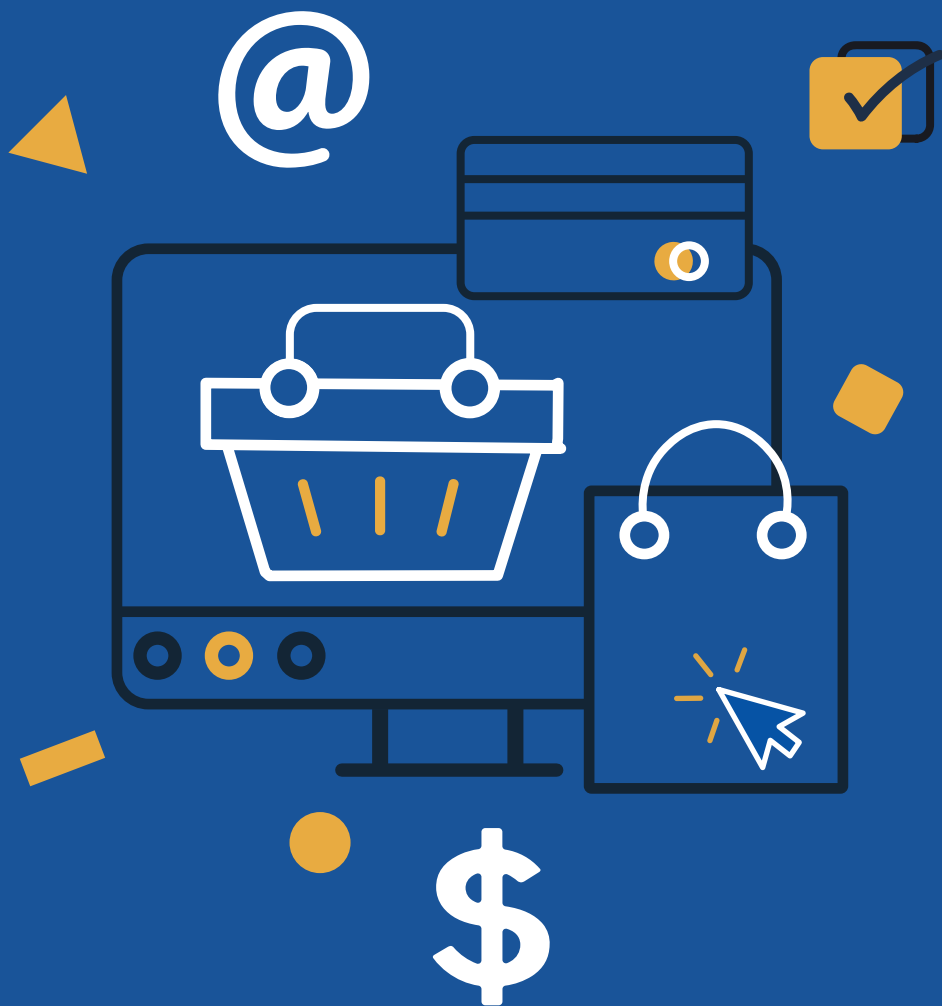




Legal Guides for Ecommerce



Preface

There's a lot to consider when starting a retail business: marketing, staffing, accounting. Can you take a salary and still keep the lights on? What will happen if your suppliers suddenly raise their prices? Will your website ever stop crashing?

Getting to grips with the legal implications of running an ecommerce store might be pretty far down on your list of priorities. But few things could be more important. Customers and suppliers will come and go. Blips on the balance sheet are inevitable. Ending up in court, however, can easily sink a small business.

In market economies, the contract is sacred. And an ecommerce store hopes to enter into as many contracts as possible. Every time you make a sale, after all, you take on contractual obligations. The better your understanding of your position under the law, the more control you can exercise over the terms of these obligations. Similarly, the less you understand about your legal position, the more likely you are to encounter problems.

However, it isn't only buying and selling that you have to worry about. While the Internet is well-established as a medium of exchange, privacy law is still playing catch-up. The passing of increasingly strict data protection laws has meant a huge amount of extra work for businesses. And if you think that's an exaggeration, it might be because you haven't done what's required.

This book is an exploration of the legal issues that every ecommerce store will have to deal with. It will give you an edge over any of your competitors who don't understand their legal obligations.

This book is not legal advice, and it isn't designed to get you out of legal trouble. It's not filled with legal theory or musings on the development of case law. Think of it as a guidebook, filled with practical information.

This book will help you understand what you need to do, and how to do it. You're probably too busy running or preparing your business to worry about much more than that.

Table of Contents

Preface.....	1
Table of Contents.....	2
Chapter 1: What this Book Covers.....	6
Privacy Policies.....	6
Terms and Conditions Agreements.....	7
Return and Refund Policies.....	7
Disclaimers.....	8
Proper Consent For Email Marketing.....	8
Chapter 2: Creating Your Own Store vs Using a Third Party Platform.....	9
Creating Your Own Ecommerce Store.....	9
Advantages of a Creating Your Own Ecommerce Store.....	10
Disadvantages of Creating Your Own Ecommerce Store.....	10
Legal Considerations When Creating Your Own Ecommerce Store.....	11
Using a Third-Party Platform.....	12
Advantages of Using a Third-Party Platform.....	12
Disadvantages of Using a Third-Party Platform.....	12
Legal Considerations when Choosing a Third-Party Platform.....	13
Case Study.....	14
Which Option is Best?.....	14
Chapter 3: Privacy Policy and Ecommerce Businesses.....	16
Laws on Collecting Personal Information.....	16
United States.....	16
European Union.....	17
Other Jurisdictions.....	17
Third Parties Your Ecommerce Store Shares Data With.....	18
Ecommerce Platforms.....	18
Payment Processors.....	19
App Marketplaces.....	19
Advertising Services.....	21
Email Marketing Services.....	21
Website Analytics Services.....	22
What Your Privacy Policy Should Cover.....	23
Types of Information You Collect.....	23
Your Reasons For Collecting Personal Information.....	25
Third Parties You Share Information With.....	26
Privacy Rights and Opt-outs.....	27
Other Required Information.....	29
Where to Display Your Privacy Policy on Your Ecommerce Store.....	30

On Your Website.....	30
In Your Mobile App.....	32
Other Locations.....	34
Case Study.....	35
Chapter 4: Terms & Conditions and Ecommerce Businesses.....	38
What Your Terms and Conditions Agreement Should Include.....	38
Limitation of Liability.....	39
Laws on Limitation of Liability Clauses.....	40
Different Types of Damages.....	42
Limiting Liability to a Specific Amount.....	44
Disclaimer of Warranties.....	45
Laws on Disclaimers of Warranties.....	46
Provided “As Is”.....	48
Returns and Refunds.....	49
Delivery Information.....	50
Delivery Options.....	51
Shipping Costs.....	52
Timescales for Dispatch and Delivery.....	52
Delivery Restrictions.....	53
Customs and Duties.....	54
Payment Methods.....	54
Other Information.....	55
Where to Display Your Terms and Conditions on Your Ecommerce Store.....	56
On Your Website.....	56
Within Your Mobile App.....	57
Other Locations.....	58
Case Study.....	58
Chapter 5: Return & Refund Policy and Ecommerce Businesses.....	60
Laws on Returns and Refunds.....	60
United States.....	61
European Union.....	63
Legal Warranty.....	64
Returns for Online Purchases.....	64
Other Jurisdictions.....	64
What to Include in Your Return and Refund Policy.....	65
Whether You Accept Returns.....	65
Exceptions and Conditions.....	66
Instructions for Making a Return.....	69
Where to Display Your Return and Refund Policy on Your Website.....	71
On Your Website.....	71
On a Mobile App.....	72
Other Locations.....	74

Case Study.....	75
Chapter 6: Disclaimers and Ecommerce Businesses.....	77
Responsibilities of Different Types of Businesses.....	77
Manufacturers.....	78
Importers.....	79
Companies that Customize or Service Products.....	79
Potentially Dangerous Goods.....	80
Responsible Use Warning.....	82
California's Proposition 65.....	82
Pharmaceuticals and Alternative Medicines.....	83
"Results Not Typical" Disclaimers.....	85
Sports Recovery.....	86
Cosmetics.....	86
Age-Restricted Items.....	87
Offers and Promotions.....	87
Restrictions on Normal Service.....	88
Affiliate Link Disclaimers.....	89
Results Not Typical Disclaimers.....	90
Where to Display Your Disclaimers.....	91
Case Study.....	94
Chapter 7: Email Marketing and Ecommerce Businesses.....	95
Laws on Email Marketing.....	95
United States.....	96
At the Top of Your Email.....	96
At the Bottom of Your Email.....	97
Canada.....	98
Implied Consent.....	99
Express Consent.....	99
Compliant Emails.....	101
Australia.....	101
Australian Link.....	101
Inferred Consent.....	102
Express Consent.....	102
Compliant Emails.....	102
European Union.....	103
Affirmative Consent.....	103
Granular Consent.....	104
Compliant Emails.....	106
Laws Across the EU.....	106
Other Major Economies.....	106
Case Study.....	109
Chapter 8: Growing Your Ecommerce Store.....	110

Analytics..... 110

 Analytics and Privacy Law..... 111

Session Recording Tools..... 112

 Session Recording Tools and Privacy Law..... 112

Remarketing..... 115

 Remarketing and Privacy Law..... 115

Case Study..... 116

Note From the Editors..... 118

Chapter 1:

What this Book Covers

Ecommerce is increasingly accessible to businesses. It's relatively simple to integrate an ecommerce store into your existing website using one of many ecommerce platforms such as **Shopify** and **BigCommerce**. Or, with some web development expertise, you can create your own.

By carving out a place in this growing marketplace, your business can take advantage of the potential benefits that ecommerce holds over traditional brick-and-mortar outlets - including lower overheads, wider reach, and personalized advertising.

Regardless of whether you choose to use an existing ecommerce platform or create your own, you need to take steps to ensure that you are complying with the **legal requirements** associated with online selling. You also need to be aware of the **legal issues** that can come up for online retailers, and how you can effectively protect your business against legal claims.

Here's a brief overview of some legal agreements your ecommerce store will need. Each will be covered in great detail in later chapters.

Privacy Policies

[A Privacy Policy](#) sets out what types of personal information you collect from your users and what you intend to do with that information. "Personal information" means anything that could be used to identify a person including but definitely not limited to names, payment account details, mailing addresses and email addresses.

A Privacy Policy is essential for any business that operates an ecommerce store. It's a legal requirement under various national and regional laws, such as:

- The California Online Privacy Protection Act ([CalOPPA](#))
- The California Consumer Privacy Act of 2018 ([CCPA/CPRA](#))
- The European Union (EU) General Data Protection Regulation ([GDPR](#))
- Canada's Personal Information Protection and Electronic Documents Act ([PIPEDA](#))
- Singapore's Personal Data Protection Act 2012 ([PDPA](#))
- Australia's Privacy Act 1988 ([Privacy Act](#))

Each of these laws has a different set of requirements. And in many cases, particularly with regard to California and EU law, your business doesn't have to be based in a jurisdiction to be bound by

its laws. **So, as long as you have customers within that area, you will need to comply with the laws of that area.**

Many ecommerce platforms also require that their users have a Privacy Policy. After all, they want you to demonstrate transparency and comply with the law.

Terms and Conditions Agreements

It's important to ask your customers to [agree to certain Terms and Conditions](#) when they make a purchase from your ecommerce store. This is an essential way to guard against any potential legal issues that might arise.

By selling goods or services to your customers, your business is entering into a **contract** with them. You have certain **obligations** under this contract, and your customer has certain **rights**. Your business has the opportunity, and the responsibility, to set the terms of your agreement with your customers in a fair way that benefits both parties.

A robust set of Terms and Conditions means that your customers should know where they stand.

You can use Terms and Conditions to:

- Choose the **legal jurisdiction** in which any disputes will be settled
- Explain the reasons that you might have to **refuse service** to a customer
- Manage issues of **intellectual property** and trademark

While a Terms and Conditions agreement isn't required by law, it's an exceptionally important agreement for businesses to have.

Return and Refund Policies

Legal problems might arise if your customers are unhappy with something they've purchased from your ecommerce store. The best way to manage these types of issues is by having [a clear Return and Refund Policy](#) that sets out:

- The reasons that a customer might be entitled to a refund
- The period over which a customer can request a refund
- What a customer must do to initiate a return and refund
- Whether you'll offer a cash refund, an exchange, or store credit
- Your policy around return shipping costs

Different countries and states have different laws around returns and refunds that your ecommerce store may need to comply with.

There's no federal law regulating returns in the U.S., but there are laws **specific to some states**, such as [California's](#) Civil Code Section 1723.

Business to consumer selling rules in the EU are [governed by](#) the Consumer Rights Directive. **Individual EU countries** have some quite strict retail laws, such as the UK's Consumer Rights [Act 2015](#).

The business of selling goods and services is a potential legal minefield. But if you have **clear and robust policies and terms in place**, you'll know what to expect if legal issues do arise. This means you'll be in a position to offer your customers the best ecommerce service possible while protecting your assets and reputation.

Disclaimers

[Disclaimers are short statements](#) or clauses in a legal agreement that work to inform your reader of something important. While most aren't legally required, they do work to help limit your legal liability in the event something goes wrong.

For example, you can benefit greatly from including a warranty saying that you aren't responsible for any injuries that result from the use of your products. Imagine that you sell snowboards, and you can see how this disclaimer will help keep anyone who has a snowboarding accident while using your board from trying to sue you as somehow being responsible.

Some commonly used ecommerce disclaimers include but aren't limited to the following:

- Results not typical
- Medical advice
- Warranty
- Affiliate links

Proper Consent For Email Marketing

If you engage in the lucrative act of email marketing, you will need to comply with requirements for getting [consent](#) to send marketing messages. These laws vary by region, and will be addressed in detail later on. For now, be aware that there are rules to follow here for your ecommerce store to operate compliantly.

Chapter 2:

Creating Your Own Store vs Using a Third Party Platform

A properly functioning ecommerce store seamlessly integrates the front end and back end of your retail website. It not only enables customers to buy your products, but it also makes it more likely that they'll do so. An ecommerce store should fulfill your customers' purchases in a quick and secure way.

A poorly functioning ecommerce store will not only make you lose sales, but could land your business in serious legal trouble. Data breaches happen, and they can have disastrous consequences for any company.

Ecommerce is no longer the domain for those with advanced web development expertise or access to an in-house IT department. You can now outsource the software development and payment handling aspects of your store to an out-of-the-box third-party ecommerce platform. This allows anyone to create an ecommerce store in literally minutes.

But doing this doesn't relinquish you from guarding against potential legal issues.

Creating Your Own Ecommerce Store

An ecommerce store has several elements. For example, there's the shopping cart software - the user interface that allows your customers to choose products. There's the payments gateway, which allows your customers to pay for those products. The payments gateway links the front-end of your website with a payment processing bank.

Creating a payments gateway from scratch would be a huge undertaking. Some of the implications include:

- Setting up a merchant account with a major bank and letting them know your intentions to become a payment processor
- Becoming certified with the bank's card acquirer (e.g. Worldpay)
- Becoming Payment Card Industry Data Security Standard (PCI DSS)-compliant. This involves an annual certification process

Taking on a project like this and dealing with the associated legal ramifications goes beyond the scope of this book.



Image: Paypal logo



Image: Stripe logo

However, you could consider developing your own shopping cart software, then using a third-party payment gateway like [PayPal](#) or [Stripe](#) to take your customers' payments. This is an option for those who want to have a more customized online store and maintain more control over it. But it does take a lot of work.

You'll need to have knowledge of web development to create your own online store, including:

- Client and server-side coding techniques and languages
- Database access
- Domains, DNS, HTTP requests and responses

Advantages of a Creating Your Own Ecommerce Store

The advantages of building your own software very much depend on the context in which you're running your business.

- You can create something truly tailored to your brand.
- You maintain control over your software indefinitely.
- You are free to experiment with the framework (within limits), and you might have greater opportunities to run conversion rate optimization.

Disadvantages of Creating Your Own Ecommerce Store

Taking this level of control over your operations is not an unequivocally good thing.

- Development and maintenance will be resource-heavy.
- It will take real skill to build software that looks good and functions well.
- Each extra feature (e.g. abandoned cart recovery) will require a whole new round of development.

Legal Considerations When Creating Your Own Ecommerce Store

The more control you have over your ecommerce website, the more work you'll have to do to keep your customers' information safe.

Creating shopping cart software may not by itself require you to become PCI-compliant. But it does require you to take steps to keep your customers' data safe.

The EU has very strict data protection laws. Although your business might not be operating in the EU, it's worth considering a principle from EU privacy law here.



Image: EU flag

[Article 25](#) of the GDPR speaks of “data protection by design and default.” Under [Recital 78](#), developers are required to implement technical measures like [pseudonymization](#) and data minimization when creating software.

When it comes to collecting your customers' personal information, the following principles should apply throughout your development process:

- Only collect the personal information from your customers that you absolutely need.
- Ensure that your customers' personal information is deleted at the earliest opportunity.
- You'll normally need to ensure that your customers' personal information doesn't appear in your log files. This might happen if you're collecting log data from payment forms, for example.

You also need to consider how you might guard against, respond to, and recover from [data breaches](#).

- Consider how your website can continue to function throughout denial of service (DNS) attacks.
- Maintain effective security measures such as encryption, firewalls, and virus protection.
- Make sure you have a system in place that allows you to inform your customers and any relevant data protection authorities if a breach occurs.

As [privacy and data protection laws](#) continue to become stricter and more comprehensive, providing a secure website that keeps your customers' data safe is increasingly a matter of law.

Using a Third-Party Platform

Businesses now have scores of different ecommerce platforms to choose from. The software is written and administered by someone else, and you simply have to follow their instructions and agree to their terms to use it on your website.

These platforms vary in what extra features they'll provide, and in what they require you to do to comply with their terms.

It's important to remember that outsourcing some of the groundwork around taking payments and maintaining your store **doesn't mean outsourcing all of your legal obligations**. There are actually some legal implications in using a third-party platform that aren't relevant if you're doing everything yourself. Overall, however, this option is a lot simpler.

Advantages of Using a Third-Party Platform

There are obvious benefits to choosing to integrate a third-party ecommerce platform into your website rather than developing one from scratch:

- You don't need to spend time, effort and resources developing the platform.
- You can choose the extra features you want without having to develop them individually.
- You have a support team available that's trained in delivering advice on how to make the most out of the platform.

Disadvantages of Using a Third-Party Platform

There are potentially some downsides to using a third-party ecommerce platform. These are mostly relevant only in the long term.

- You could have serious problems if the platform provider ever goes out of business.
- You will have to accept the platform provider's terms. Only very large merchants will have much hope of negotiating on prices or contractual clauses.
- You're trusting a third party company with your customers' personal data.

Even with that having been said, there are positives to these negatives.

Yes, you're handing over some control over one aspect of your business to a third party. But keeping control over this part of your business would divert resources away from actually selling your products and services.

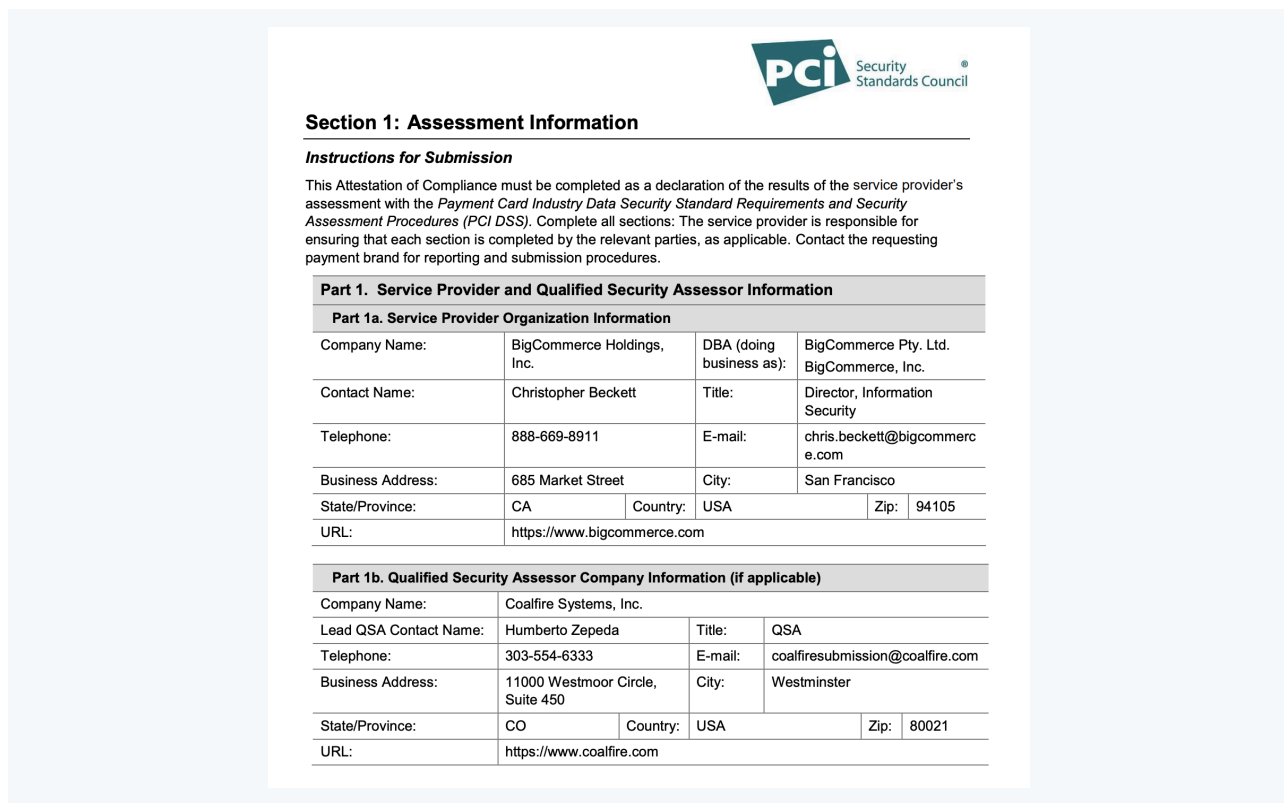
You're trusting a third party company with your customers' personal data. You need to check that they've done the work required to keep it safe. And you need to keep your customers informed each step of the way. But it's very likely that a third-party company whose business is payment-processing will do a better job of keeping it secure than you could.

Legal Considerations when Choosing a Third-Party Platform

We've all been guilty of agreeing to Terms and Conditions that we haven't read. But when it comes to choosing an ecommerce platform, it's not enough to quickly scroll to the bottom and click "I Agree." You're obliged, both legally and on principle, to ensure that you know what you're agreeing to.

You must ensure that any third party platform you choose is PCI DSS-compliant. If you're asked to provide proof that your ecommerce store is compliant, you'll need to produce an Attestation of PCI DSS Compliance.

Here's an example:



The image shows a sample of a PCI DSS Attestation of Compliance form for onsite assessments, specifically Section 1: Assessment Information. The form is titled "Section 1: Assessment Information" and includes instructions for submission. It is divided into two main parts: Part 1a. Service Provider Organization Information and Part 1b. Qualified Security Assessor Company Information (if applicable). The form is filled out with example data for BigCommerce and Coalfire Systems, Inc.

PCI Security Standards Council

Section 1: Assessment Information

Instructions for Submission

This Attestation of Compliance must be completed as a declaration of the results of the service provider's assessment with the *Payment Card Industry Data Security Standard Requirements and Security Assessment Procedures (PCI DSS)*. Complete all sections: The service provider is responsible for ensuring that each section is completed by the relevant parties, as applicable. Contact the requesting payment brand for reporting and submission procedures.

Part 1. Service Provider and Qualified Security Assessor Information

Part 1a. Service Provider Organization Information

Company Name:	BigCommerce Holdings, Inc.	DBA (doing business as):	BigCommerce Pty. Ltd. BigCommerce, Inc.		
Contact Name:	Christopher Beckett	Title:	Director, Information Security		
Telephone:	888-669-8911	E-mail:	chris.beckett@bigcommerce.com		
Business Address:	685 Market Street	City:	San Francisco		
State/Province:	CA	Country:	USA	Zip:	94105
URL:	https://www.bigcommerce.com				

Part 1b. Qualified Security Assessor Company Information (if applicable)

Company Name:	Coalfire Systems, Inc.				
Lead QSA Contact Name:	Humberto Zepeda	Title:	QSA		
Telephone:	303-554-6333	E-mail:	coalfiresubmission@coalfire.com		
Business Address:	11000 Westmoor Circle, Suite 450	City:	Westminster		
State/Province:	CO	Country:	USA	Zip:	80021
URL:	https://www.coalfire.com				

Image: PCI DSS Attestation of Compliance for Onsite Assessments - Service Providers - BigCommerce Section 1: Assessment Information

You'll need to consider whether the platform of your choice is compliant with the privacy laws of your customers' home countries. **If you're trading in the EU, for example, is the platform compatible with the EU's main privacy law, the GDPR?**

Case Study

A US-based ecommerce business, Solomon's Shoes, hopes to sell shoes to customers in the EU. Under [Article 3](#) of the GDPR, any business that offers goods or services in the EU is bound by EU privacy law, whether it has any physical presence in the EU or not.

Solomon's Shoes has a website. It asks customers to submit their names, credit card details, billing and shipping addresses, email addresses to this website. Solomon's Shoes asks its customers for this information so it can sell them shoes.

Solomon's Shoes is, therefore, deciding how and why its customers should provide it with their personal information. In legal terms, Solomon's Shoes qualifies as a "data controller" under [Article 4](#) of the GDPR.

Solomon's Shoes plans to use **Shopify** as its ecommerce platform. Shopify will carry out certain activities for Solomon's Shoes in order to help it serve its customers. Because Shopify is handling personal information on behalf of Solomon's Shoes, Shopify qualifies as a "data processor" under Article 4 of the GDPR.

[Article 28](#) of the GDPR requires data controllers, such as Solomon's Shoes, to ensure that any data processors it employs, such as Shopify, comply with the GDPR. This is a legal requirement on Solomon's Shoes. It's not good enough for a data controller to say that it didn't know that a data processor wasn't legally compliant.

Happily, [Shopify](#) has taken the necessary steps to comply with the GDPR and has added a [Data Processing Addendum](#) to make its duties under EU law clear.

Which Option is Best?

It's clear that using a third party platform to provide a payment gateway and shopping cart for your ecommerce website will save you a lot of work. But there's no getting away from your legal obligations.

You need to carefully check that any platform you use is legally compliant before you ask your customers to submit their personal information to it. This is true even if you're just using a payments gateway like PayPal, or an out-of-the-box ecommerce platform like Shopify. This will require some knowledge of the privacy laws and payment protection regulations of the jurisdictions in which your website operates.

You'll need to inform your customers that you'll be sharing their personal information with third parties when they make a purchase from you. You can do this in your **Privacy Policy**. You may also need to make reference to the privacy implications of some of the platform's functions.

We'll look at this in more detail in the next chapter.

Chapter 3:

Privacy Policy and Ecommerce Businesses

While some policies like Terms and Conditions or Return and Refund Policies are strongly recommended, a [Privacy Policy](#) (sometimes called a Privacy Notice, Privacy Statement or Data Policy) is a **legal requirement**, and is also mandatory under the terms of some third-party ecommerce platforms.

