available to senior management.
- Get external advice and/or assistance if needed.

Once your compliance programme is in place, you shouldn't just forget it. Update it regularly by:

- Monitoring clients' accounts or activity with you for potentially suspicious activity.
- Regularly review your risk assessment and compliance programme.
- Have your risk assessment and compliance programme audited every 2 years.
- Submit an annual report to your supervisor.

6 //

Anti-money laundering and countering financing of terrorism *continued*

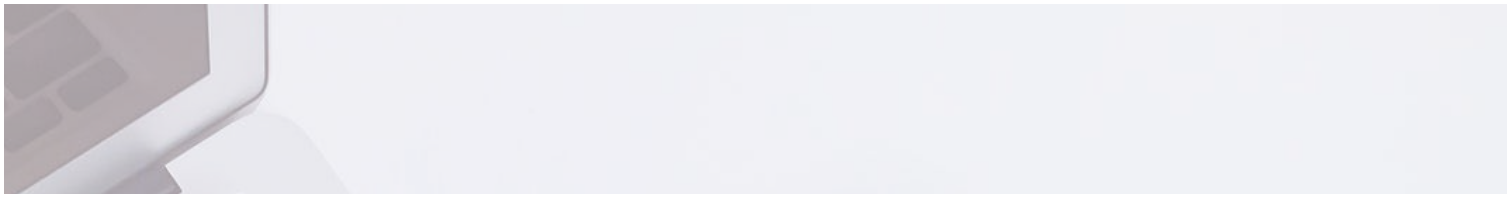
1 // Identify customers

Some companies are now required to verify clients' identity before doing business with them. If a customer pays cash deposits of $10,000 or more, you may also need to ask where the money came from and report the transaction to the Police Financial Intelligence Unit.

2 // Be responsible and don't panic

Following these guides will keep you on the right side of the law. The underlying principle is to do what you know to do to prevent criminals hiding dirty money by using your firm.

If you do that and inadvertently break the law, you will likely receive a warning only. On the other hand, deliberately avoiding your obligations can result in criminal charges.



“It’s our job every day to make every important aspect of the customer experience a little bit better.”

– JEFF BEZOS

At FileInvite, ensuring client onboarding and document collection meets the ever more rigorous standards of legislation around privacy and personal data security is paramount.

Find out how FileInvite can help you with compliant, secure, client document and data collection.

CURIOUS ABOUT HOW FILEINVITE CAN HELP YOUR BUSINESS?

CONTACT US

fileinvite