Businesses are collecting more and more personal information from their customers. It's not just social media organizations and advertising companies that do this. Ecommerce stores also collect some pretty important personal information from their customers. This doesn't just refer to credit card details. [Personal information](#) means **anything that can be used to identify a person**.

Laws on Collecting Personal Information

Different privacy laws define personal information in slightly different ways. It's important to remember that in many cases, you don't only have to obey the law of the country in which your business is based. You also have to obey the law of the **countries where your customers live**.

United States

At the federal level, privacy law in the U.S. is very weak. U.S. states have passed laws which require companies to act in the event of a data breach.

For example, if you're planning to sell goods or services to Californians - or if your website collects the personal information of California residents - you'll need to comply with privacy laws including the California Online Privacy Protection Act ([CalOPPA](#)). This applies anywhere in the world - whether you're based in Los Angeles or Laos.

CalOPPA gives several examples of "personally identifiable information" (personal information), some of which you're likely to be collecting via your ecommerce store:

- A first and last name
- A home or other physical address
- An email address
- A telephone number

If you collect any of these and your website visitors (not necessarily your customers) include California residents **you must comply with CalOPPA**.

View [our directory of U.S. state privacy laws](#) for up to date status on current laws. CalOPPA is just an example of one.

European Union

The EU's General Data Protection Regulation ([GDPR](#)) is arguably the world's toughest privacy law. Its broad scope and wide territorial reach had many businesses scrambling to adjust their Privacy Policies and practices in the early part of 2018. Your business is affected if it provides goods or services to customers in the EU.

The GDPR defines "[personal data](#)" (personal information) as: "*any information relating to an identified or identifiable natural person.*"

This has been interpreted very broadly by the EU's courts. In addition to the examples listed above, personal information under the GDPR includes:

- [Cookie](#) data
- IP addresses (including *dynamic* IP addresses)
- Any "online identifiers"

This is the type of information you can easily collect on your website even if you don't specifically ask your customers for it, and even if they don't make a purchase. You'll likely collect this sort of data in your log files, and if you run conversion rate optimization or website analytics.

You have to be very careful about people's personal information if you're hoping to attract EU visitors to your website.

Other Jurisdictions

The above examples are taken from two major economies. There are privacy laws that define personal information in a similar way in other countries, too, such as:

- [Canada](#)
- [Australia](#)
- [Singapore](#)

- [Malaysia](#)
- [South Korea](#)
- [Vietnam](#)
- [Brazil](#)

Note that this is not an exhaustive list.

As businesses collect greater amounts of personal information online, governments are increasingly introducing tighter controls. But the aim is not to prevent commerce or stifle innovation. So long as you're behaving legally responsibly, it's possible to **take the necessary steps to comply with any privacy law**.

Third Parties Your Ecommerce Store Shares Data With

Running an ecommerce store isn't something your business will do alone. There's a host of different services out there designed to help your business thrive. Having a Privacy Policy is often a requirement for using these services.

When your customers interact with these services on your website, you're asking them to share their personal information with a third party. This is something you need to be clear about in your Privacy Policy.

Ecommerce Platforms

Having a Privacy Policy is a **requirement** if you're using a third-party ecommerce platform. The legally-binding Terms and Conditions you agree to when you sign up to use the platform will usually contain a clause about this.

Here's how [BigCommerce](#) addresses this:

2. Merchants.

- 2.1. **Merchant Policies.** Merchants should help Shoppers understand how the Merchant, BigCommerce and relevant third parties collect and process Shoppers' Personal Data. To that end, Merchants must:
- post an accurate privacy policy on their storefront that complies with all applicable laws and regulations;
 - process Personal Data in accordance with applicable laws and, to the extent required under such laws, provide notice to and obtain informed consent from Shoppers for the use and access of their Personal Data by BigCommerce and other third parties; and
 - if the Merchant is collecting any Sensitive Personal Data from Shoppers, obtain affirmative, explicit, and informed consent and allow such Shoppers to revoke their consent to the use and access of Sensitive Personal Data at any time.

Image: BigCommerce Privacy Policy: Merchants clause with Privacy Policy highlighted

It reads:

2. Merchants.

2.1. Merchant Policies. Merchants should help Shoppers understand how the Merchant, BigCommerce and relevant third parties collect and process Shoppers' Personal Data. To that end, **Merchants must:**

- **post an accurate privacy policy** on their storefront that complies with all applicable laws and regulations;
- process Personal Data in accordance with applicable laws and, to the extent required under such laws, provide notice to and obtain informed consent from Shoppers for the use and access of their Personal Data by BigCommerce and other third parties; and
- if the Merchant is collecting any Sensitive Personal Data from Shoppers, obtain affirmative, explicit, and informed consent and allow such Shoppers to revoke their consent to the use and access of Sensitive Personal Data at any time.

Payment Processors

Even if you aren't using a third-party ecommerce platform and instead are opting to integrate a payment processor like PayPal or Stripe into your website, you'll need a Privacy Policy. Your customers need to be completely clear on who you're sharing their data with.

This is a requirement under a number of privacy laws including CalOPPA, which states that your Privacy Policy must disclose:

"the categories of third-party persons or entities with whom the operator may share [...] personally identifiable information."

Under the GDPR, you must make your customers aware of:

"the recipients or categories of recipients of [their] personal data, if any."

App Marketplaces

If your ecommerce store has a mobile application, you'll need a Privacy Policy to get your app into Google Play Store ([Android](#)) or Apple's App Store ([iPhone](#)).

Here's what [Google](#) says about how developers must handle their users' data:

You must be transparent in how you handle user data (for example, information collected from or about a user, including device information). That means disclosing the access, collection, use, handling, and sharing of user data from your app, and limiting the use of the data to the policy compliant purposes disclosed. Please be aware that any handling of personal and sensitive user data is also subject to additional requirements in the "Personal and Sensitive User Data" section below. These Google Play requirements are in addition to any requirements prescribed by applicable privacy and data protection laws.

Image: Google Play: Privacy Security and Deception - User Data requirements section

It reads:

You must be transparent in how you handle user data (for example, information collected from or about a user, including device information). That means disclosing the access, collection, use, handling, and sharing of user data from your app, and limiting the use of the data to the policy compliant purposes disclosed. Please be aware that any handling of personal and sensitive user data is also subject to additional requirements in the "Personal and Sensitive User Data" section below. These Google Play requirements are in addition to any requirements prescribed by applicable privacy and data protection laws.

And here's an extract from [Apple's](#) App Store Review Guidelines:

5.1.1 Data Collection and Storage

(i) Privacy Policies: All apps must include a link to their privacy policy in the App Store Connect metadata field and within the app in an easily accessible manner. The privacy policy must clearly and explicitly:

- Identify what data, if any, the app/service collects, how it collects that data, and all uses of that data.
- Confirm that any third party with whom an app shares user data (in compliance with these Guidelines) — such as analytics tools, advertising networks and third-party SDKs, as well as any parent, subsidiary or other related entities that will have access to user data — will provide the same or equal protection of user data as stated in the app's privacy policy and required by these Guidelines.
- Explain its data retention/deletion policies and describe how a user can revoke consent and/or request deletion of the user's data.

Image: Apple App Store Review Guidelines: Data Collection and Storage section - Privacy Policy Link required section highlighted

It reads:

5.1.1 Data Collection and Storage

(i) Privacy Policies: All apps must include a link to their privacy policy in the App Store Connect metadata field and within the app in an easily accessible manner. The privacy policy must clearly and explicitly:

- Identify what data, if any, the app/service collects, how it collects that data, and all uses of that data.
- Confirm that any third party with whom an app shares user data (in compliance with these Guidelines) — such as analytics tools, advertising networks and third party SDKs, as well as any parent, subsidiary or other related entities that will have access to user data — will provide the same or equal protection of user data as stated in the app's privacy policy and required by these Guidelines.
- Explain its data retention/deletion policies and describe how a user can revoke consent and/or request deletion of the user's data.

Advertising Services

There are privacy considerations when it comes to advertising, particularly with regard to practices like [remarketing](#).

If you use services such as any of the following, review their requirements for your Privacy Policy:

- [AdRoll](#)
- [Twitter](#)
- [Perfect Audience](#)
- [AppNexus](#)

Email Marketing Services

Email direct marketing campaigns help ecommerce businesses acquire new customers and maintain loyalty among existing customers. It's important (in most contexts) that you [gain your customers' consent](#) for direct marketing.

If you're using a third-party email marketing service, it's also important that you make it clear that you'll be sharing your customers' data with this service.

A Privacy Policy is a requirement under the terms of some of these companies. For example, here's what [Mailchimp](#) requires in its terms:

You agree, represent, and warrant to Mailchimp that:

1. You will clearly post, maintain, and abide by a publicly accessible privacy notice on the digital properties from which the underlying data is collected that (a) satisfies the requirements of applicable Data Protection Laws, (b) describes your use of the Service, and (c) includes a link to our Global Privacy Statement.

Image: Mailchimp Terms of Use: Privacy Policy requirement

It reads:

You agree, represent, and warrant to Mailchimo that:

1. ***You will clearly post, maintain, and abide by a publicly accessible privacy notice on the digital properties from which the underlying data is collected that (a) satisfies the requirements of applicable Data Protection Laws, (b) describes your use of the Service, and includes a link to our Global Privacy Statement.***

Website Analytics Services

You may wish to run analytics on your website in order to track your customers' and visitors' behavior. This can help you increase sales and drive traffic to your website.

The EU, in particular, is very clear that the types of information collected from individuals by web analytics can constitute personal information. Such services collect information about visitors' behavior on your site and what devices they use to access your site. This qualifies as "monitoring behavior" under EU law.

Besides which, maintaining a Privacy Policy is a **prerequisite** of using some analytics services, such as [Google Analytics](#):

7. Privacy.

You will not and will not assist or permit any third party to pass information, hashed or otherwise, to Google that Google could use or recognize as personally identifiable information, except where permitted by, and subject to, the policies or terms of Google Analytics features made available to You, and only if, any information passed to Google for such Google Analytics feature is hashed using industry standards. You will have and abide by an appropriate Privacy Policy and will comply with all applicable laws, policies, and regulations relating to the collection of information from Users. You must post a Privacy Policy and that Privacy Policy must provide notice of Your use of cookies, identifiers for mobile devices (e.g., Android Advertising Identifier or Advertising Identifier for iOS) or similar technology used to collect data. You must disclose the use of Google Analytics, and how it collects and processes data. This can be done by displaying a prominent link to the site "How Google uses information from sites or apps that use our services", (located at www.google.com/policies/privacy/partners/, or any other URL that Google may provide from time to time). You will use commercially reasonable efforts to ensure that a User is provided with clear and comprehensive information about, and consents to, the storing and accessing of cookies or other information on the User's device where such activity occurs in connection with the Service and where providing such information and obtaining such consent is required by law.

Image: Google Analytics Terms of Service: Updated Privacy clause

It reads:

7. Privacy.

You will not and will not assist or permit any third party to pass information, hashed or otherwise, to Google that Google could use or recognize as personally identifiable information, except where permitted by, and subject to, the policies or terms of Google Analytics features made available to You, and only if, any information passed to Google for such Google Analytics feature is hashed using industry standards. You will have and abide by an appropriate Privacy Policy and will comply with all applicable laws, policies, and regulations relating

to the collection of information from Users. You must post a Privacy Policy and that Privacy Policy must provide notice of Your use of cookies, identifiers for mobile devices (e.g., Android Advertising Identifier or Advertising Identifier for iOS) or similar technology used to collect data. You must disclose the use of Google Analytics, and how it collects and processes data. This can be done by displaying a prominent link to the site "How Google uses from sites or apps that use our services", (located at www.google.com/policies/privacy/partners/, or any other URL that Google may provide from time to time). You will use commercially reasonable efforts to ensure that a User is provided with clear and comprehensive information about, and consents to, the storing and accessing of cookies or other information on the User's device where such activity occurs in connection with the Service and where providing such information and obtaining such consent is required by law.

What Your Privacy Policy Should Cover

To ensure that you're handling your customers' personal data in a way that complies with any of the laws we've discussed, you'll need to have a Privacy Policy. You must make your Privacy Policy available to your customers so that they know, amongst other things:

- What types of information you're collecting from them
- How you'll collect it
- What you'll use the information for

Writing a Privacy Policy is about more than just providing transparent information to your customers. It's a process that will help you make sure that your privacy practices are legal, ethical and safe.

Let's take a look at the things your [ecommerce store's Privacy Policy](#) will need to include.

Types of Information You Collect

As noted above, all ecommerce stores will collect **personal information** from their customers in various ways. Take this opportunity to think carefully about what information you need, and how you're getting it.

Your Privacy Policy should spell out exactly **what types** of information you collect, and **how** you collect it.

Let's take a look at how [Amazon UK](#) does this. Amazon breaks the personal information it handles into three broad types:

1. Information customers **provide to** Amazon
2. Information Amazon **collects** from customers **automatically**

3. Information Amazon **receives** about customers from other sources

Here's a sample of **how** Amazon customers might provide Amazon with personal information:

16. Examples of Information Collected

Information You Give Us When You Use Amazon Services

You provide information to us when you:

- search for products or services in our stores;
- place an order through Amazon Services;
- download, stream, view, or use content on a device, or through a service or application on a device;
- provide information in [Your Account](#) (and you might have more than one if you have used more than one e-mail address or mobile number when shopping with us) or [Your Profile](#);
- talk to or otherwise interact with our Alexa Voice service;
- upload your contacts;
- configure your settings on, provide data access permissions for, or interact with an Amazon device or service;
- provide information in your [Seller Account](#), [Kindle Direct Publishing \(KDP\)](#) account, Developer account or any other account we make available that allows you to develop or offer software, goods, or services to Amazon customers;
- offer your products or services on or through Amazon Services;
- communicate with us by phone, e-mail, or otherwise;
- complete a questionnaire, a support ticket, or a contest entry form;
- upload or stream images, videos or other files to Prime Photos, Amazon Drive, or other Amazon Services;
- compile Playlists, Watchlists, Wish Lists or gift registries;
- Participate in community features, provide and rate [Customer Reviews](#);
- specify a Special Occasion Reminder; or
- employ Product Availability Alerts, such as Available to Order Notifications.

Image: Amazon UK Privacy Notice - Excerpt of Examples of Information You Give Us When You Use Amazon Services clause - How information is given

Then Amazon describes what personal information will be used, and how:

3. For What Purposes Does Amazon Europe Process Your Personal Information?

We process your personal information to operate, provide, and improve the Amazon Services that we offer our customers. These purposes include:

- **Purchase and delivery of products and services.** We use your personal information to take and handle orders, deliver products and services, process payments, and communicate with you about orders, products and services, and promotional offers.
- **Provide, troubleshoot, and improve Amazon Services.** We use your personal information to provide functionality, analyse performance, fix errors, and improve usability and effectiveness of the Amazon Services.
- **Recommendations and personalisation.** We use your personal information to recommend features, products, and services that might be of interest to you, identify your preferences, and personalise your experience with Amazon Services.
- **Provide voice, image and camera services.** When you use our voice, image and camera services, we process your voice input, images, videos, and other personal information to respond to your requests, provide the requested service to you, and improve our Amazon services. For more information about Alexa voice services click [here](#).
- **Comply with legal obligations.** In certain cases, we collect and use your personal information to comply with laws. For instance, we collect from sellers information regarding place of establishment and bank account information for identity verification and other purposes.
- **Communicate with you.** We use your personal information to communicate with you in relation to Amazon Services via different channels (e.g., by phone, email, chat).
- **Advertising.** We use your personal information to display interest-based ads for features, products, and services that might be of interest to you. To learn more, please read our [Interest-Based Ads notice](#).

Image: Amazon UK Privacy Notice - For What Purposes Does Amazon Europe Process Your Personal Information clause excerpt

Your Reasons For Collecting Personal Information

You've explained **what** personal information you collect, and **how** you collect it. You also need to explain **why you need** this information, and what you'll be using it **for**.

If you have EU customers, you should also disclose the [legal basis](#) on which you're collecting and using each type of personal information. There are six legal bases, and you can only collect or use a person's personal information if you have a legal basis to do so.

Here's an example from [eBay UK's](#) Privacy Notice:



5. Purposes and legal basis for data processing and categories of recipients

We process your personal data for various purposes and based on several different legal bases that allow this processing. For example, we process your personal data to provide and improve our Services, to provide you with a personalised user experience on this website, to contact you about your eBay account and our Services, to provide customer service, to provide you with personalised advertising and marketing communications, and to detect, prevent, mitigate and investigate fraudulent or illegal activity. We also share your information with third parties, including service providers acting on our behalf, for these purposes. In addition, we may share your personal data among eBay Affiliates in order to fulfil our contract with you under the User Agreement and, if applicable, the [Payments Terms of Use](#).

Image: eBay UK User Privacy Notice - Purposes and legal basis for data processing and categories of recipients clause

It reads:

We process your personal data for various purposes and based on several different legal bases that allow this processing. For example, we process your personal data to provide and improve our Services, to provide you with a personalised user experience on this website, to contact you about your eBay account and our Services, to provide customer service, to provide you with personalised advertising and marketing communications, and to detect, prevent, mitigate and investigate fraudulent or illegal activity. We also share your information with third parties, including service providers acting on our behalf, for these purposes. In addition, we may share your personal data among eBay Affiliates in order to fulfil our contract with you under the User Agreement and, if applicable, the Payments Terms of Use.

eBay first gives its legal basis (consent) for using these types of information. It then gives the reasons that it needs to collect this information.

Third Parties You Share Information With

As noted above, a lot of different companies are likely to come into possession of your customers' personal information. In your Privacy Policy, it's only necessary to reveal the [types of third parties](#) you'll be sharing your customers' data with.

Here's how [Toys R Us UK](#) does this:

Disclosure of Personal Information to Third Parties

We may disclose your personal information to third parties for the purpose for which the information was collected or for related purposes, for example, to complete a transaction on your behalf or provide you with a product that you purchased. We engage third-party contractors to perform services for us which involves the contractor handling personal information we hold. For example, we currently engage third-party contractors to:

- Deliver products purchased from this website.
- Provide electronic funds transfer services, credit card account processing and related services.

In these situations, the third-party contractor is strictly restricted from using any prohibited personal information about you except for the specific purpose for which we have supplied. We may also disclose your personal information to various law enforcement agencies and governments around the world for security, to comply with a subpoena, customs and immigration purposes. Google may receive information about transactions conducted on this site for the purpose of product reviews or service reviews. Other than the above, we will not disclose your personal information without your consent unless disclosure is either necessary to prevent a threat to life or health, authorised or required by law, reasonably necessary to enforce the law or necessary to investigate a suspected unlawful activity.

Image: Toys R Us UK Privacy Statement - Disclosure of Personal Information to Third Parties clause

It reads:

Disclosure of Personal Information to Third Parties

We may disclose your personal information to third parties for the purpose for which the information was collected or for related purposes, for example, to complete a transaction on your behalf or provide you with a product that you purchased. We engage third-party contractors to perform services for us which involves the contractor handling personal information we hold. For example, we currently engage third-party contractors to:

- *Deliver products purchased from this website.*
- *Provide electronic funds transfer services, credit card account processing and related services.*

In these situations, the third-party contractor is strictly restricted from using any prohibited personal information about you except for the specific purpose for which we have supplied. We may also disclose your personal information to various law enforcement agencies and governments around the world for security, to comply with a subpoena, customs and immigration purposes. Google may receive information about transactions conducted on this site for the purpose of product reviews or service reviews. Other than the above, we will not disclose your personal information without your consent unless disclosure is either necessary to prevent a threat to life or health, authorised or required by law, reasonably necessary to enforce the law or necessary to investigate a suspected unlawful activity.

You can list out specific third parties if you know them and want to, but it's not a requirement.

Privacy Rights and Opt-outs

No matter where your customers are based, your Privacy Policy should contain information about how they can [opt out](#) of receiving certain communications from you.

Here's an example of how to do this:

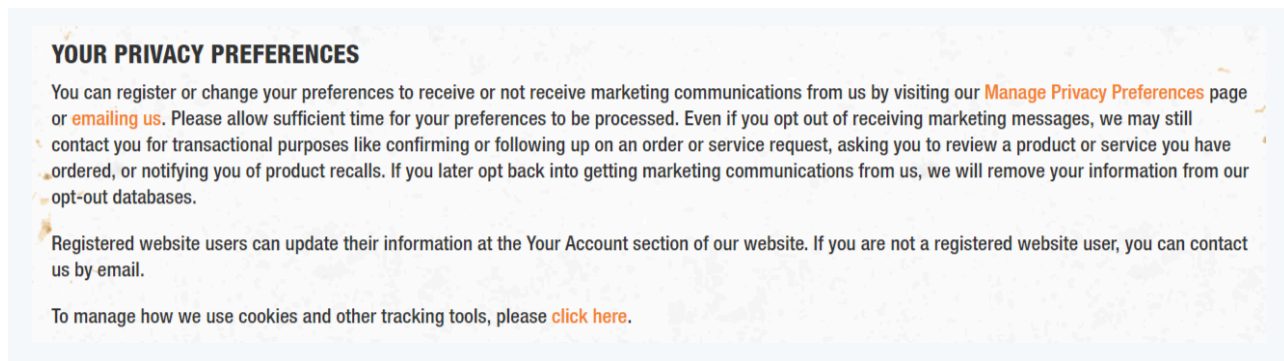
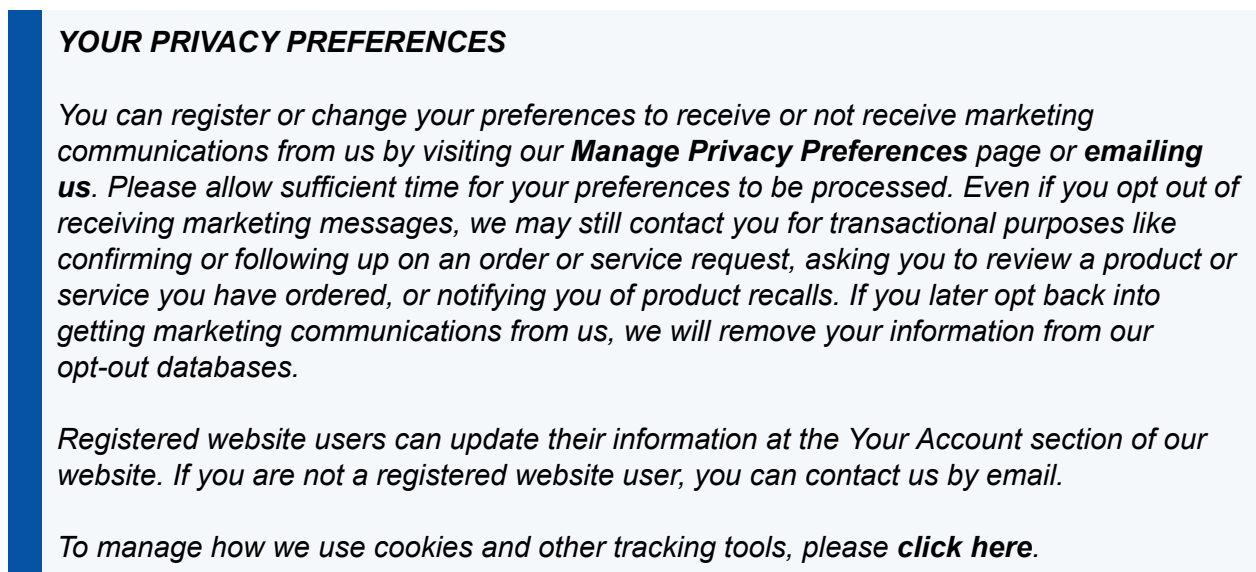


Image: Home Depot Privacy Policy: Your Privacy Preferences clause

It reads:



As noted above, if you're using Google AdWords this service also requires you to provide an opt-out from remarketing.

[Grey Ltd Interiors](#) does this with a separate Google Privacy Policy:

PRIVACY POLICY

GOOGLE PRIVACY POLICY

This website has implemented Google Analytics display advertising features including remarketing, Google Display Network Impression Reporting, and Google Analytics Demographics and Interest Reporting. This website uses remarketing with Google Analytics to advertise online. These ads may be shown to third-party vendors, including Google, on sites across the Internet.

This website and third-party vendors, including Google, use first-party cookies (such as the Google Analytics cookie) and third-party cookies (such as the DoubleClick cookie) together to inform, optimize, and serve ads based on visitors past visits to this website. These cookies are also used together to report on ad impressions, ad services, and related visitor interactions with this site. This site uses data aggregated from Google's Interest-based advertising or 3rd-party audience data (such as age, gender, and interests) for general website reporting and improvement, and possibly for ad remarketing lists.

Using [Ads Settings](#) provided by Google, visitors of this site can opt-out of Google Analytics for Display Advertising and customize Google Display Network ads.

Google also provides website visitors Google Analytics' [opt-outs](#) for the web, which provides a browser add-on for opting out of Google Analytics tracking altogether.

Image: Screenshot of full text of Grey Ltd Google Privacy Policy

It reads:

PRIVACY POLICY

GOOGLE PRIVACY POLICY

This website has implemented Google Analytics display advertising features including remarketing, Google Display Network Impression Reporting, and Google Analytics Demographics and Interest Reporting. This website uses remarketing with Google Analytics to advertise online. These ads may be shown to third-party vendors, including Google, on sites across the Internet.

This website and third-party vendors, including Google, use first-party cookies (such as the Google Analytics cookie) and third-party cookies (such as the DoubleClick cookie) together to inform, optimize, and serve ads based on visitors past visits to this website. These cookies are also used together to report on ad impressions, ad services, and related visitor interactions with this site. This site uses data aggregated from Google's Interest-based advertising or 3rd-party audience data (such as age, gender, and interests) for general website reporting and improvement, and possibly for ad remarketing lists.

Using Ads Settings provided by Google, visitors of this site can opt-out of Google Analytics for Display Advertising and customize Google Display Network ads.

Google also provides website visitors Google Analytics' opt-outs for the web, which provides a browser add-on for opting out of Google Analytics tracking altogether.

The situation is more complicated if you have EU customers, who have **a lot of control** over what you can do with their personal information. The GDPR provides [eight data rights](#) that EU citizens can access in relation to their personal information. If you serve EU customers, it's your job to help facilitate these.

Here's an example of how these rights can be presented:

- **Right of access** – You have the right to request a copy of the personal information that we hold about you.
- **Right to rectification** – If you think any of your personal information that we hold is inaccurate, you have the right to request it is updated. We may ask you for evidence to show it is inaccurate.
- **Right to erasure** – (also known as the Right to be Forgotten) – You have the right to request that we delete your personal information that we hold.
- **Right to restriction of processing** – You have the right to request we restrict or suppress the personal data we hold about you.
- **Right to data portability** – You have the right to ask us to electronically transfer your personal information to another organisation in certain circumstances.

Image: Next Privacy Policy: Data subject rights clause

It reads:

- **Right of access** - You have the right to request a copy of the personal information that we hold about you.
- **Right to rectification** - If you think any of your personal information that we hold is inaccurate, you have the right to request it is updated. We may ask you for evidence to show it is inaccurate.
- **Right to erasure** - (also known as the Right to be Forgotten) - You have the right to request that we delete your personal information that we hold.
- **Right to restriction of processing** - You have the right to request we restrict or suppress the personal data we hold about you.
- **Right to data portability** - You have the right to ask us to electronically transfer your personal information to another organization in certain circumstances.

Other Required Information

In addition to the above, your Privacy Policy should contain the following information:

- Your [contact details](#)
- Information that your policy is likely to **change** and [how users will be notified](#) if it does

If you have customers in the EU, include information about the following:

- How long you **store** different types of personal information
- Your customers' right to [lodge a complaint](#) with a Data Protection Authority
- If you're relying on the legal basis of **legitimate interests**, details of your [Legitimate Interests Assessment](#)
- If you're **transferring personal information** from the EU to a non-EU country, you need to let your customers know about this.

If you have customers in California, include information about:

- How your website responds to [Do Not Track \(DNT\) requests](#)
- [Do Not Sell My Personal Information](#) request rights

Where to Display Your Privacy Policy on Your Ecommerce Store

Once you've written your Privacy Policy, you'll need to make it accessible to your customers. There are several ways you can do this.

On Your Website

A common best practice and way to help ensure compliance is to [link to your Privacy Policy on your website's landing page](#). Typically this will be in a **footer** that persists on every page.

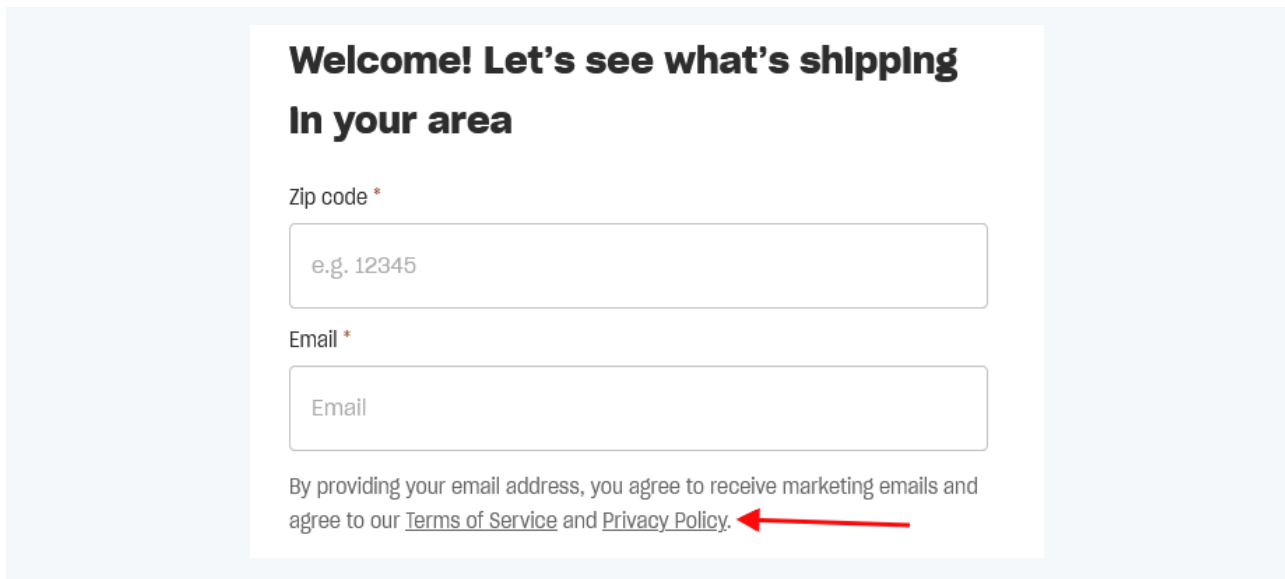
Here's an example from [Misfits Market](#):



Image: Misfits Market website footer with Privacy Policy link highlighted

You should present your Privacy Policy when your customers sign up for an account, and/or at the sign-in screen.

Here's how Misfits Market handles this:



**Welcome! Let's see what's shipping
In your area**

Zip code *

e.g. 12345

Email *

Email

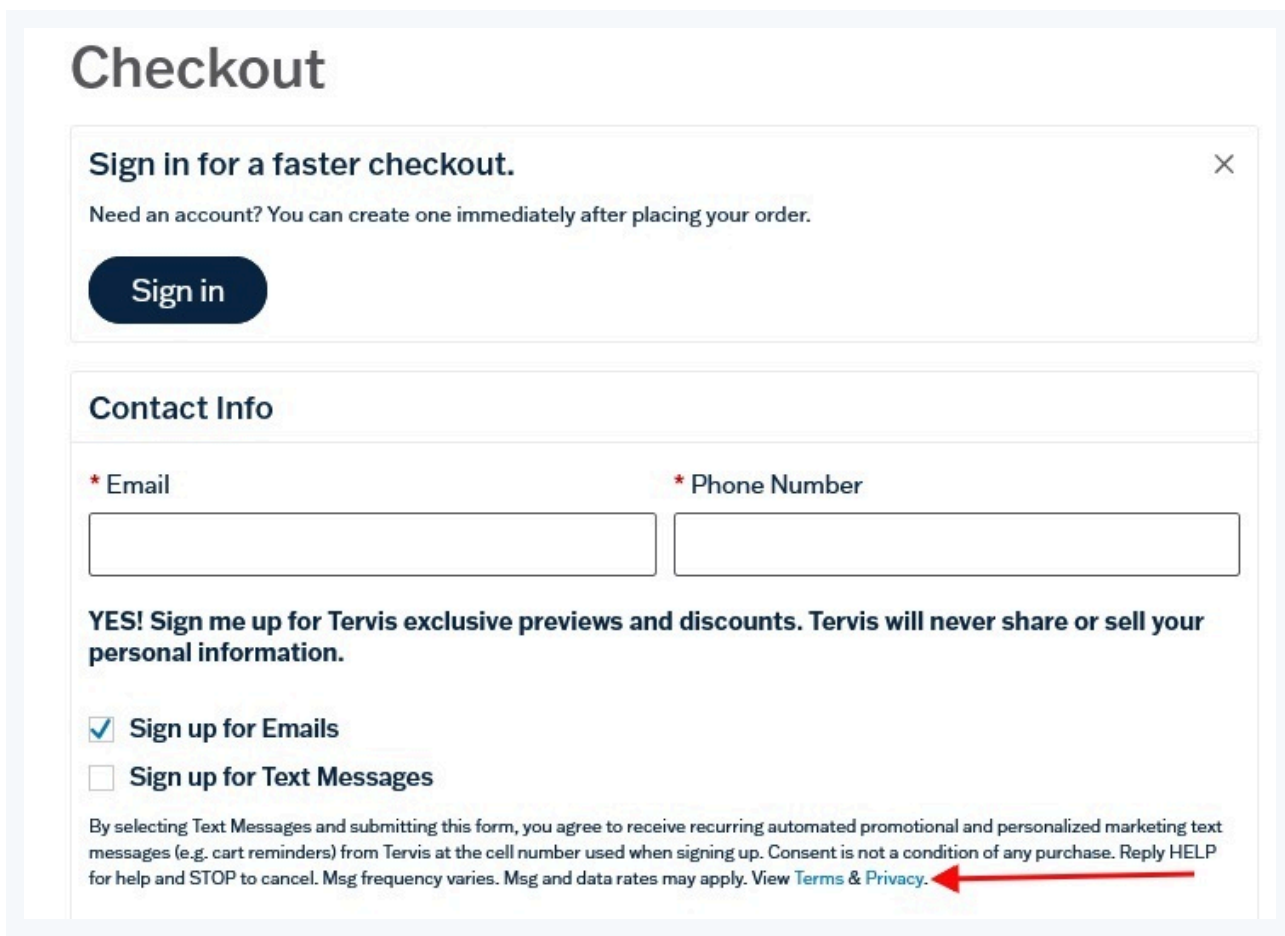
By providing your email address, you agree to receive marketing emails and agree to our [Terms of Service](#) and [Privacy Policy](#).

A red arrow points to the [Privacy Policy](#) link.

Image: Misfits Market sign-up form with Privacy Policy link highlighted

Another place to display your Privacy Policy on your website is at checkout if you have an ecommerce component, as well as when you request users give you their information for marketing purposes.

Here's an example that combines both of these, from Tervis:



Checkout

Sign in for a faster checkout. X

Need an account? You can create one immediately after placing your order.

Sign in

Contact Info

* Email * Phone Number

YES! Sign me up for Tervis exclusive previews and discounts. Tervis will never share or sell your personal information.

☒ Sign up for Emails

☐ Sign up for Text Messages

By selecting Text Messages and submitting this form, you agree to receive recurring automated promotional and personalized marketing text messages (e.g. cart reminders) from Tervis at the cell number used when signing up. Consent is not a condition of any purchase. Reply HELP for help and STOP to cancel. Msg frequency varies. Msg and data rates may apply. View [Terms & Privacy](#).

A red arrow points to the [Terms & Privacy](#) link.

Image: Tervis checkout form with Privacy Policy link highlighted

In Your Mobile App

App marketplaces such as Google Play Store and Apple's App Store have particular requirements about where to place your Privacy Policy within their app.

For example, in the [Google Play Store](#) it'll appear under the "Developer contact" section of the install page.

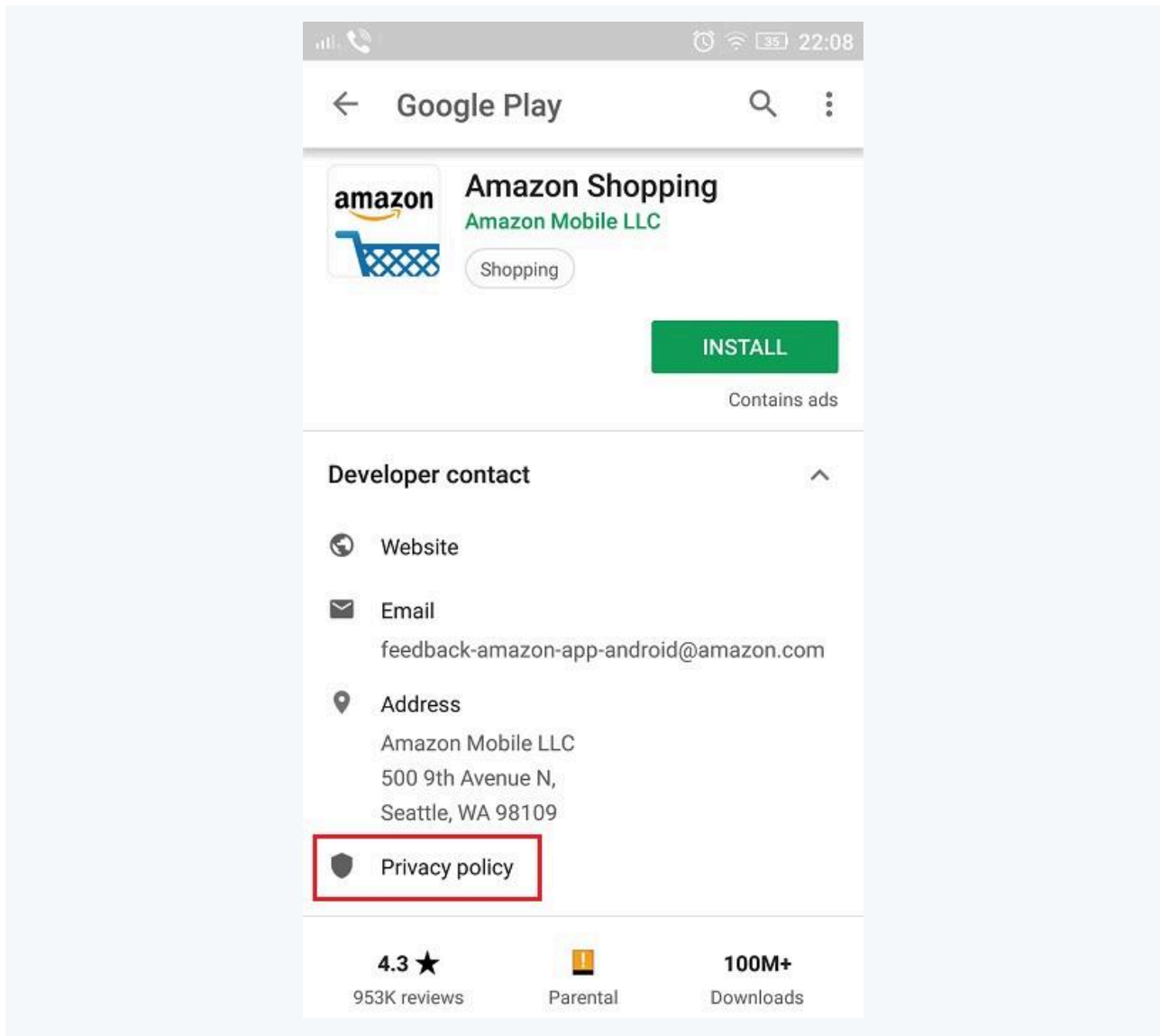


Image: Screenshot of Amazon Shopping app Google Play Store listing

You'll also need to present your new customers with your Privacy Policy when they **sign up** to use your service.

Here's an example from ecommerce app [Shpock](#):

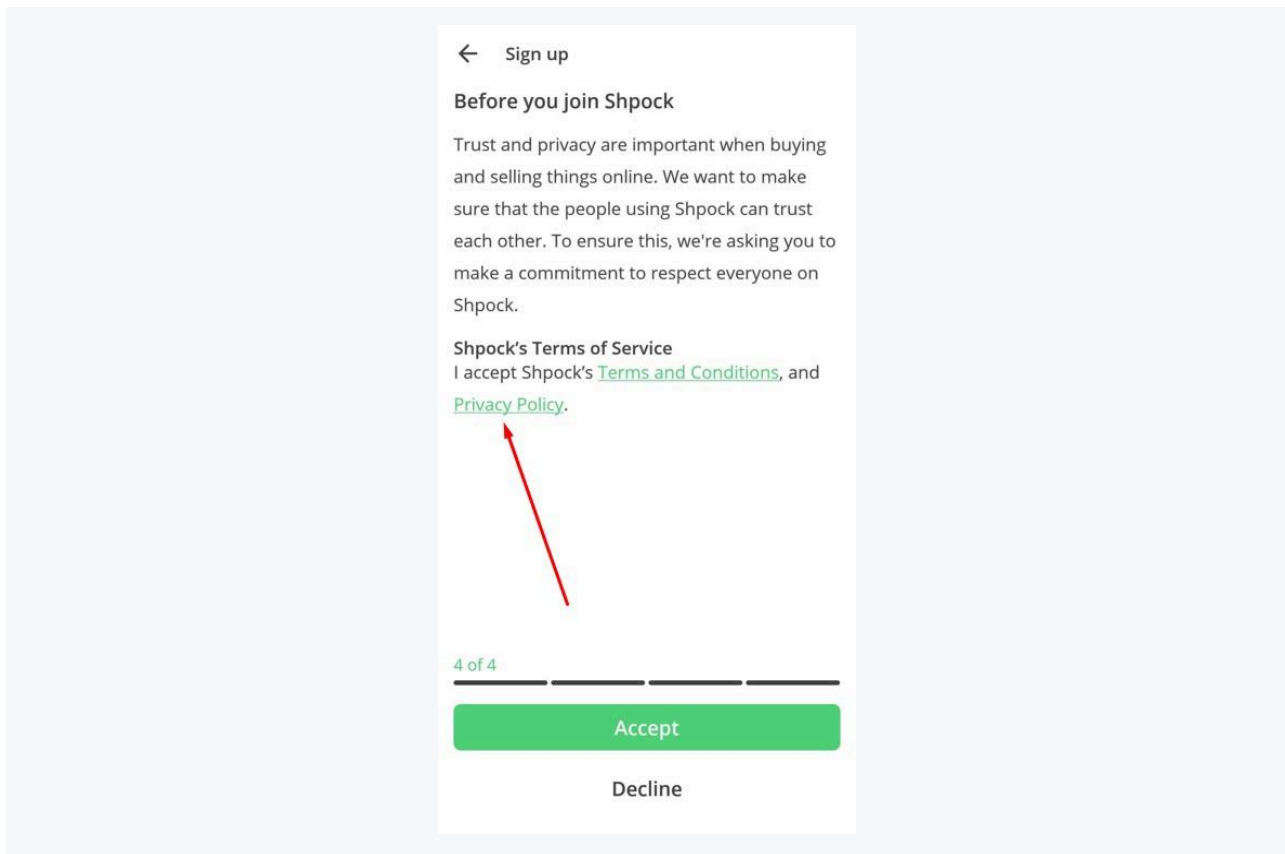


Image: Shpock app sign-up and accept Terms of Service and Privacy Policy screen

You should also make your Privacy Policy accessible from within the app, for example from the “About” or “Help” menu. Here’s an example from the [Audible](#) app:

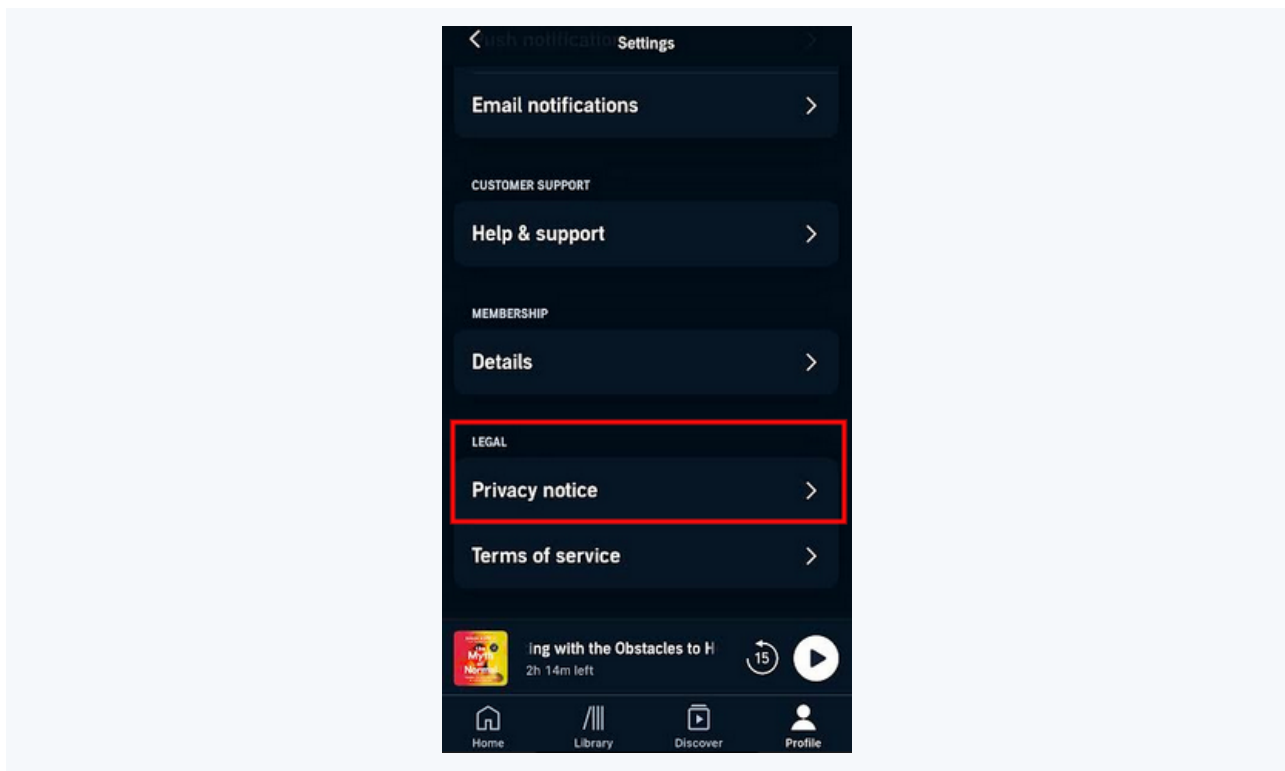


Image: Screenshot of Audible app Settings menu with Privacy Notice highlighted

Your customers should have the chance to read your Privacy Policy when making a purchase through your app.

Here's an example from the [Google Play Books](#) store and another example from Amazon:

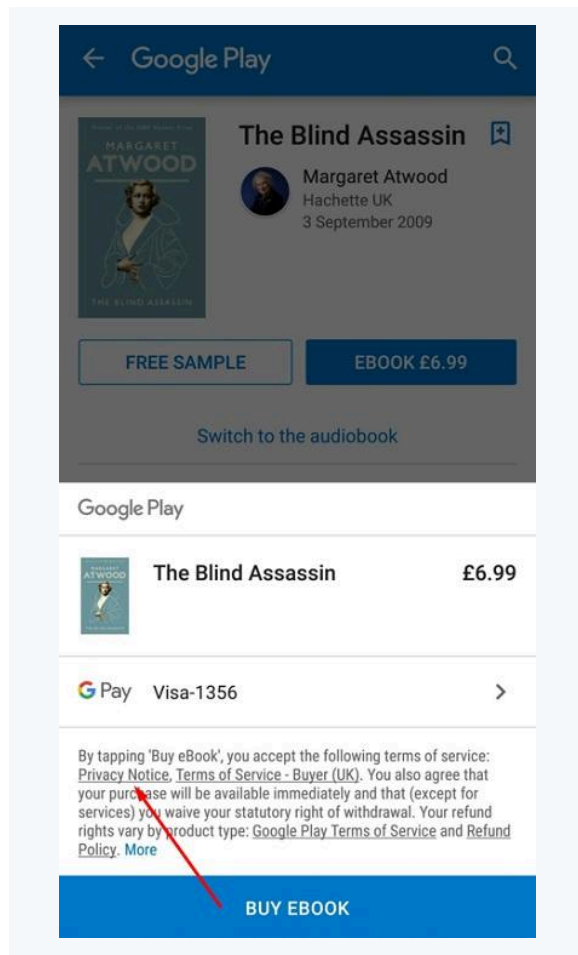


Image: Screenshot of Google Play Books store checkout page

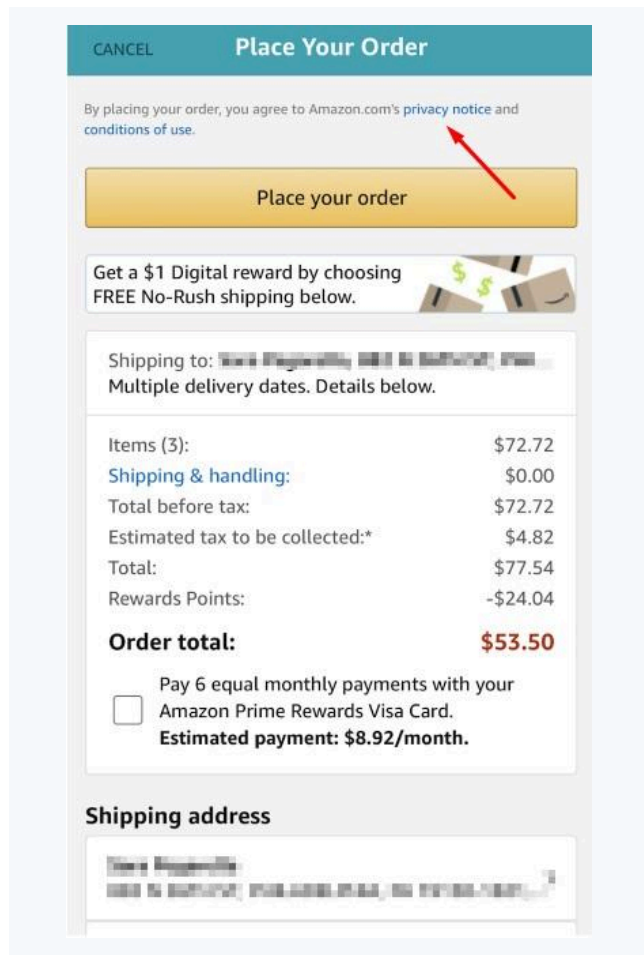


Image: Screenshot of Amazon app checkout page

Other Locations

When you send your customers **emails**, you should include a link to your Privacy Policy in the emails. You should make especially sure that it's present in marketing emails.

You can make this part of your standard email footer, like [The Economist](#) does:

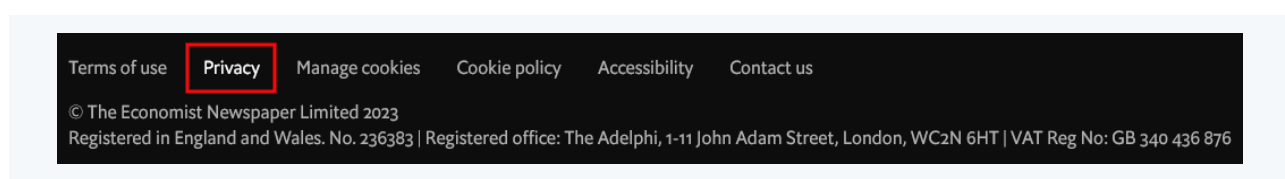


Image: Screenshot of the email footer from The Economist with Privacy Policy link highlighted

You should also ensure that you link to your Privacy Policy within other **legal agreements** like your Terms and Conditions agreement.

For example, [Walmart](#) includes a section about its Privacy Policy in its Terms of Use:

13. Privacy

You acknowledge that any personal information that you provide through the Walmart Sites will be used by Walmart in accordance with Walmart's Privacy Policy (available at <http://corporate.walmart.com/privacy-security/walmart-privacy-policy>), which may be updated by Walmart from time to time. If you purchase an item on Walmart.com sold by a Marketplace Retailer or a Walmart supplier, Walmart may share certain information with that Marketplace Retailer or supplier to permit the Marketplace Retailer or supplier, as applicable, to fulfill and ship your order, process returns, and provide customer service.

Image: Walmart Terms of Use: Privacy clause

It reads:

13. Privacy

You acknowledge that any personal information that you provide through the Walmart Sites will be used by Walmart in accordance with Walmart's Privacy Policy (available at <http://corporate.walmart.com/privacy-security/walmart-privacy-policy>), which may be updated by Walmart from time to time. If you purchase an item on Walmart.com sold by a Marketplace Retailer or a Walmart supplier, Walmart may share certain information with that Marketplace Retailer or supplier to permit the Marketplace Retailer or supplier, as applicable, to fulfill and ship your order, process returns, and provide customer service.

Linking to your Privacy Policy in your Terms and Conditions agreement is a good way to make sure that your customers have an opportunity to read both.

As mentioned, a Privacy Policy is legally **mandatory**, but a Terms and Conditions agreement isn't.

We'll discuss Terms and Conditions in more detail in the next chapter.

Case Study

Baths by Bridget is a Canadian bathroom company that sells baths, sinks, and showers. It ships domestically in Canada, and also to the U.S., the UK, and Germany. Baths by Bridget, therefore, has to write a Privacy Policy that complies with:

- Canada's **PIPEDA** privacy law,
- Privacy law in the U.S., and

- The EU's **GDPR**

Baths by Bridget uses Google AdWords to run **remarketing** campaigns. This service uses targeted **advertising cookies**. The website also **logs IP data** about its visitors to test the website's functionality and find out how visitors are discovering the site.

The company uses a **third party ecommerce store**, BigCommerce, to fulfill sales. When making a purchase, customers need to provide their email address, name, billing address, shipping address, telephone number, and payment card details.

It also asks its customers to **consent to receive direct marketing** emails and uses Mailchimp to run email direct marketing campaigns.

Baths by Bridget takes advantage of BigCommerce's "abandoned cart" feature. If a customer has registered with the site, added a product to their shopping cart, but failed to complete the sale, they'll receive an email asking them if they want to go through with the purchase.

In its Privacy Policy, Baths by Bridget needs to make certain things clear:

- The **contact details** for Baths by Bridget (the "data controller" in EU terms)
- **How** it collects information:
 - Some of it is volunteered by the customer, and some of it is collected via the customer's browser information
- **Why** it needs this information:
 - To fulfill sales
 - To run effective advertising
 - To improve the functionality and security of the website
- Its **legal basis** for collecting the information:
 - The legal basis for collecting payment information is to enter into and fulfill a **contract** with the customer
 - The legal basis for running targeted advertising is that the customer has **consented** (if they have consented)
 - The legal basis of improving the functionality of the website is that it is in Baths by Bridget's **legitimate interests**
- What types of **third parties** it shares this information with:
 - Google, and Google's **third-party advertising partners** in the case of cookie data
 - An **ecommerce platform** (BigCommerce) in the case of shipping and billing data
 - An automated **email marketing service** (MailChimp) in the case of email marketing

- How long it will be **storing** personal information
- The fact that it **transfers** its EU customers' personal information to a non-EU country (Canada)
- The **rights** that its EU customers have over their personal data, and how to exercise these rights
- How its website responds to **Do Not Track requests**

There may be additional requirements to meet as privacy laws develop. Consider this a living outline that will change depending on your unique circumstances and the current state of the laws of the land.

Chapter 4:

Terms & Conditions and Ecommerce Businesses

The main function of a [Terms and Conditions agreement](#) is to set out what your customers can expect from your company, and what you expect from them in return.

If properly presented and actively agreed to, Terms and Conditions represent **a contract between you and your customers**. If carefully drafted, this contract has **legal effect** and will be enforced by the courts in the event of a legal dispute.

Unlike a Privacy Policy, Terms and Conditions aren't a legal requirement. But having a clear and robust set of Terms and Conditions in place is an extremely good idea.

Having a strong set of Terms and Conditions in place means that you can:

- Set the limits of your company's legal **liability**
- Set the terms of your product **warranties**
- Manage your customers' **expectations**

What Your Terms and Conditions Agreement Should Include

[What you include in your Terms and Conditions](#) will depend on the nature of your business and where your business is based.

Whereas there are specific legal requirements for what appears in your Privacy Policy, this is not really true of your Terms and Conditions. You are free to write whatever you want, but that doesn't necessarily mean it will all benefit you.

Writing a Terms and Conditions agreement is a balancing act. You want to **protect your company's interests**, but you also need to be **fair to your customers**. If you're asking your customers to agree to something that's fair for both parties, your Terms and Conditions agreement is far more likely to be effective and legally enforceable.

Limitation of Liability

[A limitation \(or exclusion\) of liability](#) is a way to protect your business against legal claims.

Selling your customers products in your ecommerce store means that you're entering into a contract with them. Every contract involves some degree of risk. Businesses can make mistakes that cause their customers injuries and costs (losses).

Obviously you will take care to ensure that you don't cause your customers any losses. But you only want to be liable for a fair proportion of the damage if something goes wrong. Your customers should be buying your products with this understanding.

In theory, liability can be either:

- **Limited** to a particular sum. You accept that if someone suffers a loss and it's your company's fault, you will pay damages - but only, say, \$100.
- **Excluded** altogether. If someone suffers a loss, even where it's clearly your company's fault, you won't pay damages at all.

In practice, the courts will refuse to enforce limitation or exclusion clauses which are **unfair or unconscionable**.

Here's an example of a typical limitation of liability clause from [Hobby Lobby's](#) Terms of Use:

16. Limitations of Liability

TO THE FULLEST EXTENT PERMITTED BY LAW, IN NO EVENT WILL HOBBY LOBBY, ITS SUBSIDIARIES, AFFILIATES, OFFICERS, EMPLOYEES, AGENTS, SUPPLIERS OR LICENSORS BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, INCIDENTAL, SPECIAL, PUNITIVE OR EXEMPLARY DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOST PROFITS, REVENUE, GOODWILL, USE OR CONTENT) HOWEVER CAUSED, UNDER ANY THEORY OF LIABILITY, INCLUDING, WITHOUT LIMITATION, CONTRACT, TORT, WARRANTY, NEGLIGENCE OR OTHERWISE, EVEN IF IT HAS BEEN ADVISED AS TO THE POSSIBILITY OF SUCH DAMAGES IN ADVANCE. NOTWITHSTANDING ANYTHING TO THE CONTRARY CONTAINED HEREIN, HOBBY LOBBY'S MAXIMUM AGGREGATE LIABILITY AND THAT OF OUR AFFILIATES, OFFICERS, EMPLOYEES, AGENTS, SUPPLIERS OR LICENSORS, TO YOU FOR ANY CAUSE OF ACTION WHATSOEVER AND REGARDLESS OF THE FORM OF THE ACTION WILL BE LIMITED TO FIFTY U.S. DOLLARS (\$50.00). THIS LIMITATION OF LIABILITY SHALL APPLY REGARDLESS OF A FAILURE OF THE ESSENTIAL PURPOSE OF ANY OTHER REMEDY. THE PARTIES AGREE THAT THE ABOVE PROVISIONS FAIRLY ALLOCATE THE RISK BETWEEN THE PARTIES, WITHOUT WHICH THEY WOULD NOT HAVE ENTERED INTO THESE TERMS. SOME JURISDICTIONS DO NOT ALLOW THE FOREGOING LIMITATION OR EXCLUSION OF LIABILITY IN CONTRACTS WITH CONSUMERS, AND AS A CONSEQUENCE THIS LIMITATION OR EXCLUSION MAY NOT APPLY TO YOU BUT ONLY TO THE EXTENT PROHIBITED BY APPLICABLE LAW.

Image: Hobby Lobby Terms of Use - Limitations of Liability clause

It reads:

16. **Limitations of Liability**

TO THE FULLEST EXTENT PERMITTED BY LAW, IN NO EVENT WILL HOBBY LOBBY, ITS SUBSIDIARIES, AFFILIATES, OFFICERS, EMPLOYEES, AGENTS, SUPPLIERS OR LICENSORS BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, INCIDENTAL, SPECIAL, PUNITIVE OR EXEMPLARY DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOST PROFITS, REVENUE, GOODWILL, USE OR CONTENT) HOWEVER CAUSED, UNDER ANY THEORY OF LIABILITY, INCLUDING, WITHOUT LIMITATION, CONTRACT, TORT, WARRANTY, NEGLIGENCE OR OTHERWISE, EVEN IF IT HAS BEEN ADVISED AS TO THE POSSIBILITY OF SUCH DAMAGES IN ADVANCE.

NOTWITHSTANDING ANYTHING TO THE CONTRARY CONTAINED HEREIN, HOBBY LOBBY'S MAXIMUM AGGREGATE LIABILITY AND THAT OF OUR AFFILIATES, OFFICERS, EMPLOYEES, AGENTS, SUPPLIERS OR LICENSORS, TO YOU FOR ANY CAUSE OF ACTION WHATSOEVER AND REGARDLESS OF THE FORM OF THE ACTION WILL BE LIMITED TO FIFTY U.S. DOLLARS (\$50.00). THIS LIMITATION OF LIABILITY SHALL APPLY REGARDLESS OF A FAILURE OF THE ESSENTIAL PURPOSE OF ANY OTHER REMEDY. THE PARTIES AGREE THAT THE ABOVE PROVISIONS FAIRLY ALLOCATE THE RISK BETWEEN THE PARTIES, WITHOUT WHICH THEY WOULD NOT HAVE ENTERED INTO THESE TERMS. SOME JURISDICTIONS DO NOT ALLOW THE FOREGOING LIMITATION OR EXCLUSION OF LIABILITY IN CONTRACTS WITH CONSUMERS, AND AS A CONSEQUENCE THIS LIMITATION OR EXCLUSION MAY NOT APPLY TO YOU BUT ONLY TO THE EXTENT PROHIBITED BY APPLICABLE LAW.

You'll notice that many Limitation of Liability clauses are in [all capital letters](#). This convention originates partly from the requirement in the [Uniform Commercial Code](#) (UCC) that certain terms are made "conspicuous."

The reality is that the tendency to write in a large block of all capital letters actually makes these clauses harder to read for many consumers. There are other options (bold type, bullet points) for making certain contractual terms conspicuous. You don't have to use all caps.

Let's break Hobby Lobby's clause down. There are several statements here which we can explore in turn.

1. To the fullest extent **permitted by law**
2. Direct, indirect, consequential, incidental, special, punitive or exemplary **damages**
3. **Limited** to \$50

Laws on Limitation of Liability Clauses

What does Hobby Lobby mean by "to the fullest extent permitted by law"?

Any contract is only useful insofar as it will be **enforced** by a court. A court is less likely to enforce a contract that it deems unconscionable or unfair. In some countries, courts are stricter in their interpretations of unconscionability than in others. It's harder for businesses to argue that their limitation clauses should be enforced.

In the U.S., there is some scope for courts to find that contractual terms are **unconscionable** under the Uniform Commercial Code [§ 2-302](#). This places some **theoretical limits** on what a contract can include.

In the UK, business to consumer contracts are governed by the Consumer Rights Act [2015](#). This law instructs courts not to enforce clauses that attempt to **exclude liability for death or personal injury caused by negligence**. In fact, it's almost impossible to exclude liability for **any** effects of negligence under this law. Liability for negligence can realistically only be **limited**.

Here's part of [eBay's](#) limitation of liability clause in its User Agreement for UK users:

Regardless of the previous paragraphs, if we are found to be liable, our liability to you or to any third party is limited to the greater of (a) any amounts due under eBay Money Back Guarantee up to the price the item sold for on eBay and its original postage costs, (b) the amount of fees in dispute not to exceed the total fees which you paid to us in the 12 months prior to the action giving rise to the liability, or (c) £100.

Nothing in this User Agreement shall limit or exclude our liability for fraudulent misrepresentation, for death or personal injury resulting from our negligence or the negligence of our agents or employees or for any other liability that cannot be limited or excluded by law.

Compensation

You will compensate us in full (and our officers, directors, agents, subsidiaries, joint ventures and employees) for any losses or costs, including reasonable legal fees, we incur arising out of any breach by you of this User Agreement, your improper use of eBay's Services or your breach of any law or the rights of a third party.

Image: eBay UK User Agreement - Limitation of Liability clause excerpt highlighted

It reads:

Regardless of the previous paragraphs, if we are found to be liable, our liability to you or to any third party is limited to the greater of (a) any amounts due under eBay Money Back Guarantee up to the price the item sold for on eBay and its original postage costs, (b) the amount of fees in dispute not to exceed the total fees which you paid to us in the 12 months prior to the action giving rise to the liability, or (c) £100.

Nothing in this User Agreement shall limit or exclude our liability for fraudulent misrepresentation, for death or personal injury resulting from our negligence or the negligence of our agents or employees or for any other liability that cannot be limited or excluded by law.

Here, eBay is acknowledging that liability for certain things **can't be excluded** under UK law.

Here's how [Macy's](#) acknowledges the differences between jurisdictions:

To the fullest extent allowed by applicable laws, neither macys.com nor its corporate affiliates, nor the directors, officers, employees, agents, contractors, successors or assigns of each, shall be liable for any damages whatsoever arising out of or related to the use of this website, email sent in connection with this website or any other website linked to this website. This limitation of liability applies to direct, indirect, consequential, special, punitive or other damages you or others may suffer, as well as damages for lost profits, business interruption or the loss of data or information, even if macys.com is notified in advance of the potential for any such damages. **These terms are binding in New Jersey but some other jurisdictions limit consumer limitations of liability, so some or all of the provisions above may not apply to you.**

Image: Macys Legal Notice: Limitations of Liability clause excerpt - Jurisdiction section

It reads:

*To the fullest extent allowed by applicable laws, neither macys.com nor its corporate affiliates, nor the directors, officers, employees, agents, contractors, successors or assigns of each, shall be liable for any damages whatsoever arising out of or related to the use of this website, email sent in connection with this website or any other website linked to this website. This limitation of liability applies to direct, indirect, consequential, special, punitive or other damages you or others may suffer, as well as damages for lost profits, business interruption or the loss of data or information, even if macys.com is notified in advance of the potential for any such damages. **These terms are binding in New Jersey but some other jurisdictions limit consumer limitations of liability, so some or all of the provisions above may not apply to you.***

Different Types of Damages

What does Hobby Lobby mean by “*direct, indirect, consequential, incidental, special, punitive or exemplary damages*”?

The purpose of limiting liability is to limit the amount that your company will pay out in **damages**. “Damages” refers to the **money** paid out to compensate for a loss.

Broadly speaking:

- **Direct** damages cover the things that a reasonable person might see as **obvious** losses, directly resulting from a breach of contract.
- Indirect, special or **consequential** damages are the other losses that **might** result from a breach of contract.

For example, a tech company supplies a faulty hard drive that damages a customer's computer. The customer uses his computer for work and is therefore unable to work for one week.

The cost of **the damage to the computer** itself is a **direct** loss and would be compensated by direct damages.

The loss of **one week's operating profits** is an **indirect** loss. If compensated, this would be compensated by consequential (also known as "special" or "indirect") damages.

Most companies, like Hobby Lobby, try to cover all bases. Some express themselves slightly differently, but they are aiming for the same effect.

Here's how [Walmart](#) puts it:

18. Limitation of Liability

YOU ACKNOWLEDGE AND AGREE THAT, TO THE FULLEST EXTENT PROVIDED BY APPLICABLE LAW, WALMART WILL NOT BE LIABLE TO YOU OR TO ANY OTHER PERSON UNDER ANY CIRCUMSTANCES OR UNDER ANY LEGAL OR EQUITABLE THEORY, WHETHER IN TORT, CONTRACT, STRICT LIABILITY, OR OTHERWISE, **FOR ANY INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL LOSSES OR DAMAGES OF ANY NATURE** ARISING OUT OF OR IN CONNECTION WITH THE USE OF OR INABILITY TO USE THE WALMART SITES, EVEN IF AN AUTHORIZED REPRESENTATIVE OF A WALMART ENTITY HAS BEEN ADVISED OF OR SHOULD HAVE KNOWN OF THE POSSIBILITY OF SUCH DAMAGES. TO THE FULLEST EXTENT PROVIDED BY APPLICABLE LAW, THIS DISCLAIMER APPLIES TO ANY DAMAGES OR INJURY ARISING FROM ANY FAILURE OF PERFORMANCE, ERROR, OMISSION, INTERRUPTION, DELETION, DEFECTS, DELAY IN OPERATION OR TRANSMISSION, LOST PROFITS, LOSS OF GOODWILL, LOSS OF DATA, WORK STOPPAGE, ACCURACY OF RESULTS, COMPUTER FAILURE OR MALFUNCTION, COMPUTER VIRUSES, FILE CORRUPTION, COMMUNICATION FAILURE, NETWORK OR SYSTEM OUTAGE, THEFT, DESTRUCTION, UNAUTHORIZED ACCESS TO, ALTERATION OF, LOSS OF USE OF ANY RECORD OR DATA, AND ANY OTHER TANGIBLE OR INTANGIBLE LOSS. SUBJECT TO THE FOREGOING, TO THE FULLEST EXTENT PROVIDED BY APPLICABLE LAW, NO WALMART ENTITY WILL BE LIABLE FOR ANY DAMAGES IN EXCESS OF THE FEES PAID BY YOU IN CONNECTION WITH YOUR USE OF THE WALMART SITES DURING THE SIX (6) MONTH PERIOD PRECEDING THE DATE ON WHICH THE CLAIM AROSE.

Image: Walmart Terms of Use - Limitation of Liability clause with direct and consequential losses and damages section highlighted

It reads:

18. Limitation of Liability

YOU ACKNOWLEDGE AND AGREE THAT, TO THE FULLEST EXTENT PROVIDED BY APPLICABLE LAW, WALMART WILL NOT BE LIABLE TO YOU OR TO ANY OTHER PERSON UNDER ANY CIRCUMSTANCES OR UNDER ANY LEGAL OR EQUITABLE THEORY, WHETHER IN TORT, CONTRACT, STRICT LIABILITY, OR OTHERWISE, **FOR ANY INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL LOSSES OR DAMAGES OF ANY NATURE** ARISING OUT OF OR IN CONNECTION WITH THE USE OF OR INABILITY TO USE THE WALMART SITES, EVEN IF AN AUTHORIZED REPRESENTATIVE OF A WALMART ENTITY HAS BEEN ADVISED OF OR SHOULD HAVE KNOWN OF THE POSSIBILITY OF SUCH DAMAGES. TO THE FULLEST EXTENT PROVIDED BY APPLICABLE LAW, THIS DISCLAIMER APPLIES TO ANY DAMAGES OR INJURY ARISING

FROM ANY FAILURE OF PERFORMANCE, ERROR, OMISSION, INTERRUPTION, DELETION, DEFECTS, DELAY IN OPERATION OR TRANSMISSION, LOST PROFITS, LOSS OF GOODWILL, LOSS OF DATA, WORK STOPPAGE, ACCURACY OF RESULTS, COMPUTER FAILURE OR MALFUNCTION, COMPUTER VIRUSES, FILE CORRUPTION, COMMUNICATION FAILURE, NETWORK OR SYSTEM OUTAGE, THEFT, DESTRUCTION, UNAUTHORIZED ACCESS TO, ALTERATION OF, LOSS OF USE OF ANY RECORD OR DATA, AND ANY OTHER TANGIBLE OR INTANGIBLE LOSS. SUBJECT TO THE FOREGOING, TO THE FULLEST EXTENT PROVIDED BY APPLICABLE LAW, NO WALMART ENTITY WILL BE LIABLE FOR ANY DAMAGES IN EXCESS OF THE FEES PAID BY YOU IN CONNECTION WITH YOUR USE OF THE WALMART SITES DURING THE SIX (6) MONTH PERIOD PRECEDING THE DATE ON WHICH THE CLAIM AROSE.

Limiting Liability to a Specific Amount

What does Hobby Lobby mean by “*liability [...] will be limited to fifty US dollars*”?

In theory, you can attempt to **exclude liability** completely - to state that your company will pay no damages whatsoever. But there is a danger, sometimes even an inevitability, that this will be seen as **unconscionable**.

Getting your limitation of liability clause thrown out of court would be a very bad thing.

Many companies, including Hobby Lobby, choose to cap their total liability at a specific amount. Hobby Lobby chooses \$50. [Tracking Wonder](#) chose \$100 in its amusingly-titled limitation of liability clause:

THE “LIMITATION OF LIABILITY” CLAUSE, OR, THE ONE WHERE YOU AGREE NOT TO SUE OUR PANTS OFF

You agree that under no circumstances shall we be liable for direct, indirect, incidental, consequential, special, punitive, exemplary, or any other damages arising out of your use of the Site or Service. Additionally, Center to Page is not liable for damages in connection with (i) any failure of performance, error, omission, denial of service, attack, interruption, deletion, defect, delay in operation or transmission, computer virus or line or system failure; (ii) loss of revenue, anticipated profits, business, savings, goodwill or data; and (iii) third party theft of, destruction of, unauthorized access to, alteration of, or use of your information or property, regardless of our negligence, gross negligence, failure of an essential purpose and whether such liability arises in negligence, contract, tort, or any other theory of legal liability. The foregoing applies even if Center to Page has been advised of the possibility of or could have foreseen the damages. In those states that do not allow the exclusion or limitation of liability for the damages, our liability is limited to the fullest possible extent permitted by law. In no event shall Center to Page's cumulative liability to you exceed the total purchase price of the Service you have purchased from Center to Page, and if no purchase has been made by you **Center to Page's cumulative liability to you shall not exceed \$100.**

Image: Tracking Wonder Terms and Conditions: Limitation of Liability clause

It reads:

THE “LIMITATION OF LIABILITY” CLAUSE, OR, THE ONE WHERE YOU AGREE NOT TO SUE OUR PANTS OFF

*You agree that under no circumstances shall we be liable for direct, indirect, incidental, consequential, special, punitive, exemplary, or any other damages arising out of your use of the Site or Service. Additionally, Center to Page is not liable for damages in connection with (i) any failure of performance, error, omission, denial of service, attack, interruption, deletion, defect, delay in operation or transmission, computer virus or line or system failure; (ii) loss of revenue, anticipated profits, business, savings, goodwill or data; and (iii) third party theft of, destruction of, unauthorized access to, alteration of, or use of your information or property, regardless of our negligence, gross negligence, failure of an essential purpose and whether such liability arises in negligence, contract, tort, or any other theory of legal liability. The foregoing applies even if Center to Page has been advised of the possibility of or could have foreseen the damages. In those states that do not allow the exclusion or limitation of liability for the damages, our liability is limited to the fullest possible extent permitted by law. In no event shall Center to Page's cumulative liability to you exceed the total purchase price of the Service you have purchased from Center to Page, and if no purchase has been made by you **Center to Page's cumulative liability to you shall not exceed \$100.***

Limiting your liability is much more likely to be seen as **reasonable** than excluding it altogether.

Disclaimer of Warranties

A [warranty](#) is a **promise** or a **guarantee** about the **quality** of a **product** or service. If you make a promise about your products, a customer can hold you to it. A [disclaimer of warranties](#) is a way for your ecommerce store to **avoid making certain promises automatically**.

Here's an example of a disclaimer of warranties from [Shop.com](#):

DISCLAIMER OF WARRANTIES.

USE OF THE SITE IS AT YOUR OWN RISK. THE SHOP.COM SITE, FEATURES, PRODUCTS, CONTENT AND MATERIALS MADE AVAILABLE ON, IN CONJUNCTION WITH OR THROUGH THE SITE ARE PROVIDED TO YOU ON AN "AS IS" AND "AS AVAILABLE" BASIS WITHOUT WARRANTIES OF ANY KIND EITHER EXPRESS OR IMPLIED. TO THE MAXIMUM EXTENT PERMITTED BY LAW SHOP.COM DISCLAIMS ALL WARRANTIES, STATUTORY, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO, IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, NON-INFRINGEMENT, TITLE, QUIET ENJOYMENT, DATA ACCURACY AND SYSTEMS INTEGRATION.

Image: Shop Terms of Use - Disclaimer of Warranties clause

It reads:

DISCLAIMER OF WARRANTIES.

USE OF THE SITE IS AT YOUR OWN RISK. THE SHOP.COM SITE, FEATURES, PRODUCTS, CONTENT AND MATERIALS MADE AVAILABLE ON, IN CONJUNCTION WITH OR THROUGH THE SITE ARE PROVIDED TO YOU ON AN "AS IS" AND "AS AVAILABLE" BASIS WITHOUT WARRANTIES OF ANY KIND EITHER EXPRESS OR IMPLIED. TO THE MAXIMUM EXTENT PERMITTED BY LAW SHOP.COM DISCLAIMS ALL WARRANTIES, STATUTORY, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO, IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, NON-INFRINGEMENT, TITLE, QUIET ENJOYMENT, DATA ACCURACY AND SYSTEMS INTEGRATION.

Let's break this down. The disclaimer says two things of particular interest:

- To the maximum extent permitted by law
- Provided "As is"

Laws on Disclaimers of Warranties

As is the case with limitation of liability clauses, disclaimers of warranties take different legal effect in different places. They also attract **close scrutiny** from the courts.

In the U.S., the Uniform Commercial Code (UCC) [§ 2-314](#) imposes two "**implied**" **warranties** on all goods:

1. **Merchantability**, which applies to professional merchants (businesses) only. The warranty of merchantability guarantees that goods are:
 - Of average quality (at a minimum),
 - Labeled and packaged properly, and
 - Fit for purpose
2. **Fitness** for a particular purpose, which applies to all sellers

The law means that, by default, **businesses are assumed to have made these promises** about their products.

It is possible to **disclaim** these warranties in most states. This means that you will not be making these promises about your goods. **But you must be specific about this in your terms.**

The implied warranties cannot be disclaimed under the laws of the some states, including:

- [Connecticut](#)
- [Kansas](#)
- [Maine](#)
- [Maryland](#)
- [Massachusetts](#)
- [Mississippi](#)
- [Vermont](#)
- [West Virginia](#)

There are some heavy restrictions on the extent to which a disclaimer of an implied warranty is valid in some other states, including:

- [Alabama](#)
- [California](#)
- [Minnesota](#)
- [New Hampshire](#)
- [Oregon](#)

- [Rhode Island](#)

Some other states require specific wording to be used in a disclaimer - for example the use of the word “merchantability.”

Here’s an example of a company explicitly disclaiming different types of warranties:

Informational Content Disclaimer

THE INFORMATION PROVIDED ON THIS WEB SITE IS PROVIDED “AS IS” AND ALL WARRANTIES, EXPRESS OR IMPLIED, ARE DISCLAIMED, INCLUDING, BUT NOT LIMITED TO, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, MERCHANTABILITY OF ANY COMPUTER PROGRAM, FITNESS FOR A PARTICULAR PURPOSE, ACCURACY OF INFORMATIONAL CONTENT, OR SYSTEM INTEGRATION, OR NON-INFRINGEMENT. VYZE, INC.’S MAXIMUM LIABILITY FOR ANY INACCURATE INFORMATION AND YOUR SOLE AND EXCLUSIVE REMEDY FOR ANY CAUSE WHATSOEVER, SHALL BE LIMITED TO THE AMOUNT PAID BY YOU FOR THE INFORMATION RECEIVED (IF ANY). VYZE, INC. IS NOT LIABLE FOR ANY INDIRECT, SPECIAL, INCIDENTAL, LOSS OF BUSINESS, LOSS OF PROFITS OR CONSEQUENTIAL DAMAGES, WHETHER BASED ON BREACH OF CONTRACT, BREACH OF WARRANTY, TORT, NEGLIGENCE, PRODUCT LIABILITY OR OTHERWISE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Image: Vyze Terms and Conditions: Informational Content Disclaimer

It reads:

Informational Content Disclaimer

THE INFORMATION PROVIDED ON THIS WEB SITE IS PROVIDED “AS IS” AND ALL WARRANTIES, EXPRESS OR IMPLIED, ARE DISCLAIMED, INCLUDING, BUT NOT LIMITED TO, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, MERCHANTABILITY OF ANY COMPUTER PROGRAM, FITNESS FOR A PARTICULAR PURPOSE, ACCURACY OF INFORMATIONAL CONTENT, OR SYSTEM INTEGRATION, OR NON-INFRINGEMENT. VYZE, INC.’S MAXIMUM LIABILITY FOR ANY INACCURATE INFORMATION AND YOUR SOLE AND EXCLUSIVE REMEDY FOR ANY CAUSE WHATSOEVER, SHALL BE LIMITED TO THE AMOUNT PAID BY YOU FOR THE INFORMATION RECEIVED (IF ANY). VYZE, INC. IS NOT LIABLE FOR ANY INDIRECT, SPECIAL, INCIDENTAL, LOSS OF BUSINESS, LOSS OF PROFITS OR CONSEQUENTIAL DAMAGES, WHETHER BASED ON BREACH OF CONTRACT, BREACH OF WARRANTY, TORT, NEGLIGENCE, PRODUCT LIABILITY OR OTHERWISE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

There is no obligation to provide an express (written) warranty in U.S. federal law. But where a warranty *is* provided, the [Magnuson-Moss Warranty Act](#) forces that warranty to guarantee certain things. You should familiarize yourself with these requirements if you’re planning to offer your customers a warranty and you’re based in the United States.

The situation is very different in the EU, where consumer protection is **a lot stronger**.

In the EU, the [Sale of Goods and Associated Guarantees Directive](#) means that all consumer goods sold in the EU must:

- **Match** the **description** given,
- Be **fit for purpose**, and
- Be of **satisfactory quality**

EU law also guarantees a [14-day cancellation period](#) for goods bought online (for any reason) and a 2-year guarantee for all consumer goods. Some EU countries go above and beyond this. Technically, the legal guarantee extends to 6 years in parts of the UK.

It's generally **not possible to disclaim** such statutory consumer rights in EU countries. If an EU company inserts a disclaimer of warranties in its Terms and Conditions that does not comply with consumer law, **it will be disregarded by the courts**.

Provided "As Is"

What does Shop.com mean by "as is"?

Saying that a product is sold "as is" is one way of **disclaiming the warranties** of merchantability and fitness for purpose. Sometimes this is accompanied by the term "with all faults." The phrase "final sale" can have a similar effect.

Here's a disclaimer of warranties from [Aaron Equipment](#):

6. DISCLAIMER OF WARRANTIES

- A. ALL GOODS ARE PURCHASED BY THE PURCHASER "AS IS" AND "WITH ALL FAULTS".
- B. SELLER MAKES NO REPRESENTATION OR WARRANTY, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, WARRANTY AGAINST INFRINGEMENT OF INTELLECTUAL PROPERTY RIGHTS OF A THIRD PARTY OR ANY OTHER MATTER WITH RESPECT TO THE GOODS OR SERVICES.
- C. Any affirmation of fact or promises made by Seller or its employees or representatives shall not be deemed to create an express warranty that the Goods or Services shall conform to such affirmation or promise. Any descriptions, samples and specifications with respect to Goods or Services offered for sale herein are not warranted by Seller to be accurate or complete. If a model or sample was shown to Purchaser, such model or sample was used merely to illustrate the general type and quality of goods sold by Seller and not to represent that the Goods would necessarily conform to such model or sample. Any description is for the sole purpose of identifying the Goods and no affirmation, promise, description, sample or model shall be deemed part of the basis of the bargain. SELLER STRONGLY RECOMMENDS THAT PURCHASER CONDUCT AN ON-SITE INSPECTION OF THE GOODS SOLD HEREUNDER PRIOR TO PURCHASE. SELLER SHALL NOT BE RESPONSIBLE FOR THE CONSEQUENCES OF PURCHASER'S FAILURE TO INSPECT THE GOODS OR FOR ANY INACCURACIES, INSUFFICIENCIES, OR OMISSIONS IN SUCH DESCRIPTIONS, SAMPLES AND/OR SPECIFICATIONS.

Image: Aaron Equipment Used Equipment Terms and Conditions - Disclaimer of Warranties As Is clause

It reads:

6. DISCLAIMER OF WARRANTIES

- A. **ALL GOODS ARE PURCHASED BY THE PURCHASER "AS IS" AND "WITH ALL FAULTS"**
- B. **SELLER MAKES NO REPRESENTATION OR WARRANTY, EXPRESS, OR IMPLIED, INCLUDING BUT NOT LIMITED TO WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, WARRANTY AGAINST INFRINGEMENT OF INTELLECTUAL PROPERTY RIGHTS OF A THIRD PARTY OR ANY OTHER MATTER WITH RESPECT TO THE GOODS.**
- C. *Any affirmation of fact or promises made by Seller or its employees or representatives shall not be deemed to create an express warranty that the Goods or services shall conform to such affirmation or promise. Any descriptions, samples and specifications with respect to goods offered for sale herein are not warranted by*

Seller to be accurate or complete. If a model or sample was shown to Purchaser, such model or sample was used merely to illustrate the general type and quality of goods sold by Seller and not to represent that the Goods would necessarily conform to such model or sample. Any description is for the sole purpose of identifying the Goods and no affirmation, promise, description, sample or model shall be deemed part of the basis of the bargain. SELLER STRONGLY RECOMMENDS THAT PURCHASER CONDUCT AN ON-SITE INSPECTION OF THE GOODS SOLD HEREUNDER. SELLER SHALL NOT BE RESPONSIBLE FOR THE CONSEQUENCES OF PURCHASER'S FAILURE TO INSPECT THE GOODS OR FOR ANY INACCURACIES, INSUFFICIENCIES, OR OMISSIONS IN SUCH DESCRIPTIONS, SAMPLES AND/OR SPECIFICATIONS. The employees or representatives of Seller are not authorized to make any statement or representation as to the quality, character, size, condition, quantity, etc. of the goods offered for sale inconsistent with these Terms and Conditions. Any such statements made will not be binding on Seller or be grounds for any subsequent claim.

You can see that goods are sold “as is” and “with all faults.” The customer is advised to inspect the goods on-site before purchase. This is basically what is implied by selling something “as is” - the buyer can take it or leave it.

Such a clause would **not** apply in some states, or jurisdictions such as the EU, for goods bought **online**. It's assumed that the buyer hasn't had the opportunity to inspect the product until it's delivered.

It's also not possible for a business in the states listed above or the EU to sell **faulty goods** and refuse a refund.

We'll be looking at other types of disclaimers in Chapter 6.

Returns and Refunds

As the online marketplace grows, competition increases as well. Customers expect a good level of service, and their repeat business depends on you providing it.

Having a [Return and Refund Policy](#) means that your customers know where they stand if something goes wrong with one of your products. And if they don't know, you can point to the policy that they agreed to when they made the purchase.

It's also reassuring for your customers to know that they're covered if something goes wrong.

We'll discuss your Return and Refund Policy in more detail in the next chapter. At this point, it will suffice to say this: if you're going to have a Return and Refund Policy (and it's strongly recommended that you do), it's important that you **ask your customers to agree to it before they make a purchase**.

Your Return and Refund Policy should be a separate agreement, but should also be linked to and referenced within your Terms agreement. This way, when getting users to agree to your terms, they will also be agreeing to your return policy by default.

Here's an example of how you can mention and link to a Return and Refund Policy within a Terms agreement:

5. Returns, Cancellations and Substitutions

5.1 We offer a 30-day money back guarantee, [please refer to Returns and refunds](#). Some products are excluded from the Guarantee and are clearly marked by a † next to the product name. In the unlikely event that you receive faulty or damaged goods, please refer to our [Returns and refunds](#) section.

5.2 Sometimes the product specifications from the manufacturer may change, in which case we will do our best to offer you a similar alternative. We may experience problems with the supply of certain products and may therefore supply a substitute of the same or better quality at the same price. If you are not happy with the replacement or substitute you can return it in accordance with our 30-day money back guarantee. Where applicable, you may cancel your order in accordance with your rights under the Consumer Contracts (Information, Cancellation & Additional Charges Regulations (see the [Returns and refunds](#) page for further details

5.3 All sizes and measurements are approximate but we do try to make sure that they are as accurate as possible.

[Back to top](#)

Image: Argos Terms and Conditions: Returns, Cancellations and Substitutions clause

It reads:

5. Returns, Cancellations and Substitutions

5.1 We offer a 30-day money back guarantee, [please refer to Returns and refunds](#). Some products are excluded from the Guarantee and are clearly marked by a † next to the product name. In the unlikely event that you receive faulty or damaged goods, please refer to our Returns and refunds section.

5.2 Sometimes the product specifications from the manufacturer may change, in which case we will do our best to offer you a similar alternative. We may experience problems with the supply of certain products and may therefore supply a substitute of the same or better quality at the same price. If you are not happy with the replacement or substitute you can return it in accordance with our 30-day money back guarantee. Where applicable, you may cancel your order in accordance with your rights under the Consumer Contracts (Information, Cancellation & Additional Charges Regulations (see the Returns and refunds page for further details

5.3 All sizes and measurements are approximate but we do try to make sure that they are as accurate as possible.

Some **basic information and a summary is provided** about the Return and Refund Policy as well as a link to the full policy.

Delivery Information

Having your delivery information as part of (or otherwise incorporated into) your Terms and Conditions is another good way to manage your customers' expectations.

If any disputes arise, you can also demonstrate that your customers have agreed to your delivery information by having agreed to your Terms and Conditions.

Delivery Options

You should include details about your customers' delivery options, as well as any conditions you place on these. This can include different timeframes, prices, and limitations.

Here's an example from [Michaels'](#) Shipping Policy. This is just an excerpt of its full, very informative policy:

Shipping Delivery:

The following shipping methods are available: Standard Ground (4 – 6 business days), Second Day (2 business days), Next Day (1 business day) and Same Day (same day). Business days do not include weekends and there is no weekend delivery for any shipping method except Same Day. Some items cannot be shipped using Second Day, Next Day or Same Day due to size, weight, hazardous materials and delivery address. These items will only have Standard Ground available. Currently, we do not ship to U.S. Territories, APO/FPO, Canada or other international addresses. Please note that orders could arrive in multiple packages.

You can track your order by [clicking here](#).

Standard Ground:

Orders delivered within the 48 contiguous states should arrive in 4 – 6 business days depending on delivery location. Orders shipped to Alaska and Hawaii will take an additional 2 – 5 days for delivery and are subject to an additional \$15 delivery fee. Alaska and Hawaii are excluded from Free Shipping promotions.

Second Day:

Second Day is only available on select products for our customers who ship orders within the 48 contiguous United States. Second Day delivery orders will be processed on the same day if they are placed by 11:00am CT on a business day, and should arrive in 2 business days. Orders placed after 11:00am CT will be processed on the following business day, and should arrive in 3 business days. All orders must have a valid street address (no PO Boxes). Not all items are eligible for expedited delivery. This method is not available for Alaska or Hawaii.

Next Day:

Next Day delivery is only available on select products for customers who ship orders within the 48 contiguous United States. Next Day delivery orders will be processed on the same day if they are placed by 11:00am CT on a business day, and should arrive in 1 business day. Orders placed after 11:00am CT will be processed on the following business day, and should arrive in 2 business days. All orders must have a valid street address (no PO Boxes). Not all items are eligible for expedited delivery. This method is not available for Alaska or Hawaii.

Same Day:

Same-day delivery is a contactless service to get what you need, when you need it. Same-day delivery is only available at select stores and for customers who place an order within a 10-mile radius of a Michaels store. Same-day delivery orders will be processed on the same day if they are placed by 2:00pm local time and should arrive that same day. Orders placed after 2:00pm local time will be processed on the following day and should arrive the following day. All orders must have a valid street address (no PO Boxes). Not all items are eligible for same-day delivery. Only items selected as same-day delivery count toward the "spend" thresholds of the same-day delivery fees. Refer to our Stores Page for your local store hours.

Image: Michaels Shipping Policy - Delivery clause excerpt

Don't forget to include **cut-off times**:

Second Day:

Second Day is only available on select products for our customers who ship orders within the 48 contiguous United States. Second Day delivery orders will be processed on the same day if they are placed by 11:00am CT on a business day, and should arrive in 2 business days. Orders placed after 11:00am CT will be processed on the following business day, and should arrive in 3 business days. All orders must have a valid street address (no PO Boxes). Not all items are eligible for expedited delivery. This method is not available for Alaska or Hawaii.

Image: Michaels Shipping Policy - Second Day delivery clause

Shipping Costs

Make sure you include the **costs** for different shipping options so that customers are clear about this from the outset.

Here's an example from Michaels:

Shipping Rates:					
	Buy Online Pickup In Store	Standard Ground 4 - 6 Business Days	Second Day 2 Business Days (Order Before 11 am CT)	Overnight 1 Business Day (Order Before 11 am CT)	Same Day Delivery (Order Before 2 pm Local Time)
\$0.00 - \$14.99	FREE	\$8.95	\$17.95	\$24.95	\$9.99
\$15.00 - \$29.99	FREE	\$8.95	\$22.95	\$29.95	\$9.99
\$30.00 - \$49.99	FREE	\$8.95	\$29.95	\$39.95	\$9.99
\$50.00 - \$58.99	FREE	FREE	\$39.95	\$49.95	\$9.99
\$59.00 - \$74.99	FREE	FREE	\$39.95	\$49.95	\$9.99
\$75.00 - \$99.99	FREE	FREE	\$49.95	\$69.95	\$9.99
\$100.00 - \$124.99	FREE	FREE	\$69.95	\$109.95	\$7.99
\$125.00 - \$149.99	FREE	FREE	\$89.95	\$149.95	\$7.99
\$150.00 - \$174.99	FREE	FREE	\$99.95	\$169.95	\$7.99
\$175.00 - \$199.99	FREE	FREE	\$109.95	\$189.95	\$7.99
\$200.00 - \$249.99	FREE	FREE	\$119.95	\$209.95	\$7.99
\$250.00 - \$299.99	FREE	FREE	\$129.95	\$239.95	\$7.99
\$300.00 - \$349.99	FREE	FREE	\$139.95	\$259.95	\$7.99
\$350.00 - \$399.99	FREE	FREE	\$154.95	\$294.95	\$7.99
\$400.00 - \$449.99	FREE	FREE	\$169.95	\$329.95	\$7.99
\$450.00 - \$499.99	FREE	FREE	\$184.95	\$364.95	\$7.99
> \$500.00	FREE	FREE	\$199.95	\$399.95	\$7.99
*Shipping rates are subject to change at any time.					

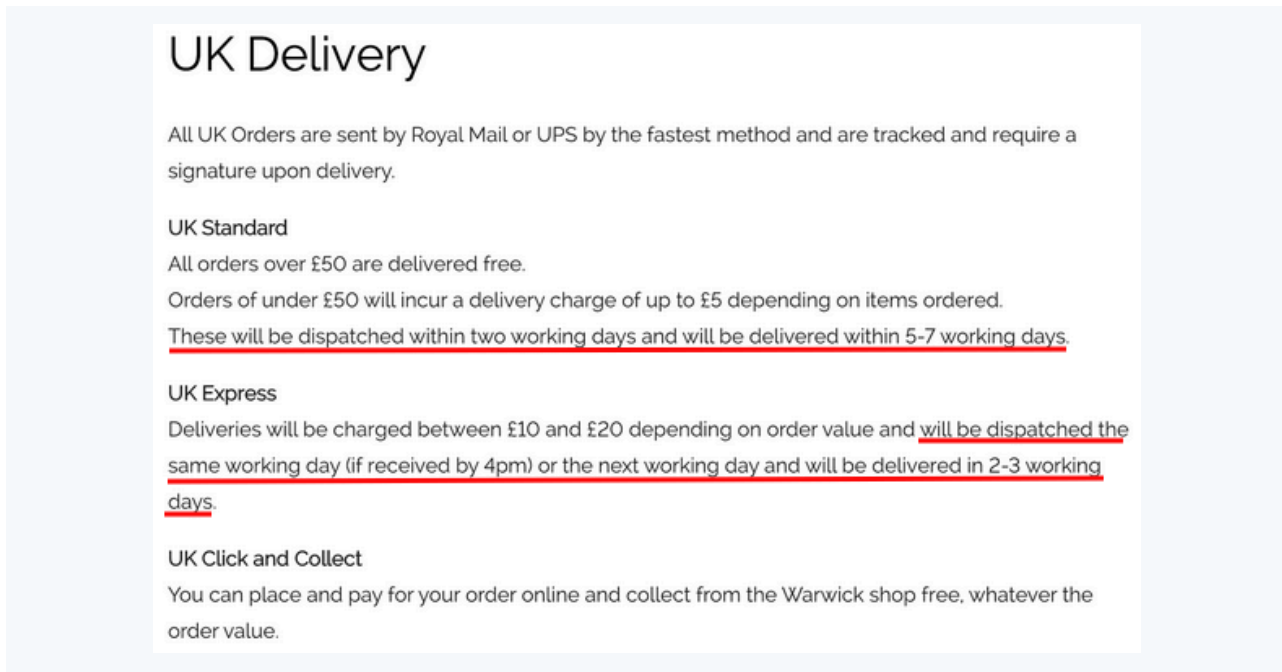
Image: Michaels Shipping Policy: Shipping Rates clause chart

Note how it also includes a note at the bottom that shipping rates are subject to change at any time. This is smart to do so you're covered in case shipping costs change and you need to adjust them to not take a huge loss.

Timescales for Dispatch and Delivery

You can use shipping information to make your **timescales** clear - your **dispatch** time (when you **send** something) and your **delivery** time (when it will **arrive**).

Here's an example of how this can look:

A screenshot of a webpage titled "UK Delivery". The text states that all UK orders are sent by Royal Mail or UPS by the fastest method and are tracked and require a signature upon delivery. It then lists three delivery options: UK Standard, UK Express, and UK Click and Collect. The UK Standard section mentions that orders over £50 are delivered free, while orders under £50 incur a delivery charge of up to £5. It also states that orders will be dispatched within two working days and delivered within 5-7 working days. The UK Express section states that deliveries will be charged between £10 and £20 depending on order value and will be dispatched the same working day (if received by 4pm) or the next working day and delivered in 2-3 working days. The UK Click and Collect section states that you can place and pay for your order online and collect from the Warwick shop free, whatever the order value. The text is presented in a clean, sans-serif font with a light blue background.

UK Delivery

All UK Orders are sent by Royal Mail or UPS by the fastest method and are tracked and require a signature upon delivery.

UK Standard

All orders over £50 are delivered free.

Orders of under £50 will incur a delivery charge of up to £5 depending on items ordered.

These will be dispatched within two working days and will be delivered within 5-7 working days.

UK Express

Deliveries will be charged between £10 and £20 depending on order value and will be dispatched the same working day (if received by 4pm) or the next working day and will be delivered in 2-3 working days.

UK Click and Collect

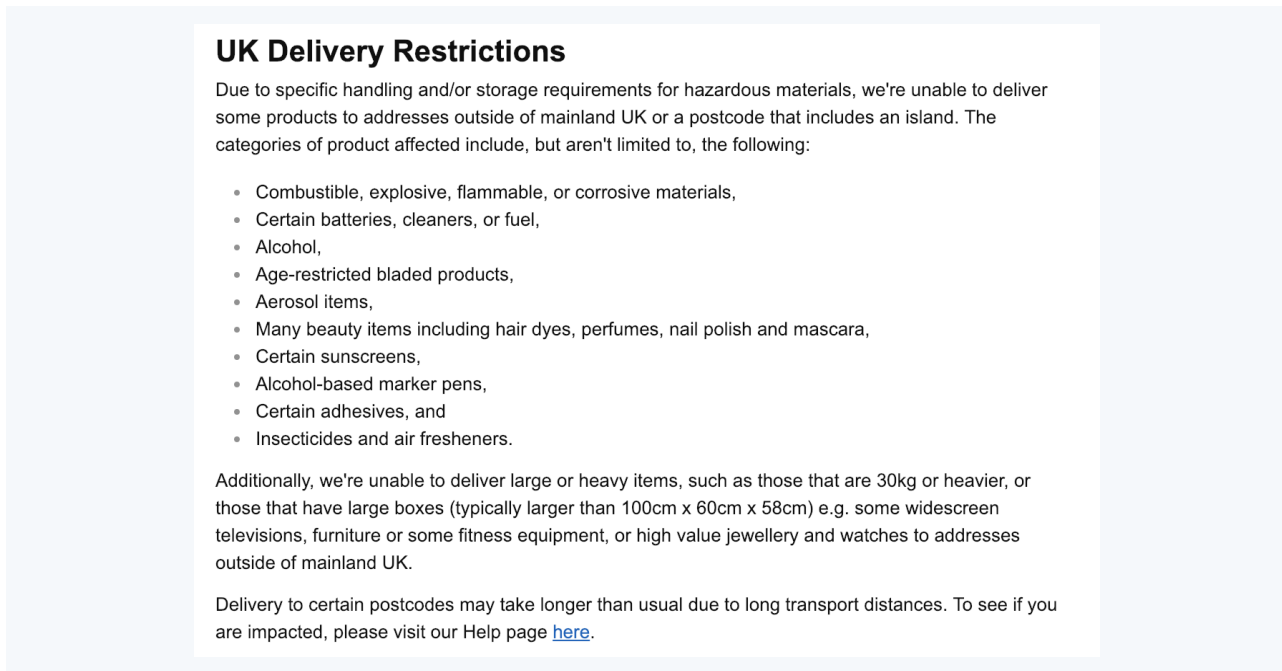
You can place and pay for your order online and collect from the Warwick shop free, whatever the order value.

Image: Present Days UK Delivery terms

Delivery Restrictions

There may be some **places** that you can't deliver to, or some **items** that you can't deliver to certain places.

Here's how [Amazon UK](#) covers this:

A screenshot of the Amazon UK Help page titled "UK Delivery Restrictions". The text explains that due to specific handling and/or storage requirements for hazardous materials, some products cannot be delivered to addresses outside of mainland UK or to postcodes that include an island. It lists categories of products affected, including combustible, explosive, flammable, or corrosive materials; certain batteries, cleaners, or fuel; alcohol; age-restricted bladed products; aerosol items; many beauty items including hair dyes, perfumes, nail polish, and mascara; certain sunscreens; alcohol-based marker pens; certain adhesives; and insecticides and air fresheners. It also mentions that large or heavy items (30kg or heavier, or larger than 100cm x 60cm x 58cm) cannot be delivered to certain addresses. Finally, it notes that delivery to certain postcodes may take longer than usual due to long transport distances and provides a link to the Help page for more information. The text is presented in a clean, sans-serif font with a light blue background.

UK Delivery Restrictions

Due to specific handling and/or storage requirements for hazardous materials, we're unable to deliver some products to addresses outside of mainland UK or a postcode that includes an island. The categories of product affected include, but aren't limited to, the following:

- Combustible, explosive, flammable, or corrosive materials,
- Certain batteries, cleaners, or fuel,
- Alcohol,
- Age-restricted bladed products,
- Aerosol items,
- Many beauty items including hair dyes, perfumes, nail polish and mascara,
- Certain sunscreens,
- Alcohol-based marker pens,
- Certain adhesives, and
- Insecticides and air fresheners.

Additionally, we're unable to deliver large or heavy items, such as those that are 30kg or heavier, or those that have large boxes (typically larger than 100cm x 60cm x 58cm) e.g. some widescreen televisions, furniture or some fitness equipment, or high value jewellery and watches to addresses outside of mainland UK.

Delivery to certain postcodes may take longer than usual due to long transport distances. To see if you are impacted, please visit our Help page [here](#).

Image: Amazon UK Help: UK Delivery Restrictions

Customs and Duties

Issues can arise when shipping **internationally**. Many countries place additional tariffs on certain goods at the border. This might be a surprise to a customer who has been quoted a particular price for delivery and then finds that their customs office has put an extra sum on top.

Many ecommerce stores handle this by saying that the customer is responsible for **additional taxes** or duties incurred when shipping internationally.

Here's an example of how you can address this issue:

HOW MUCH DUTY AND TAX WILL I HAVE TO PAY?

We're unable to supply estimated duties and taxes as this information will vary by country. Please note that if you place an order online, you will be responsible for all duties, taxes and customs charges. If your order is then refused, you will still be responsible for charges incurred in shipping the package.

Image: Lululemon UK shipping fees and timing - Duty and tax section

Payment Methods

You can also include reference to the forms of payment you accept, the terms on which a customer will be charged, and what will happen if a payment fails. This is particularly important if you're offering a **subscription service**.

Here's an example from meal kit service [Blue Apron](#):

4.7. Payment and Billing Information

By providing a credit card or other payment method that we accept, you represent and warrant that you are authorized to use the designated payment method and that you authorize us (or our third-party payment processor) to charge your payment method for the total amount of your subscription or other purchase (including any applicable taxes and other charges) (collectively, as applicable, an "Order"). If the payment method cannot be verified, is invalid or is otherwise not acceptable, your Order may be suspended or cancelled. You must resolve any payment method problems before we proceed with your Order. If you want to change or update your payment method information, you can do so at any time by logging into your account. If a payment is not successfully settled and you do not edit your payment method information or cancel your Meal Subscription, Wine Subscription, purchase of a Non-Subscription Product, or account, as applicable, you remain responsible for any uncollected amounts and, with respect to your Meal Subscription or Wine Subscription, authorize us to continue billing the payment method, as it may be updated.

You acknowledge that the amount billed may vary due to promotional offers, preferences you select, changes you make to your Meal Subscription, Wine Subscription, purchase of a Non-Subscription Product, or changes in applicable taxes or other charges, and you authorize us (or our third party-payment processor) to charge your payment method for the corresponding amount.

Notwithstanding anything provided above, for the purposes of this Section 4.6, any Third Party Purchase will be billed and charged in accordance with the applicable Third Party Terms.

Image: Blue Apron Terms of Use: Payment and Billing Information clause

Other Information

In addition to the above, there are some other sections you can consider including in your Terms and Conditions:

- A **copyright** and **trademark** section that establishes your intellectual property rights
- A set of **disclaimers** relative to the products you sell (we'll discuss this in more detail in [Chapter 6](#))
- A [governing law clause](#) that sets the jurisdiction in which legal claims will be heard

If you allow your visitors to contribute [user generated content](#) to your website, for example in a comments section under blog posts, your Terms and Conditions can also be used to manage this. You can set out:

- The type of content that visitors are permitted to post
- What they cannot post
- The conditions under which a person might be banned from your website
- An indemnity or "hold harmless" clause that protects your company from defamation claims
- How visitors can submit information about alleged copyright violations under the [Digital Millennium Copyright Act](#)

Here's how [Behr](#) lists out what content cannot be submitted:

You further agree and warrant that you shall not submit any content:

- that is known by you to be false, inaccurate or misleading;
- that infringes any third party's copyright, patent, trademark, trade secret or other proprietary rights or rights of publicity or privacy;
- that violates any law, statute, ordinance or regulation (including, but not limited to, those governing export control, consumer protection, unfair competition, anti-discrimination or false advertising);
- that is, or may reasonably be considered to be, defamatory, libelous, hateful, racially or religiously biased or offensive, unlawfully threatening or unlawfully harassing to any individual, partnership or corporation;
- that is advertising or promotional material, including any "junk mail", "chain letter" or "spam" or any other similar solicitation;
- that impersonates or attempts to impersonate Behr Process Corporation or a Behr Process Corporation employee, another user, or person or entity (including, without limitation, the use of e-mail addresses associated with any of the foregoing);
- for which you were compensated or granted any consideration by any third party;
- that includes any information that references other websites, addresses, email addresses, contact information or phone numbers; or
- that contains any computer viruses, worms or other potentially damaging computer programs or files.

Image: Behr Customer Ratings and Reviews Terms and Conditions - Prohibited content clause

It's not necessary to create a separate agreement for something like this, but mentioning it within a clause in your Terms and Conditions is a good idea.

Where to Display Your Terms and Conditions on Your Ecommerce Store

Terms and Conditions **can fail to take legal effect** if it's found that your customers did not have a good enough opportunity to examine them or didn't **properly agree to them**. There's a whole area of case law about contracts that were not enforced by the courts for this reason.

Ecommerce stores have no excuse to end up in this situation. You aren't delivering your terms on a sign hidden behind a counter or a letter that gets lost in the mail. You can make sure your customers have read and agreed to your terms before they make a purchase.

On Your Website

You'll want to put a link to your Terms and Conditions in your website's **footer** so you can make it available on **every page** of your website.

Here's an example from [The Broken Token](#):

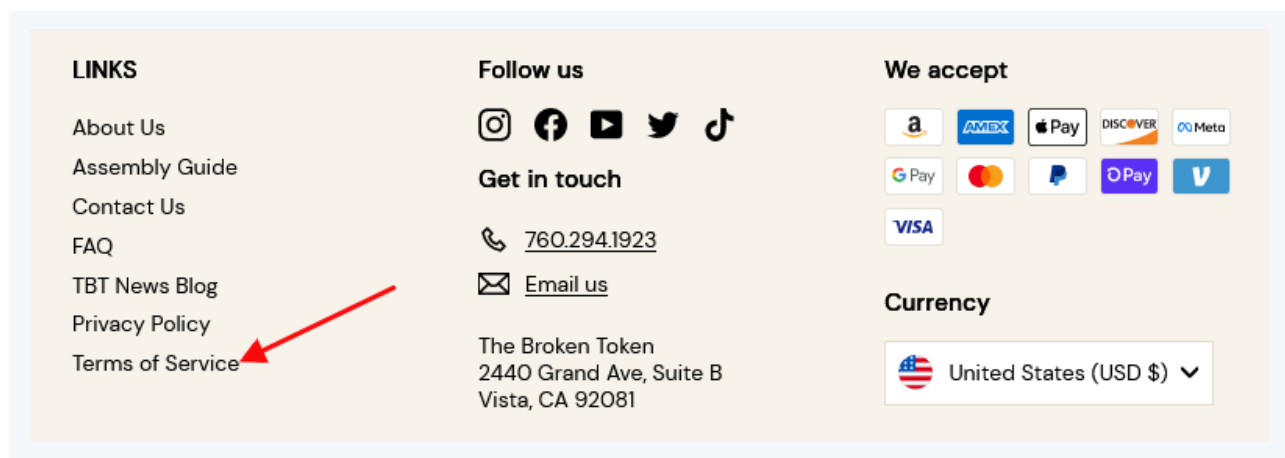


Image: The Broken Token website footer with Terms of Service link highlighted

You also need to present your Terms and Conditions in [clickwrap](#) form before your customer makes a purchase or signs up for an account. Basically, any time a contract is formed between you and the user.

Request that your users proactively [check a box](#) to show that they have read and agree with your Terms and Conditions.

Here's an example of a standard click to accept checkbox you can use:

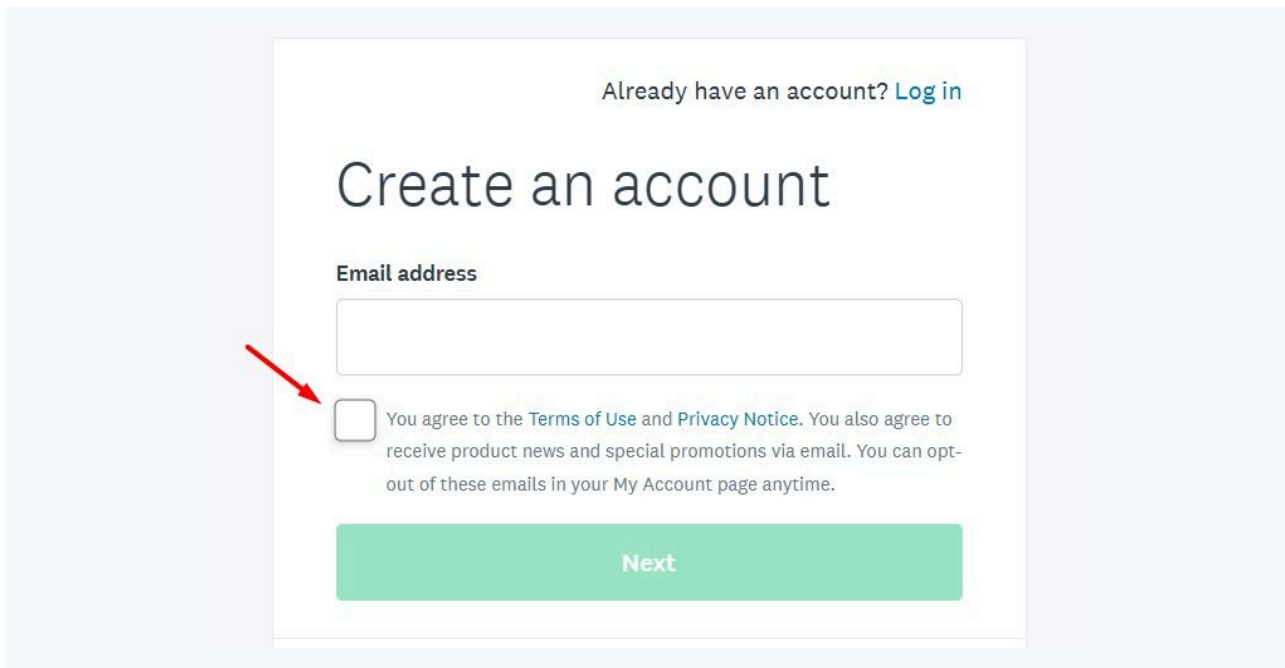
A screenshot of a 'Create an account' form. At the top, it says 'Already have an account? [Log in](#)'. Below that is the title 'Create an account'. There is a text input field for 'Email address'. Below the input field is a checkbox, which is highlighted with a red arrow. To the right of the checkbox is the text: 'You agree to the [Terms of Use](#) and [Privacy Notice](#). You also agree to receive product news and special promotions via email. You can opt-out of these emails in your My Account page anytime.' Below the checkbox and text is a green button labeled 'Next'.

Image: Generic Create Account form with I Agree checkbox highlighted - example

The alternative is what's called a "[browsewrap](#)" agreement, where the customer is deemed to have agreed to your Terms and Conditions merely by using your website or buying a product. This is **not a safe way** to ensure that your customer really agrees to your terms, and you risk not having your terms be enforceable in court.

Within Your Mobile App

Since mobile apps don't have site footers, you'll need a slightly different approach here. That's where your in-app menus come into play. **Display your Terms agreement within a menu in your app's interface.**

Here's an example of a Settings menu with legal agreement links:

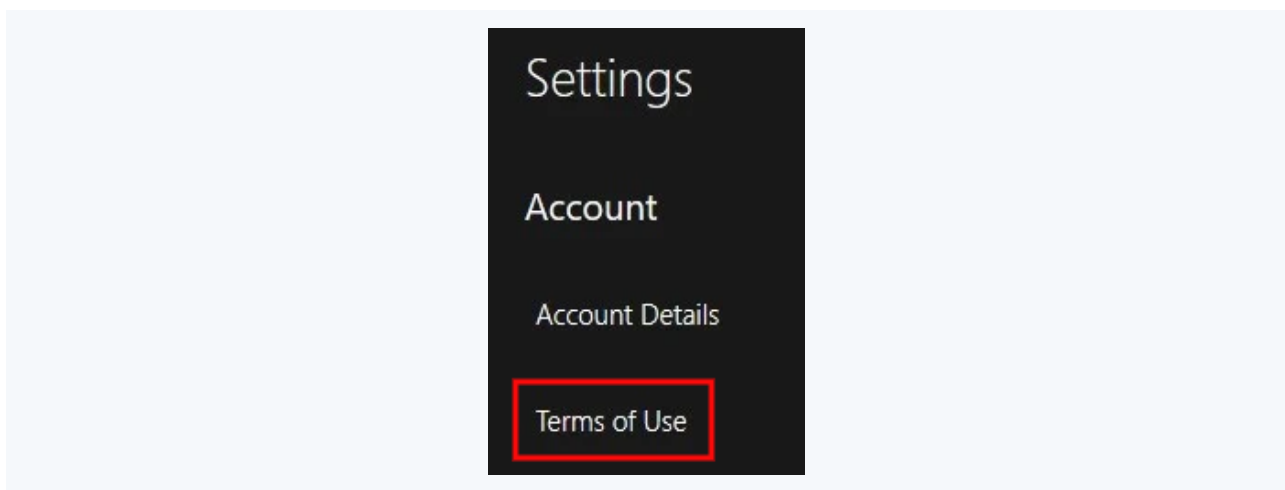


Image: Generic app Settings menu with Terms of Use link highlighted

You can also present it to users at download/sign-up, when creating an account with your app, requesting that they tap a button to show agreement. Here's an example:

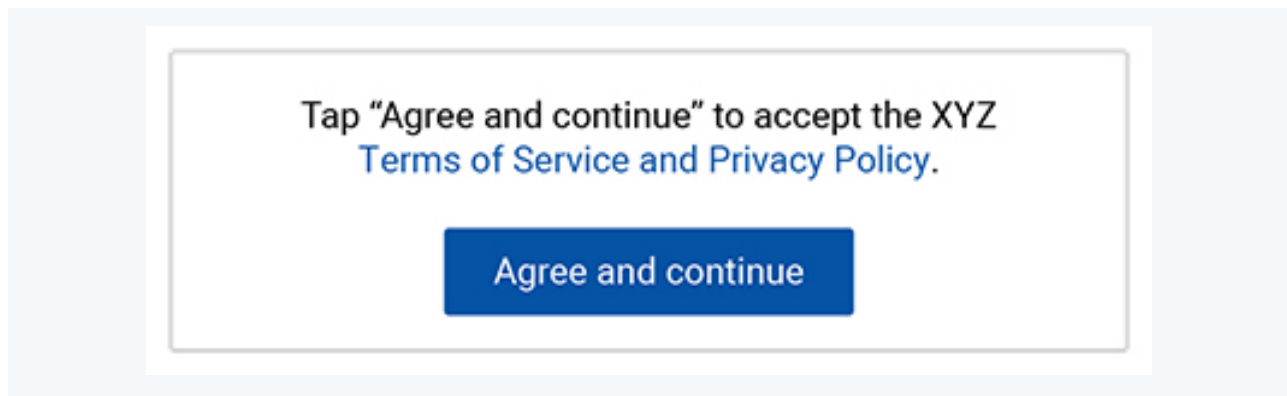


Image: Generic App - Tap Agree and continue button - example

Other Locations

You should make reference to your Terms and Conditions in **other legal agreements** such as your Privacy Policy. This cross-linking helps ensure that it's even easier for users to find all of your legal agreements, since if they find even one, they find the others by default. This also works to ensure agreement to all, since agreeing to one by default will get agreement to the others.

Here's an example of something you can include in your Privacy Policy to integrate your Terms agreement:

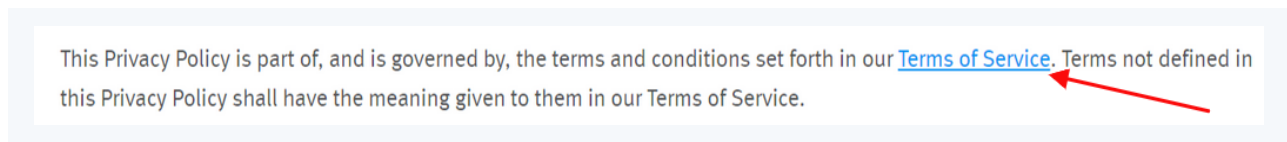


Image: Generic Privacy Policy with Terms of Service link highlighted

Case Study

Joshi's Jogging is a fitness products company based in the United States. It ships **domestically**, offering a range of delivery options, and internationally to **Canada** and the **EU**.

Joshi's Jogging should create a Terms and Conditions that:

- Links visitors to its **Privacy Policy** and any other policies that they should read
- **Limits its liability** for any losses resulting from the use of its products
- **Disclaims the warranties of merchantability and fitness for purpose** under U.S. law
- Explains that the disclaimers and limitations it sets out are valid to the **fullest extent permitted by law**

- Sets out the associated **costs** that customers might incur through **delivery**
- Explains that **overseas customers** are responsible for paying any **customs duties**
- Sets out, or points to, the store's **Return and Refund Policy**. This policy should be compliant with the laws of the jurisdictions in which it operates. (We'll cover this in more detail in the next chapter.)

Chapter 5:

Return & Refund Policy and Ecommerce Businesses

Customers routinely look for a [Return and Refund Policy](#) when deciding where to shop online. In fact, a study suggests that [67 percent](#) of online shoppers checked the returns page before making a purchase online.

Consumers are, quite naturally, nervous about buying products that they haven't seen directly or clothes they haven't tried on. Having a **clear and comprehensive** Return and Refund Policy is reassuring and it shows your company's professionalism.

So while you aren't legally required to have a Return and Refund Policy, it's a really good idea for your business to have one, and one that can actually pay off. Having one also allows you to retain some control over the conditions under which you allow returns.

Laws on Returns and Refunds

Depending on where your ecommerce business operates from, the law may enforce a **minimum level** of consumer protection. You need to make sure you're obeying the law of the jurisdiction in which your ecommerce business is based.

You're only bound by the laws of the country your business is established in - **not** necessarily the country your customer is buying from. This is unlike privacy law, where, for example, non-EU businesses are still expected to obey EU law.

Bear in mind, though, that any ecommerce business offering a better Return and Refund Policy has a competitive edge over yours in this regard. Therefore, it is worth getting to know what level of protection your international customers are **entitled to**, and what they might **expect** you to provide.

United States

There's very little consumer protection at the federal level in the United States. In the last chapter we looked at the implied warranties of merchantability and fitness for purpose imposed by the Uniform Commercial Code, and how these can often be disclaimed in a company's Terms and Conditions. There's also a federal law regarding specific issues such as [door-to-door selling](#). That's about it.

Even at the state level, businesses are largely free to create whatever Return and Refund Policy they want. However, there are **some requirements** about how certain types of policies must be **displayed** in certain states.

[State laws on refunds](#) generally refer to bricks-and-mortar stores. Where a statute requires a business to post its Return and Refund Policy "**conspicuously**," it generally refers to a **physical location** in a store, e.g. at the cash register, on the wall, etc.

There's only one sensible way for ecommerce stores to interpret this. Make sure your customers **see** (and will **agree that they've seen**) your Return and Refund Policy **before** they make their purchase. One way you can do this is by incorporating the policy into your Terms and Conditions, as mentioned in the previous chapter.

Here is some state-specific information:

[California](#)

California law promotes providing customers with information they might reasonably expect. Businesses should offer a full refund or store credit, an equal exchange, or some combination of these options when a refund is requested with proof of sale within seven days of purchase.

Businesses don't have to offer this policy. A business can have any Return and Refund Policy it wants. This can even be "no refunds."

But if a business **has** a Return and Refund Policy that deviates from the standard policy, they **must** post it **conspicuously**, and it must be detailed. If a business fails to do this correctly, it is violating [California Civil Code § 1723](#).

Where no policy has been conspicuously posted, the customer can return any new item, with proof of purchase, within **thirty days** of purchase for a refund.

[Connecticut](#)

A business can write its own Return and Refund Policy. It must post the policy conspicuously.

Where no policy has been conspicuously posted, the customer can return any new item, with proof of purchase, within **seven days** of purchase for a refund.

This **doesn't apply** to goods sold "as is" or "final sale."

[Florida](#)

A business can write its own Return and Refund Policy. It must post the policy conspicuously.

Where no policy has been conspicuously posted, the customer can return any new item, with proof of purchase, within **seven days** of purchase for a refund.

[Hawaii](#)

Businesses can have one of **four** return policies:

1. Refunds only
2. Refunds or merchandise credit only
3. Exchanges or merchandise credit only, or
4. No refunds, merchandise credit or exchanges

The policy must be conspicuously posted, and if your return period is less than 60 days, this must be clearly noted. Any excluded categories of items must also be conspicuously noted, such as no returns on seasonal or sale items.

Where a refund policy is not conspicuously posted, the business must offer a refund for any goods returned within **60 days** of purchase.

If a business offers merchandise credit and a shopper can't find a suitable substitute item to use the credit on within 30 days of the return, the shopper is entitled to a cash refund unless the business has posted a conspicuous notice stating that credit cannot be turned into cash. Merchandise credits must remain valid for at least 2 years.

[Illinois](#)

A business can write its own Return and Refund Policy.

There are some very specific rules around transactions involving door-to-door selling, gyms and hearing aids.

[Maryland](#)

A business can write its own Return and Refund Policy. It must post the policy conspicuously - in size 12 font.

Where no policy has been conspicuously posted, the customer can return any new item, with proof of purchase, within "**a reasonable period**" with proof of purchase for a refund.

[Massachusetts](#)

A business can write its own Return and Refund Policy. It must post the policy conspicuously. The statute emphasizes the requirement that the customer **must see the policy before making a purchase**.

Where no policy has been conspicuously posted, the customer can return any new item, with proof of purchase, within "**a reasonable period**" of purchase for a refund.

[Minnesota](#)

A business can write its own Return and Refund Policy. It must post the policy conspicuously - in size 14, bold font.

Where no policy has been conspicuously posted, the customer can return any new item in good condition with proof of purchase within "**a reasonable period**" of purchase for a refund.

New Jersey	<p>A business can write its own Return and Refund Policy. It must post the policy conspicuously. The policy must contain certain information such as whether it will give a refund for:</p> <ul style="list-style-type: none"> • Products on "sale" or sold "as is" • Without proof of purchase • Products returned beyond a particular time period, or • In cash, credit or store credit <p>Where no policy has been conspicuously posted, the customer can return any item within 20 days for a refund or a credit.</p>
New York	<p>A business can write its own Return and Refund Policy. It must post the policy conspicuously.</p> <p>Where no policy has been conspicuously posted, the customer can return any item within 30 days. The business is not restricted in how they refund the customer (e.g. by cash, credit or exchange).</p>
Ohio	<p>A business can write its own Return and Refund Policy. It must post the policy conspicuously, ensuring it is visible before the point of sale.</p> <p>Where no policy has been conspicuously posted, the customer is entitled to a refund. There are no caveats regarding timescale or types of goods given in the statute.</p>
Rhode Island	<p>A business can write its own Return and Refund Policy. It must post the policy conspicuously.</p> <p>Where no policy has been conspicuously posted, the customer can return any item within 10 days.</p>
Virginia	<p>A business can write its own Return and Refund Policy. It must post the policy conspicuously.</p> <p>Where no policy has been conspicuously posted, the customer can return any item within 20 days.</p>

Table 1: US States specific Return and Refund Policy information

Where refunds are required under these laws, this doesn't generally apply to **food** products or other **perishable** items.

Remember that in some states it isn't possible to disclaim the implied warranties of merchantability and fitness for purpose. These states are listed in the previous chapter.

European Union

Consumer protection in the EU is very strong. There are [many rules](#) imposed on businesses, and no way of avoiding them.

Customers in all EU countries have these rights, and in some countries the law is even stronger. This means that you can offer a *better* Return and Refund Policy than the law requires, but you can't offer a *worse* one.

Legal Warranty

Under the Consumer Sales and Guarantees [Directive](#), all goods purchased new in the EU carry a **two-year warranty**, minimum. Used goods carry a warranty of at least one year, with many EU countries enforcing a period of two or more years.

If goods are faulty when sold or develop a defect within two years of purchase, the seller must make this right for the customer. The seller can offer to **repair** or **replace** the product. If this isn't possible, they must offer a **full** or **partial refund**.

Returns for Online Purchases

Under the Consumer Rights [Directive](#), customers who have bought products **online** (or via mail or phone) have 14 days to **change their minds** and return a product for a full refund. The 14-day period starts from the day that the customer receives the order.

The customer might have to pay for the return. However, if the business hasn't warned them of any charges they might incur in returning the goods, then the business has to cover the costs of return.

The refund must include any **shipping costs** that the customer has paid and it must be delivered within **14 days** of the business receiving the product.

This doesn't apply to **digital** products that have already been used or partially used (e.g. a partially-watched downloaded film).

Other Jurisdictions

- [Canada](#): different provinces have their own laws that regulate consumer protection, for example the Sale of Goods [Act](#) in British Columbia and the Consumer Protection [Act](#) in Quebec. There is **no obligation** to provide a refund or warranty at a national level.
- [Australia](#): all goods sold for under \$40,000 or sold for household purposes carry an **implied warranty** that they are of satisfactory quality and fit for purpose. The duration of this warranty is based on **reasonable expectations** about the product's lifespan. It is unlawful for a business to state that they don't offer a refund under any circumstances.

What to Include in Your Return and Refund Policy

So long as you are obeying the law, the scope of your Return and Refund Policy is a business decision. It requires you to balance your customers' expectations against the costs that your business is able to absorb.

But whatever your Return and Refund Policy may be, there really is no good reason for it not to be **clear, comprehensive and easily accessible**.

Let's look at what your Return and Refund Policy needs to include.

Whether You Accept Returns

You must be explicit about whether you accept returns and are willing to grant refunds or exchanges.

Here's an example of a quite restrictive Return and Refund Policy from fashion retailer [NA](#):

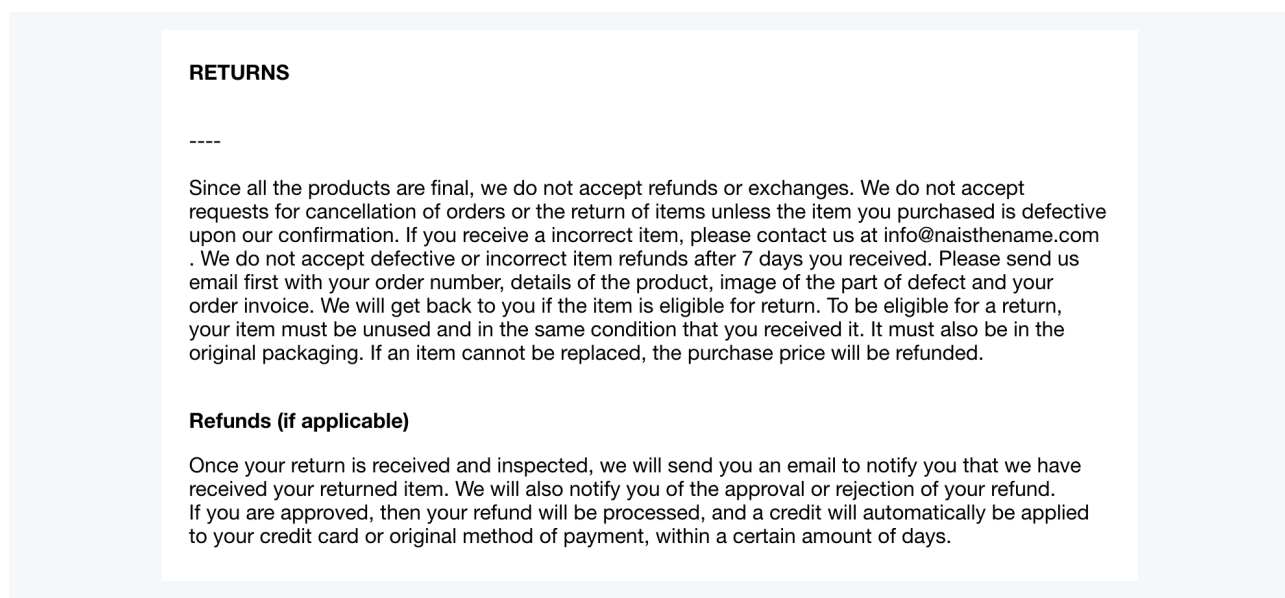


Image: NA Orders and Returns: Returns and Refunds sections

It reads:

RETURNS

Since all the products are final, we do not accept refunds or exchanges. We do not accept

requests for cancellation of orders or the return of items unless the item you purchased is defective upon our confirmation. If you receive a incorrect item, please contact us at info@naisthenname.com . We do not accept defective or incorrect item refunds after 7 days you received. Please send us email first with your order number, details of the product, image of the part of defect and your order invoice. We will get back to you if the item is eligible for return. To be eligible for a return, your item must be unused and in the same condition that you received it. It must also be in the original packaging. If an item cannot be replaced, the purchase price will be refunded.

Refunds (if applicable)

Once your return is received and inspected, we will send you an email to notify you that we have received your returned item. We will also notify you of the approval or rejection of your refund.

If you are approved, then your refund will be processed, and a credit will automatically be applied to your credit card or original method of payment, within a certain amount of days.

Bear in mind that such a policy wouldn't be lawful in some jurisdictions, such as the EU.

Exceptions and Conditions

Many ecommerce operations offer a more generous Return and Refund Policy than is required by law, but there will almost always be some restrictions on what will be refunded. It's important that you are clear about any restrictions and conditions.

You need to state:

- **Which products** are covered by your policy
- The **period** for which products can be returned
- Any requirement that the products are **unopened or in good condition**

For example, here's how you can outline exceptions and additional details:

Return Exceptions

Electrics and Electronic Items

- Electric and electronic items can be exchanged or returned within one year of purchase and must be accompanied by a receipt. Examples include, but are not limited to, small kitchen appliances, personal care appliances, vacuums, baby monitoring devices, and smart home products.

Baby, Toddler and Maternity Merchandise

- All baby, toddler and maternity merchandise must be new and in original packaging.
- All baby, toddler and maternity clothing, A Pea in the Pod®, and Motherhood Maternity® items must be new and unused. These items may only be returned within 90 days of purchase with all tags attached.
- Formula cannot be exchanged or returned.

Air Mattresses

- Opened air mattresses may only be exchanged for a similar item.

Customized Items

- Monogrammed, personalized, custom-made, or special order items cannot be exchanged or returned.

Other

- Shipping, delivery and assembly charges are non-refundable.
- All gift cards are non-refundable.
- [Mattresses](#)
- [Truck Delivery](#)

Image: Bed Bath and Beyond Simple Returns - Return Exceptions section

Failing to be clear about the exceptions to your Return and Refund Policy could lead to disputes with your customers.

Here's another example:

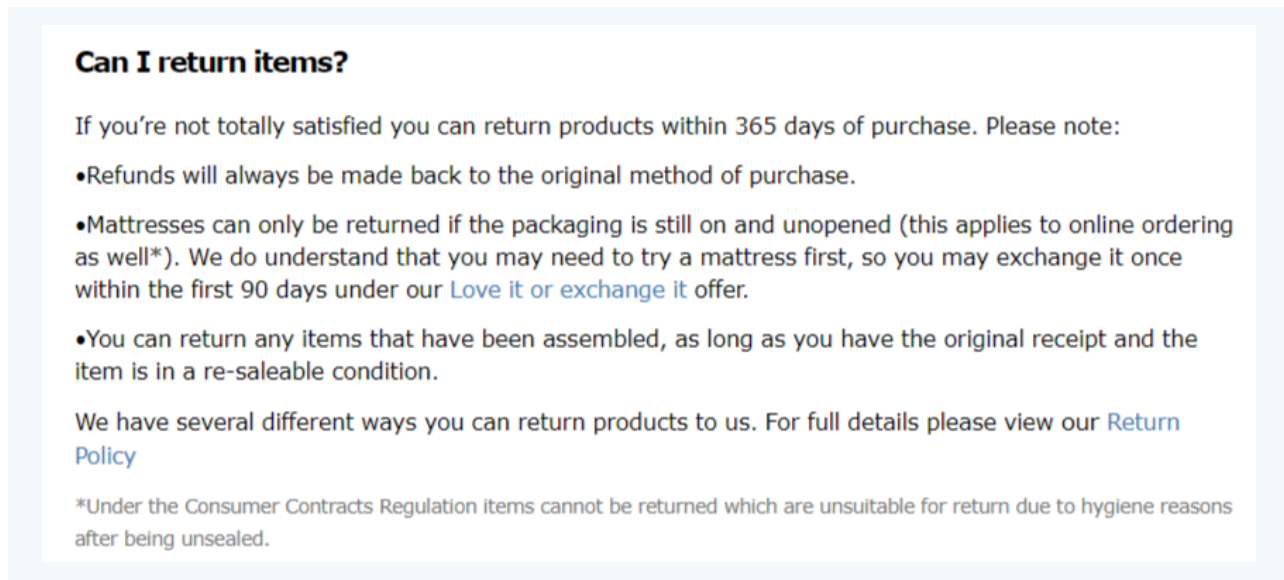
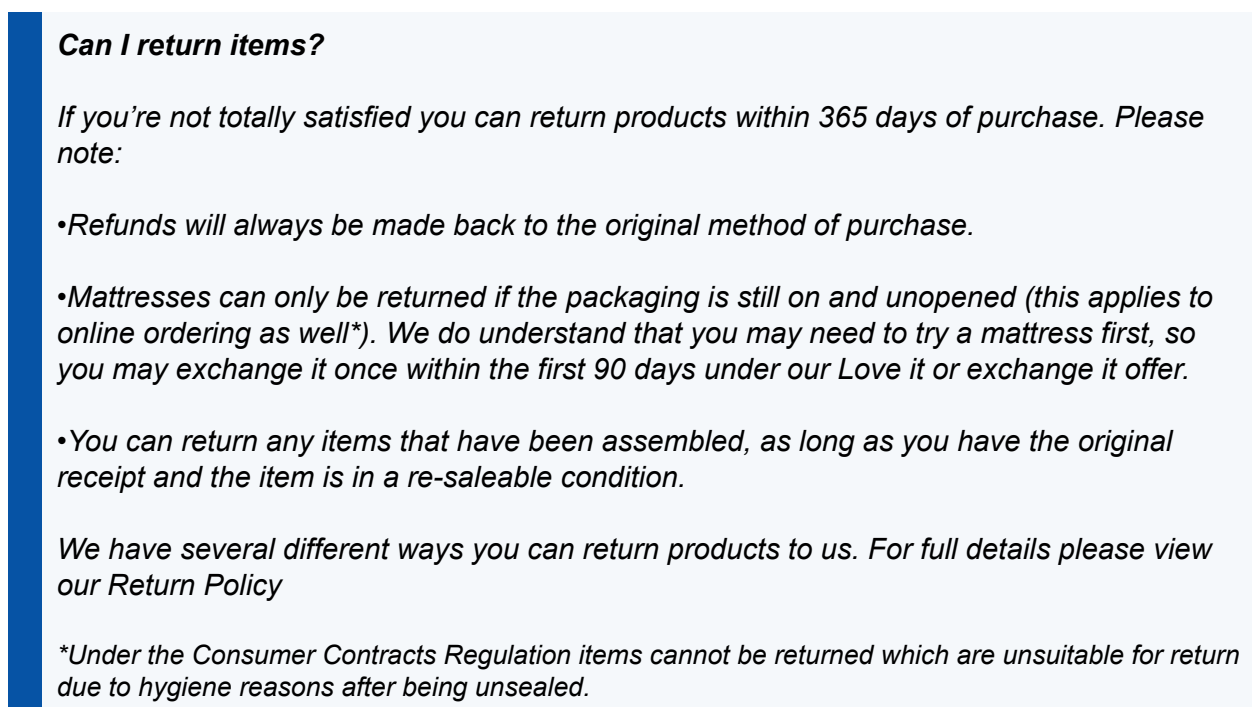


Image: IKEA Returns and Product Issues: Can I return items section

It reads:



Any conditions that you place on returns need to be detailed in your Return and Refund Policy. For example, this Return Policy notes that sometimes requires that customers verify themselves in order to use merchandise credit that has resulted from a refund:

Return Policy

Our customers continue to be our top priority. If you're not satisfied with your purchase, return the merchandise accompanied by a register receipt within 30 days of purchase for an exchange or refund in the original form of tender. A 10-day period is required for a cash refund on check purchases. Returns with a receipt over 30 days, with a gift receipt or without a receipt will receive merchandise credit only. Merchandise credits are subject to the Terms and Conditions printed thereon and imposed by the issuer which may include restrictions on transfers.

Merchandise that is used, worn or in unsellable condition will not be accepted for refund, merchandise credit or exchange. Returns of swimwear and intimate apparel require tickets properly attached to the merchandise. Other restrictions may apply.

Unfortunately, many retailers are subject to fraudulent return activity. Returns may also be limited or declined based upon our refund verification systems, which are used to process and track returns to help administer our loss prevention program.

A valid government issued photo ID, name, address, and signature are required for non-receipted returns and may be required for use of the resulting merchandise credit. Any name printed on the merchandise credit must match the name on the photo ID presented or the merchandise credit may not be used. A customer signature may also be required for receipted returns. To learn about how we use and handle your information, please see our [Privacy Notice](#).

To make your returns quicker and easier please keep your receipt.

Image: HomeGoods Return Policy - Valid photo ID may be required section highlighted

It reads:

Return Policy

Our customers continue to be our top priority. If you're not satisfied with your purchase, return the merchandise accompanied by a register receipt within 30 days of purchase for an exchange or refund in the original form of tender. A 10-day period is required for a cash refund on check purchases. Returns with a receipt over 30 days, with a gift receipt or without a receipt will receive merchandise credit only. Merchandise credits are subject to the Terms and Conditions printed thereon and imposed by the issuer which may include restrictions on transfers.

Merchandise that is used, worn or in unsellable condition will not be accepted for refund, merchandise credit or exchange. Returns of swimwear and intimate apparel require tickets properly attached to the merchandise. Other restrictions may apply.

Unfortunately, many retailers are subject to fraudulent return activity. Returns may also be limited or declined based upon our refund verification systems, which are used to process and track returns to help administer our loss prevention program.

A valid government issued photo ID, name, address, and signature are required for non-receipted returns and may be required for use of the resulting merchandise credit. Any name printed on the merchandise credit must match the name on the photo ID presented or the merchandise credit may not be used. A customer signature may also be required for receipted returns. To learn about how we use and handle your information, please see our Privacy Notice.

To make your returns quicker and easier please keep your receipt.

If you charge a **restocking fee** on certain refunds, you'll also have to make this clear in your policy. Here's an example:

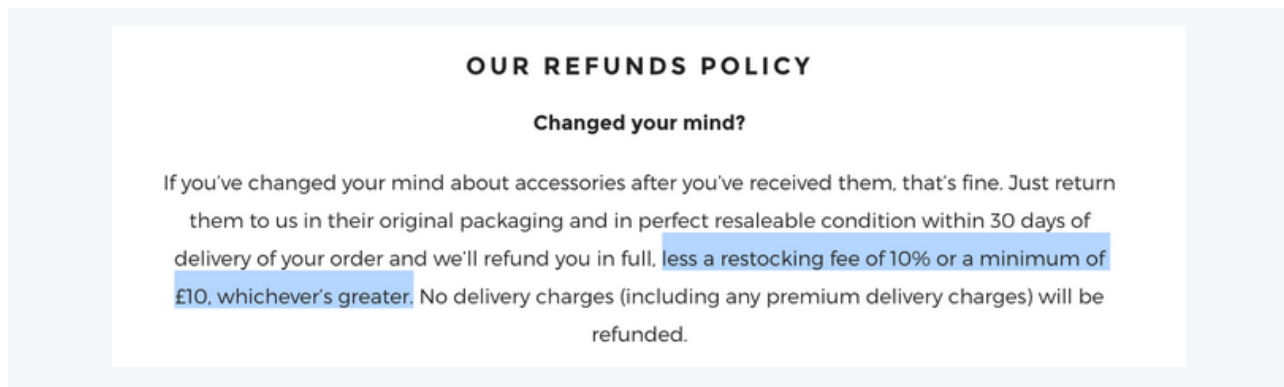
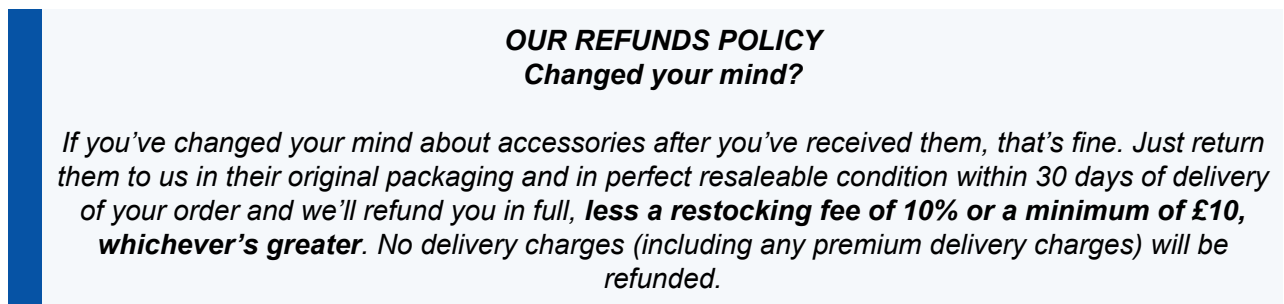


Image: Big Green Eggs Returns Policy - Restocking fee information highlighted

It reads:



Instructions for Making a Return

You should give details of **how** your customers can make a return.

Here's an example of a creative method which allows for a business to absorb shipping costs for the customer:

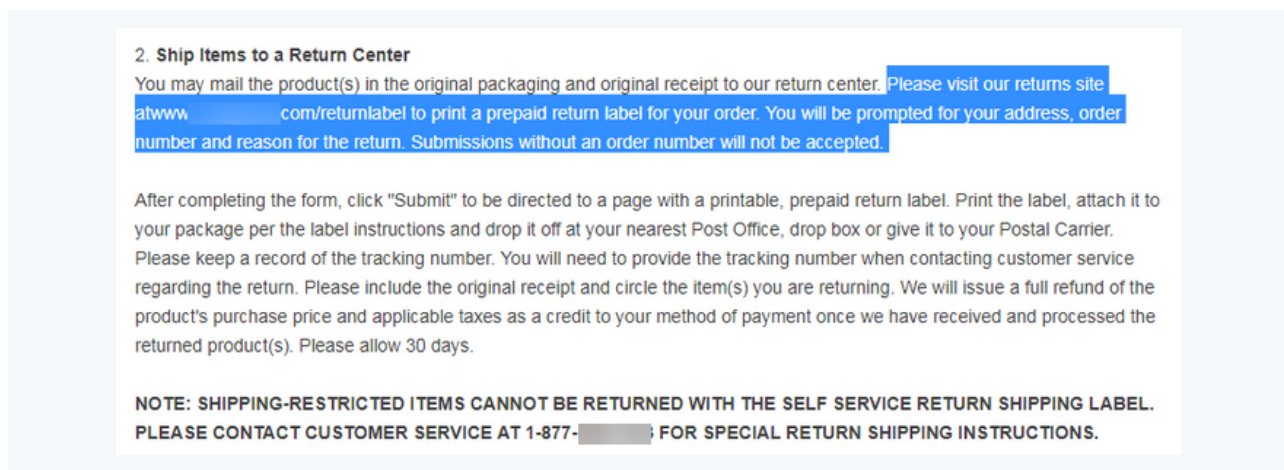


Image: Walgreens Returns Help - Instructions highlighted

Refunds are usually made to the customer's original payment method. This can be surprisingly complicated, depending on which payment methods you allow customers to use.

Here's an example of how you can handle this:

Product(s) returned within 60 days of the original purchase that include the original receipt (or can be verified in our system using your Ultimate Rewards member ID), will be fully refunded via the original form of payment. Otherwise, the refund will be made in the form of an in-store credit.

Products returned to stores that were purchased using an online payment service (i.e., PayPal, PayPal Credit) will be refunded to your preferred credit card or issued as a store merchandise credit.

Image: Ulta Beauty Return Policy excerpt

You must warn your customers if you expect them to take on any costs associated with returning a product. For example, if there's a restocking fee or if they must pay for return shipping.

Here's an example of this:

How do I return my item?

Please inform us of your intention to return your product by contacting our Returns Department on [redacted] or [contact us via email](#), and you will be given a returns authorisation number. Returned goods will only be accepted when a returns number has been given.

- The product must be returned to us **within 30 days of delivery to you.**
- The products must be returned in their original condition, including outer packaging, unused and in perfect saleable condition.
- You should return the product [at your own cost](#) to the returns address. Ensure that the product arrives safely to us, we strongly recommend that you return the product to us by recorded post.

Image: Salon Services Returns Policy: Returns at your own cost section highlighted

It's a good idea to let your customers know **how long** a refund will take. Bear in mind that there are regulations on this in some jurisdictions.

Here's how you can do this:

RETURNING BY MAIL (U.S.)

If you have an account or an order number, you can start your return now. If you don't have an account or you're missing order information, you can print a blank return form and label. Send in your item(s) using the postage-paid U.S. return label. Your return will be processed **within 10-14 business days**.

Image: Nordstrom Return Policy - Processing timeframe highlighted

You should be clear about any instances in which you're only willing to offer a **partial refund**.

Here's an example of such a clause:

There are certain situations where only partial refunds are granted: (if applicable)
Any item not in its original condition, is damaged or missing parts for reasons not due to our error.
Any item that is returned more than 30 days after delivery

Image: Bootea Returns and Refund policy - Partial refunds section

Where to Display Your Return and Refund Policy on Your Website

As mentioned previously, it's always a good idea to refer to your Return and Refund Policy in your Terms and Conditions. It's also crucial that you post it clearly, for two reasons:

1. Your Return and Refund Policy will **reassure customers** about making a purchase. If they know that they're protected, they'll be more likely to buy from you.
2. Wherever refunds are regulated by law, there is often a **legal obligation** to post a Return and Refund Policy conspicuously. A failure to do this may mean that the policy **doesn't take effect**.

On Your Website

Often a business will link to its Return and Refund Policy in its **footer** so that customers are able to access the policy on any page.

Here's an example from [Amazon](#):

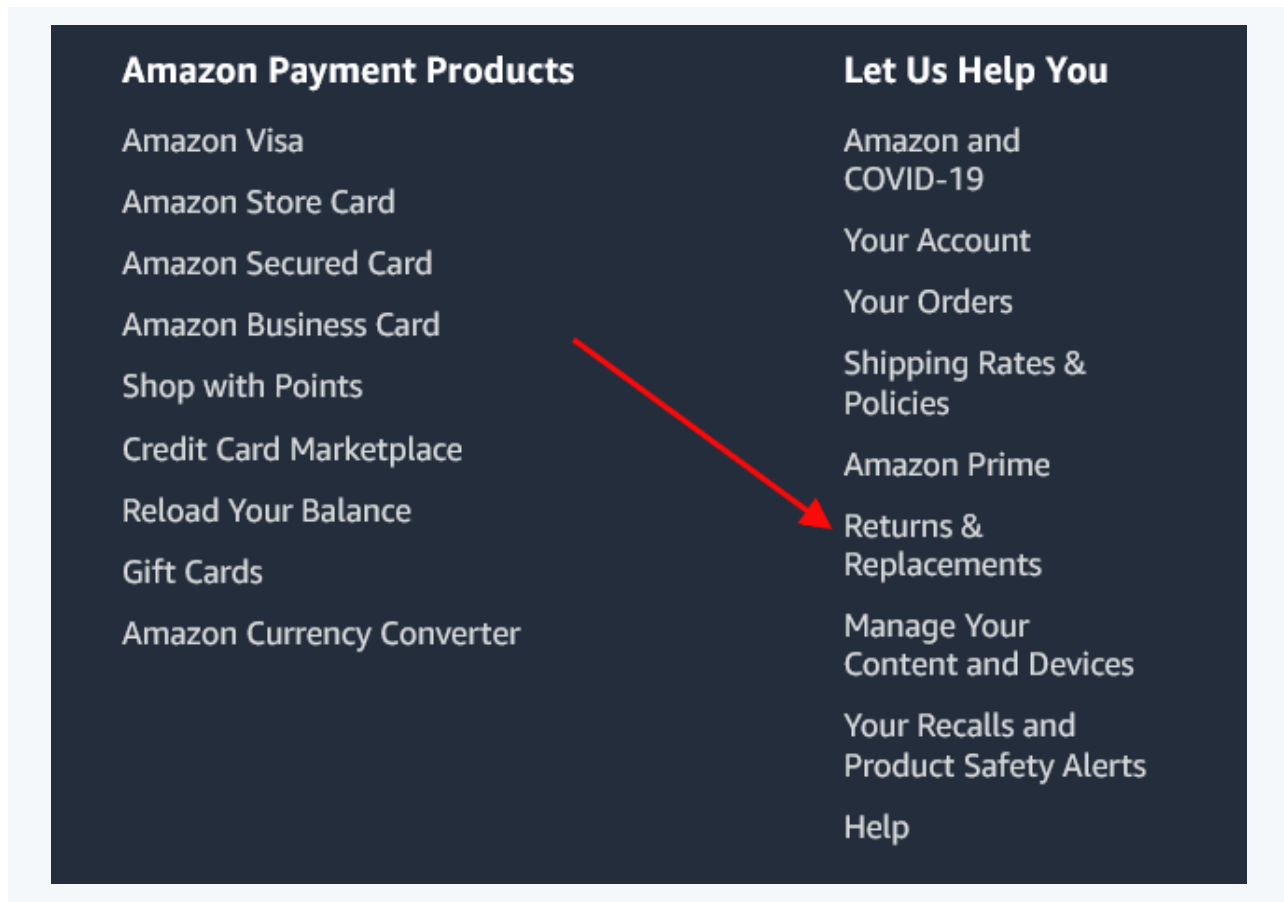


Image: Amazon website footer with Returns and Replacements link highlighted

Customers really like to see this policy, so companies often display it front-and-center. You can add something like the notice below to your website header so people will know right away that you have a great perk like free returns on all orders:

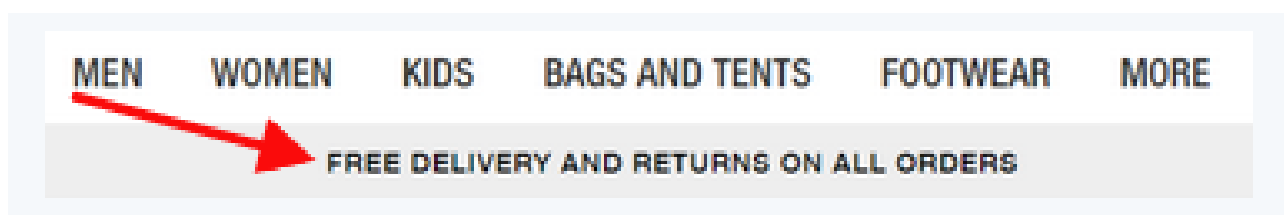


Image: Screenshot of The North Face website top banner bar

On a Mobile App

Think of the “Buy now” button as your mobile app’s cash register. Make sure you give your customers a chance to review your Return and Refund Policy right before they part with any money.

Here’s how Amazon handles this:

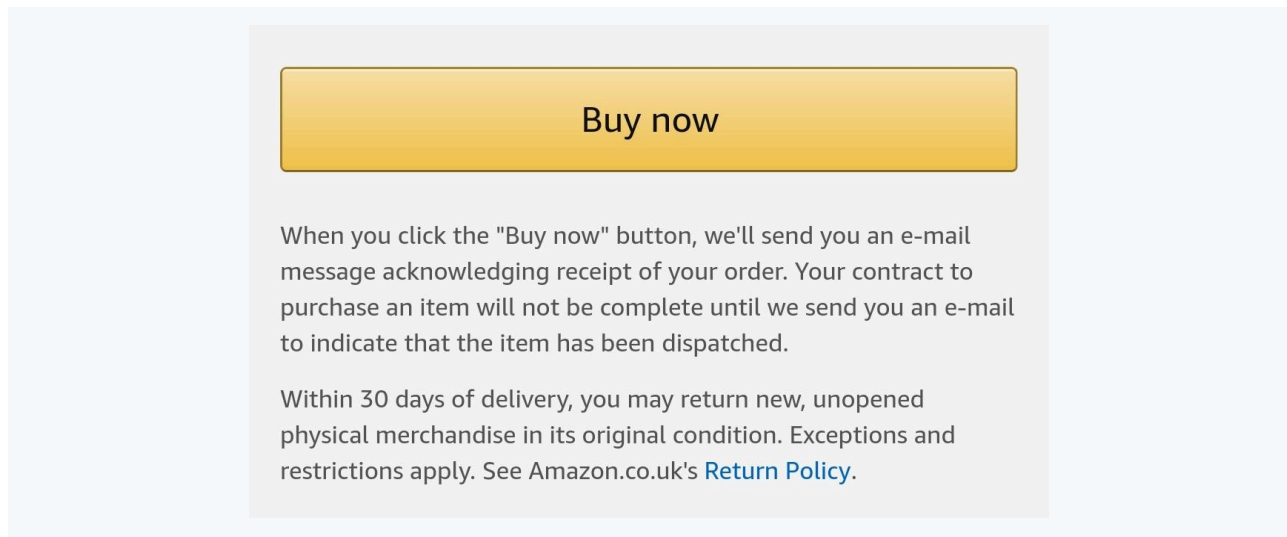


Image: Amazon app Buy now button with Return Policy link

The policy should also be available in the About or Help page of your app. Here's an example from the [Kindle](#) app:

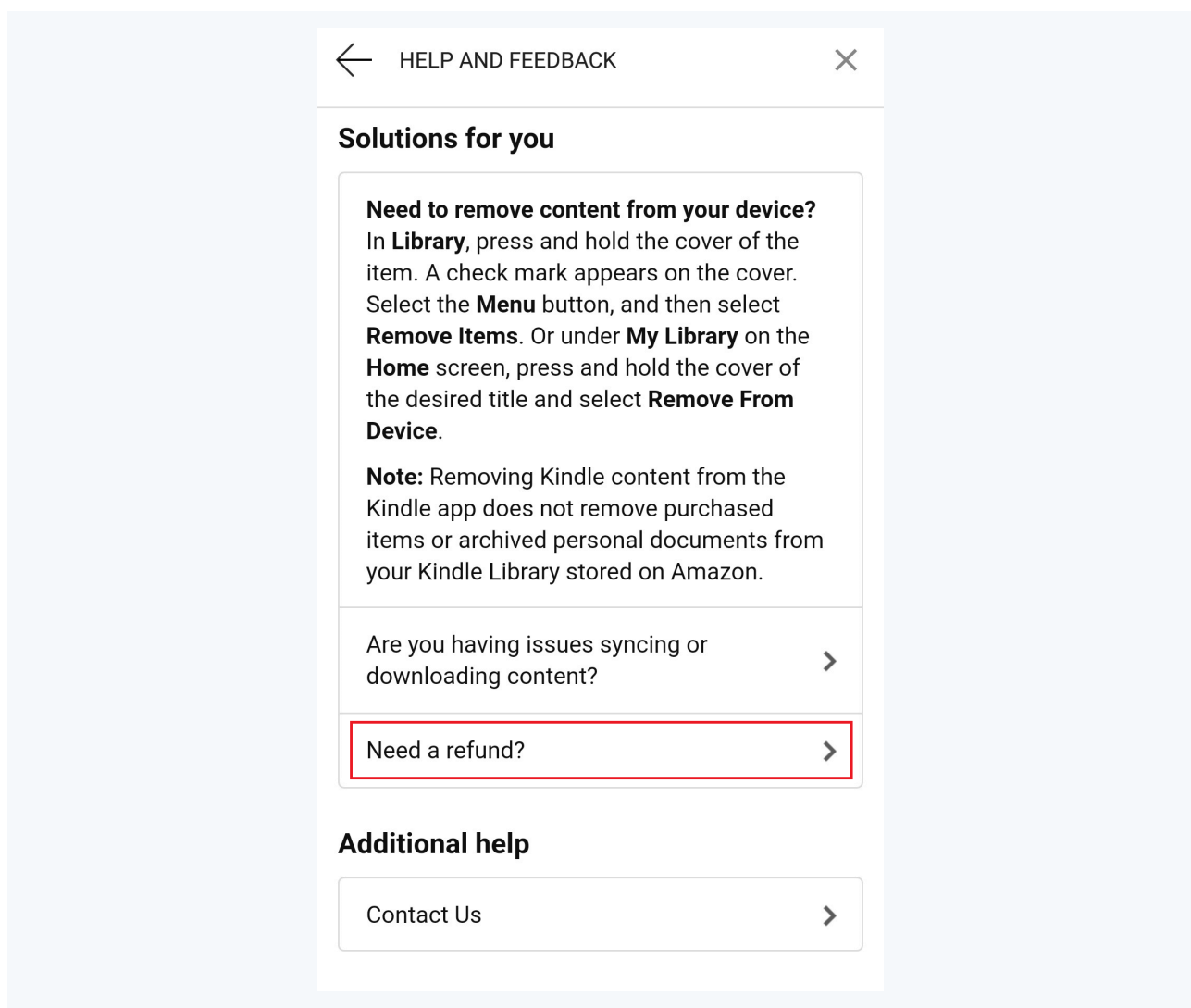


Image: Kindle app Help and Feedback screen - Need a refund? highlighted

Other Locations

Many companies very clearly connect their Return and Refund Policy in their Terms and Conditions like in the example below:

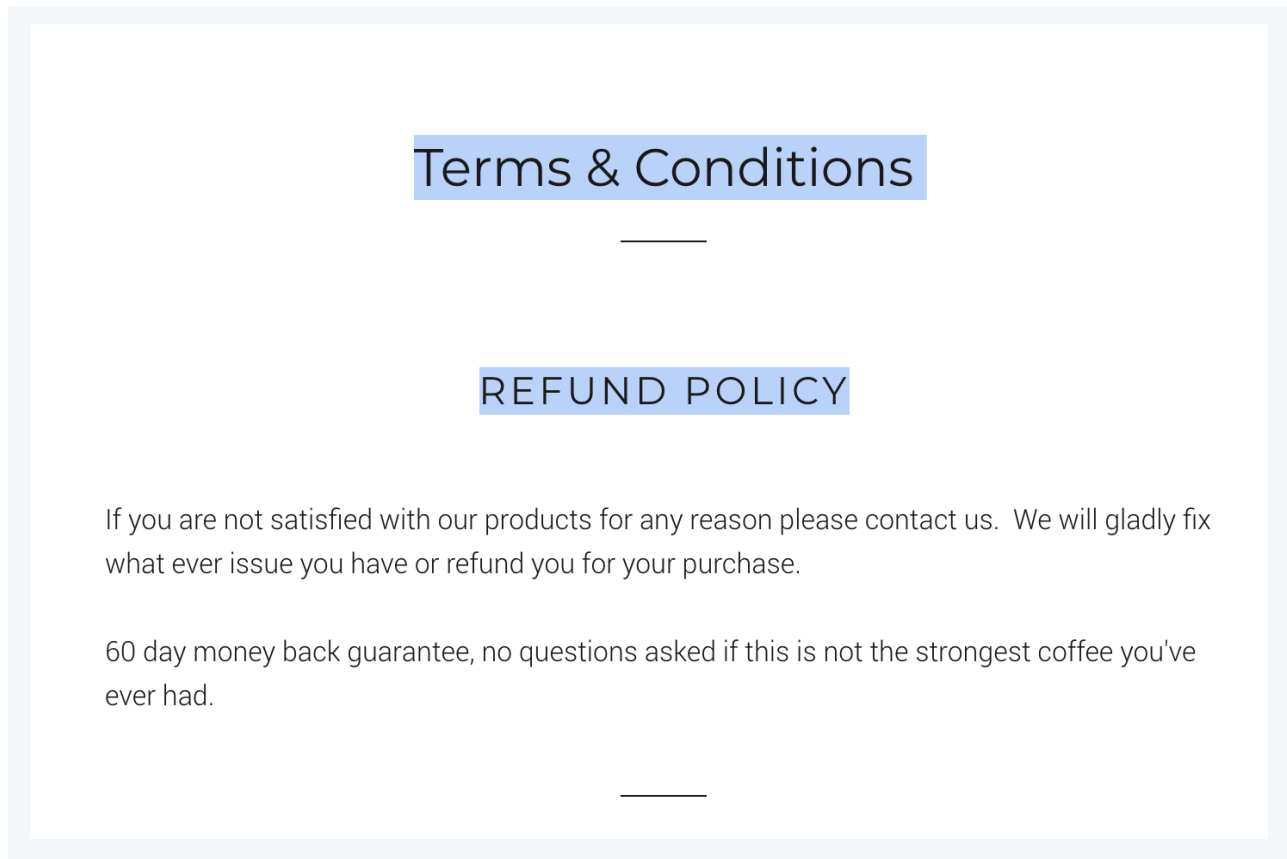
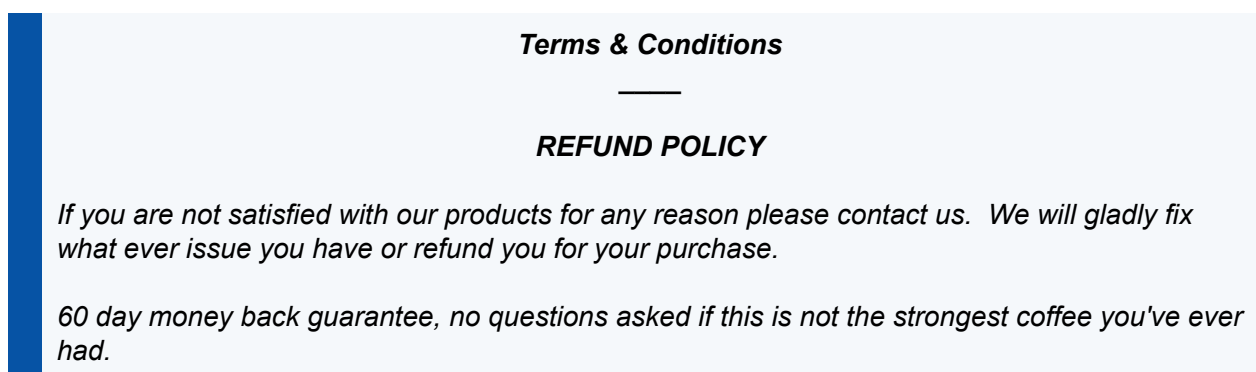


Image: Death Wish Coffee Terms and Conditions with Refund Policy included

It reads:



You should also provide a link to your Return and Refund Policy in confirmation emails.

Here's an example:

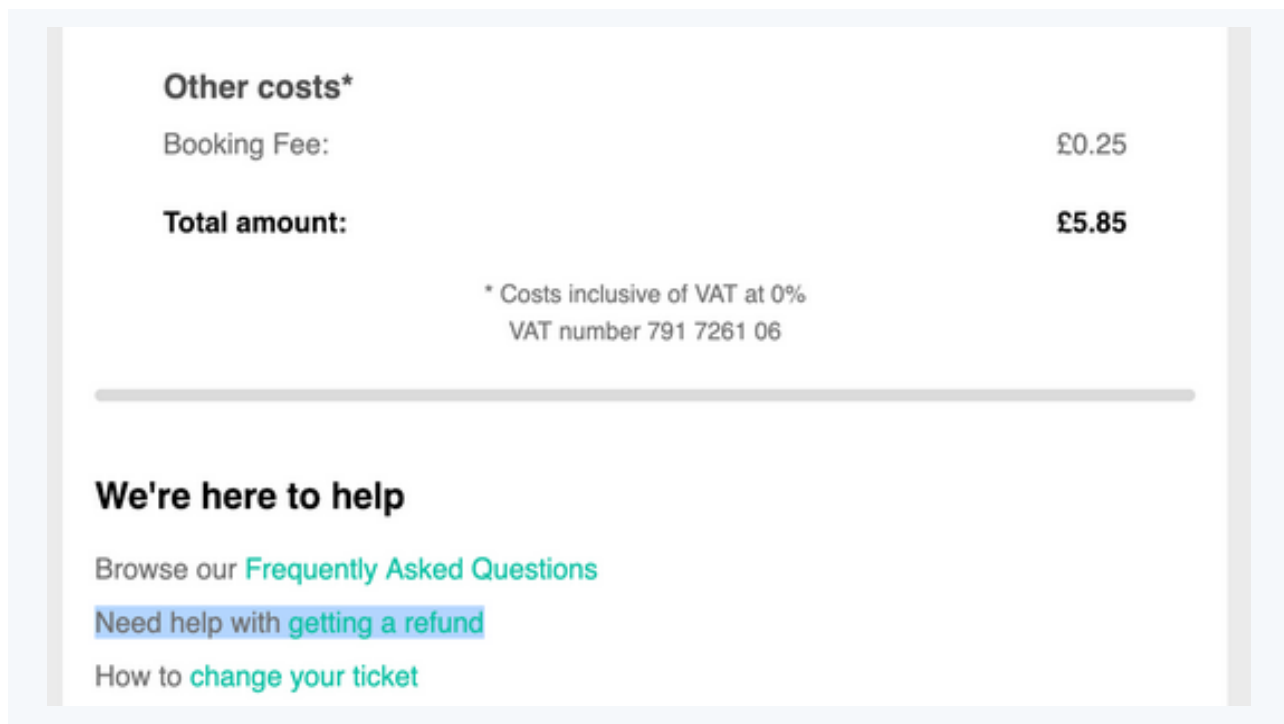


Image: Trainline email with refund help link highlighted

Your Return and Refund Policy is a great example of how you can use legal agreements to bring great **commercial benefit** to your company, and provide a **great service** to your customers. Just make sure that they read it!

Case Study

Sara's Sandwiches sells sandwiches and sandwich-making equipment. It runs a small store in New York, and an ecommerce store selling both food and non-food items. It serves customers all across North America and the EU.

Sara's Sandwiches wants to offer a **full refund** on items returned within 30 days, and an **exchange or merchandise credit** on any items returned within 60 days. Proof of purchase is required, and the policy doesn't cover **food items**.

Customers can arrange for a refund by sending their products back via **post**, or returning the item **in-store**. Customers must pay **shipping** for their return.

In addition to its Privacy Policy and Terms and Conditions, Sara's Sandwiches should write a Return and Refund Policy that:

- Is **conspicuously posted** on its website, in **emails** to customers, and **incorporated** into its Terms and Conditions
- Makes its policy **clear**, setting out **which items** will be refunded and what won't
- Provides the **timeframes** within which items must be returned

- Gives **instructions** on how to make a return
- Informs customers that refunds will be made to their **original payment method**
- Makes it clear that customers must **pay for shipping**

Chapter 6:

Disclaimers and Ecommerce Businesses

So far we've looked at three legal documents:

1. **Privacy Policy** - A legally mandatory statement about your data protection practices.
2. **Terms and Conditions** - An agreement between you and your customers which can protect you from legal claims and help you manage user actions.
3. **Return and Refund Policy** - An agreement between you and your customers which clearly sets out which products can be returned and on what terms.

We've also looked at two sorts of [disclaimers](#) so far:

1. A **disclaimer of warranties** - Ensures your company is not making implied promises about its services or products.
2. A **limitation of liability clause** - Allows you to manage the extent to which your company can be held legally liable for any losses that you cause your customers.

In this chapter, we'll be looking at other types of [disclaimers for your ecommerce store](#).

Terms and Conditions and a Return and Refund Policy contain certain disclaimers that aren't a legal requirement. But other disclaimers are legally required for certain products.

Using any product carries some degree of risk, however small. Your customers take on some of this risk when they buy and use one of your products. And by selling the product, your company takes on some risk as well. A disclaimer is a way for you to manage your side of this risk.

Responsibilities of Different Types of Businesses

Before we look at the disclaimers that ecommerce stores can use to warn customers about the risks of using the products that they sell, let's consider how liability arises further up the supply chain.

Manufacturers

If someone is injured or suffers another loss as a result of using a dangerous product, the first person they will usually look to sue is the manufacturer. The main responsibility for ensuring product safety and warning customers about the potential risks of using a product falls on manufacturers.

Disclaimers are extremely important for manufacturers, but they can only go so far. A manufacturer has a responsibility not to put dangerous or illegal products onto the marketplace, and they can't simply negate this responsibility by providing a warning for consumers.

If your ecommerce store sells goods that your company has produced, this is an especially big responsibility. You need to know the rules of your industry, and the risks associated with your products.

Here's an example of a set of disclaimers and warnings added to a product label by the manufacturer:

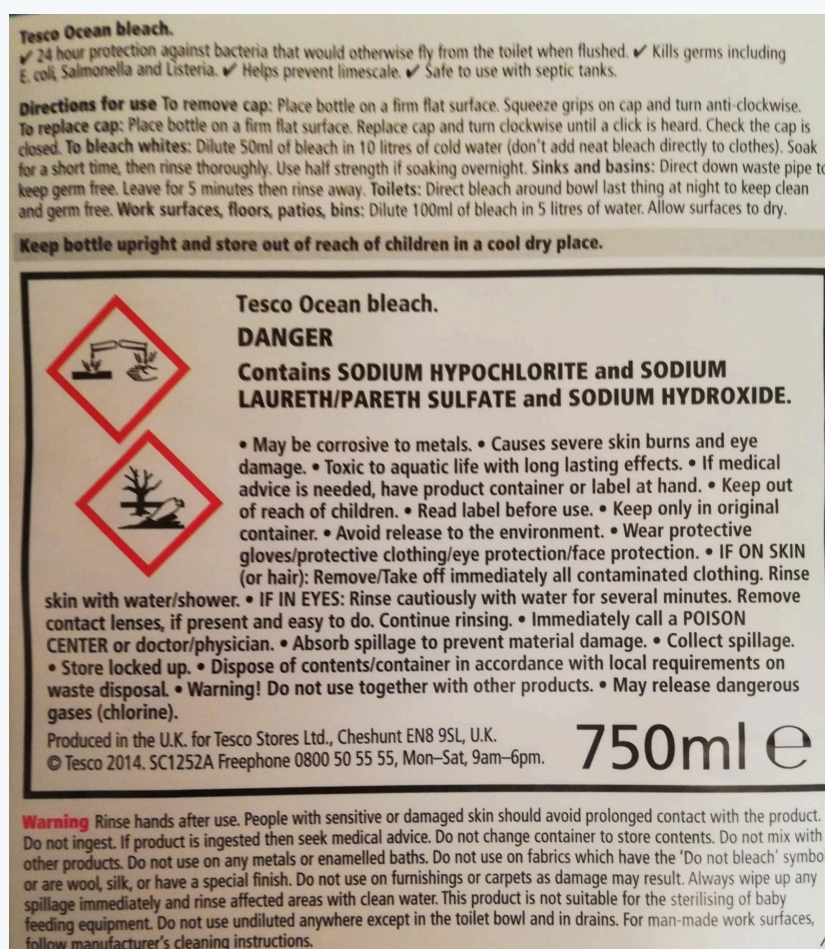


Image: Photograph of Tesco Ocean Bleach back label with disclaimers and warnings

Importers

If a consumer is injured by a product made overseas, it's difficult or impossible for them to seek damages from the manufacturer. Therefore, there's a duty on importers to ensure that any product they bring into a market meets the health and safety standards of their market.

In the U.S., the responsibility of importers to ensure adequate product safety and labeling is set out across a number of federal laws - for example, the Federal Food, Drug and Cosmetic [Act](#). And in the EU, under the General Product Safety [Directive](#), importers have the same legal responsibility as manufacturers where a manufacturer isn't established in the EU.

Some products are legal in some states or countries and not others. Some will require additional warnings when sold in some places that they might not require in others.

If your ecommerce store sells imported products, you'll need to know the relevant laws and standards inside out. It's not enough to say that you weren't aware that a product contained a particular component or ingredient, or that you weren't familiar with a regulation that applies to that type of product. This could be considered an act of negligence on your part.

Companies that Customize or Service Products

A manufacturer or importer can't be blamed for all injuries that might arise from the use of their products, particularly if the danger originated elsewhere in the supply chain.

If your company customizes, services or otherwise modifies products, you're responsible for ensuring that you do this in a safe and legal way. You could be liable for any damages resulting from the changes you've made to the product.

As a retailer, you have a big responsibility to sell safe products and provide accurate information. However, unless you manufacture all of your products from scratch, you'll never be able to absolutely control everything about all of the products that you sell.

Let's take a look at some examples of the requirements and best practices around disclaimers for retailers.

General Legal Disclaimer

In addition to limiting liability and disclaiming warranties in their Terms and Conditions, some companies link to a disclaimer from their individual product description pages.

Here's how this can be done on a website, and for certain products:

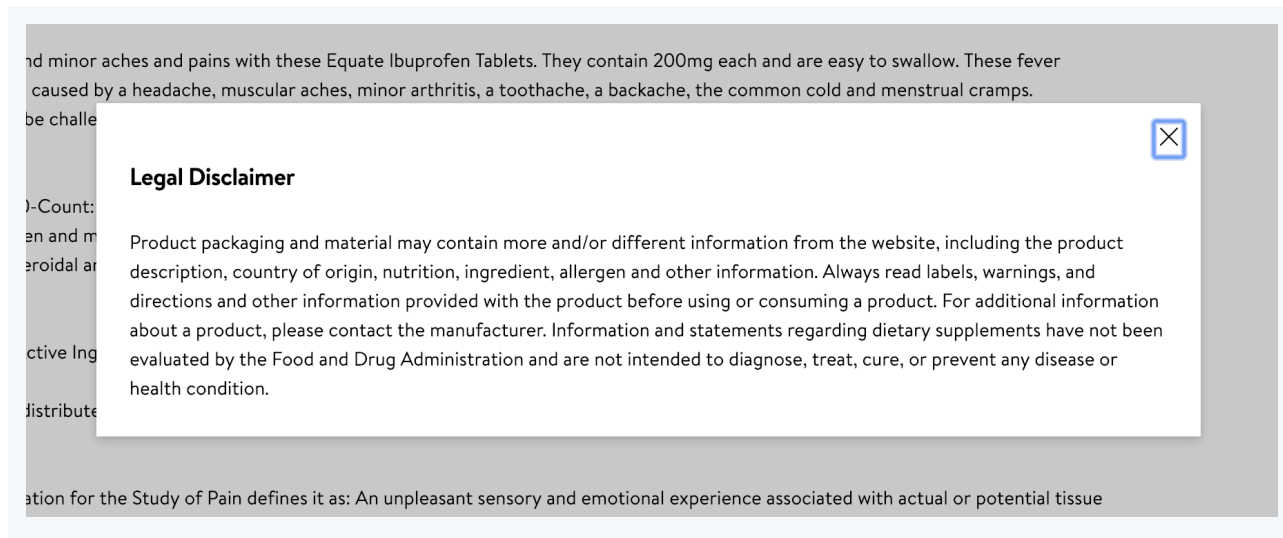


Image: Walmart legal disclaimer

It reads:

Legal Disclaimer

Product packaging and material may contain more and/or different information from the website, including the product description, country of origin, nutrition, ingredient, allergen and other information. Always read labels, warnings, and directions and other information provided with the product before using or consuming a product. For additional information about a product, please contact the manufacturer. Information and statements regarding dietary supplements have not been evaluated by the Food and Drug Administration and are not intended to diagnose, treat, cure, or prevent any disease or health condition.

Potentially Dangerous Goods

If you're selling products that might lead to injury - either because they're generally used for risky activities, or because they are dangerous if misused - it's worth displaying a disclaimer.

Some companies do this in their Terms and Conditions. They might include clauses about:

- How the customer agrees to use or not use a product
- The risks inherent in using products of this sort
- Liability for losses incurred by using a product

Here's how [Powermonkey Fitness](#) does this:

High Risk Activity

Products sold by Powermonkey include equipment and gear used in gymnastics, yoga, fitness, weight training, cross-training, high intensity athletic activity and demonstration. Participation in any of these activities is a high-risk sports activity. You participate in any of these activities at your own risk. You agree to consult with your personal physician before participating in any of these high-risk activities. Read, understand, and follow specific warnings and instructions on products and in product literature or inserts before using the product. Save these documents for reference.

Assumption of the Risk

By buying, using, providing, or allowing the use of Powermonkey's products, you understand and agree that gymnastics, yoga, fitness, weight training, cross-training, high intensity athletic activity and demonstration are high risk activities and, to the extent permitted by law, YOU EXPRESSLY AND VOLUNTARILY ASSUME THE RISK OF DEATH OR OTHER PERSONAL INJURY SUSTAINED WHILE PARTICIPATING IN SUCH ACTIVITIES WHETHER OR NOT CAUSED BY THE NEGLIGENCE OR ANY OTHER FAULT of Powermonkey including but not limited to equipment malfunction from whatever cause, or any other fault of Powermonkey. Additionally, you agree to indemnify, defend and hold Powermonkey harmless from any third party claims arising from such High Risk Activities or any other Powermonkey product.

Image: Powermonkey Fitness Disclaimers for High Risk Activity and Assumption of Risk

The disclaimer states that the customer agrees to consult with their doctor before participating in any of the fitness activities. There's a very strongly-worded exclusion of liability clause. It requires that the customer assumes (takes on) all of the risk associated with using Powermonkey's products and services.

As mentioned in previous chapters, the courts of many jurisdictions may hold that it is not possible for a company to exclude or even limit liability for causing death or personal injury through negligence.

Here's an example of a webpage that offers some guidance on the safe use of pesticides that a company sells:

[Home](#) > Pesticide Safety

Pesticide Safety



The more you know about pesticides, the safer you and your family will be. This safety list is a must-read for anyone thinking about purchasing or using pesticides.

Practicing Pesticide Safety

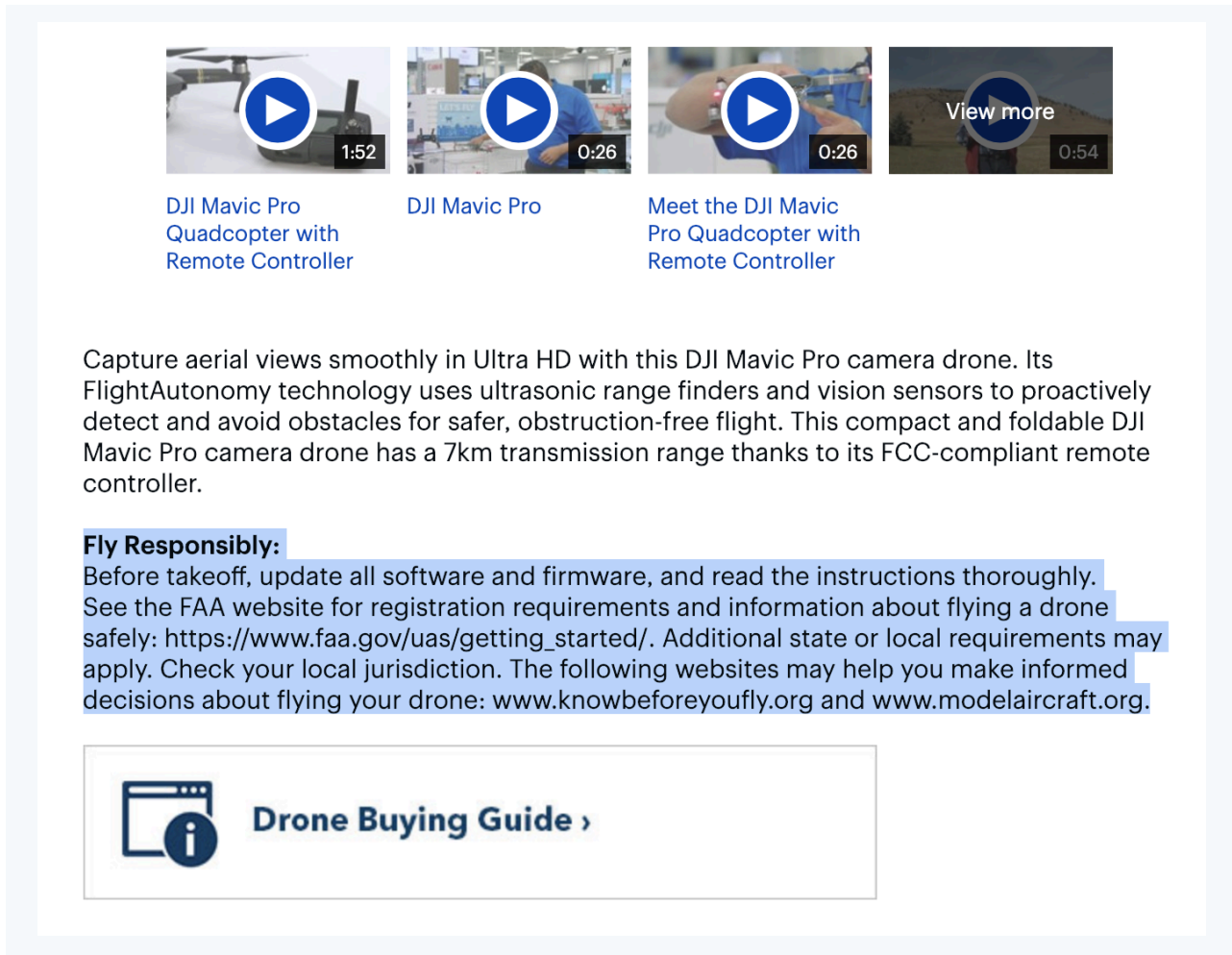
Pesticides are chemical ingredients mixed together that create a substance that kills unwanted animals. While they are very helpful in eliminating rodents from our home, they can also be very dangerous. Whether synthetic or organic in origin, you should treat ALL pesticides with caution. And always read the label carefully, following all of the recommended precautions. Here are some important safety tips when handling pesticides:

Image: Screenshot of Lowes Pesticide Safety information page

Responsible Use Warning

With some goods, there is a risk that the product might be used for illegal or irresponsible purposes, perhaps even inadvertently.

Here's a warning provided by [Best Buy](#) alongside the product description for a camera drone:



Fly Responsibly:
Before takeoff, update all software and firmware, and read the instructions thoroughly. See the FAA website for registration requirements and information about flying a drone safely: https://www.faa.gov/uas/getting_started/. Additional state or local requirements may apply. Check your local jurisdiction. The following websites may help you make informed decisions about flying your drone: www.knowbeforeyoufly.org and www.modelaircraft.org.


 [Drone Buying Guide >](#)

Image: Best Buy drone listing page with Fly Responsibly disclaimer highlighted

California's Proposition 65

California's Safe Drinking Water and Toxic Enforcement [Act](#) (known as Prop 65) requires retailers to give a "*clear and reasonable warning*" when selling products containing certain chemicals. There are over 900 chemicals on the Prop 65 [list](#), some of which are contained in certain foods, drugs, cleaning products, and pesticides.

If you're shipping to California, it's important that you're aware of your obligations under this law. The fines for violating Prop 65 are up to \$2,500 per violation per day.

Businesses with fewer than ten employees are exempt from providing such warnings.

Here's an example of a Prop 65 warning:

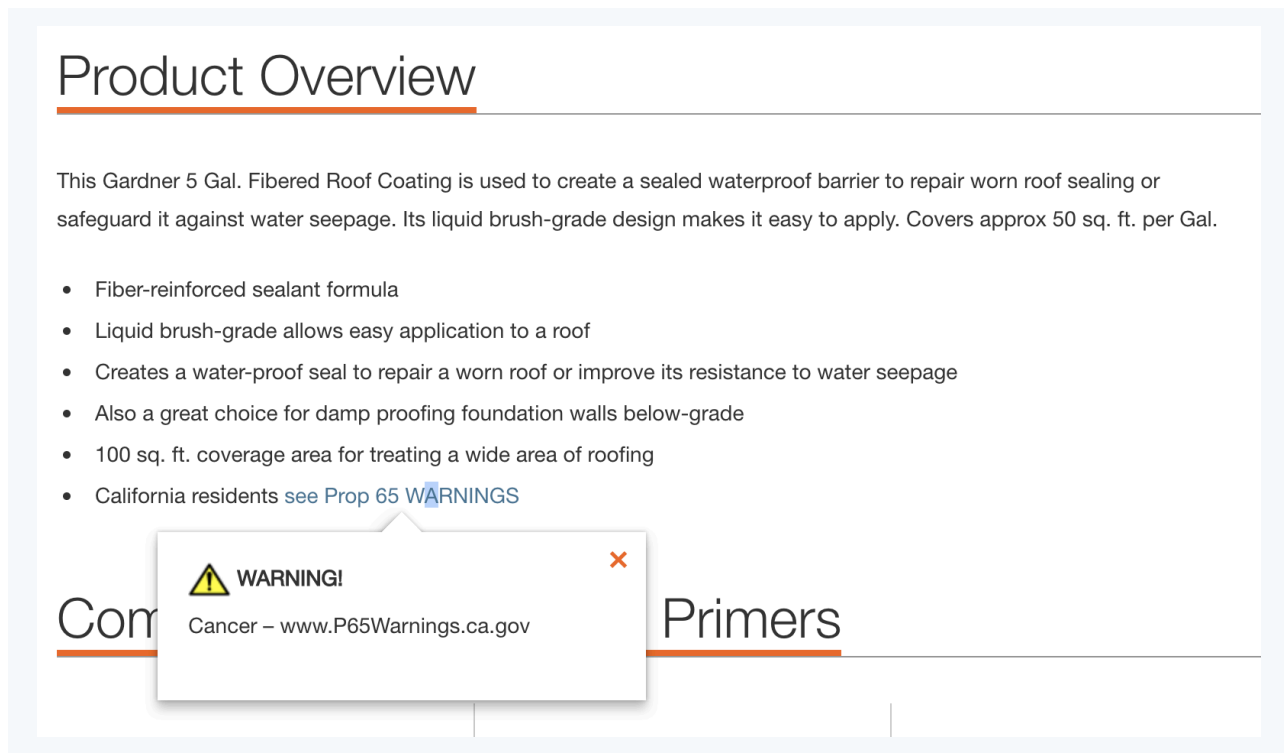


Image: Home Depot Product Overview with Prop 65 popup

California's [Office of Environmental Health Hazard Assessment](#) provides some guidance on how retailers can comply with Prop 65, including that the warning must be written in a font "*no smaller than the largest type size used for other consumer information on the product.*"

The demands on manufacturers and importers under Prop 65 are much higher than on retailers.

Pharmaceuticals and Alternative Medicines

Some medical products are only available through pharmacies. Pharmacists have their own regulations around the information they must provide consumers. Some "alternative" medicines are available from other retailers. These products are often regulated in different ways.

To emphasize the different expectations around pharmaceutical and alternative medicine, we'll look at examples of two types of weight loss pills.

First, here's a weight loss pill that's classed as a pharmaceutical product. [Boots](#) provides the following information about a weight loss product it sells called Hunger Buddy:

Product details

For the treatment and prevention of excess weight. Fight food cravings & cut portion sizes. 94% experienced a feeling of fullness.

40 capsules.

Hunger Buddy is an effective product for management of appetite, food cravings and compulsive eating habits. It is designed to rescue you from hunger pangs and snack attacks. It contains the Redusure™ formula, a unique fibre complex that reduces appetite and provides you with a pleasant feeling of fullness.

Hunger Buddy is clinically proven to promote significant weight loss through a reduced food intake. It is particularly suitable for those who constantly have a big appetite and cannot control portion size. **Hunger Buddy is a certified medical device product for the treatment and prevention of weight and general weight management. Its safety and efficacy are assessed under Medical Device Directive 93/42/EEC.**

Image: Boots Hunger Buddy product details with regulating law highlighted

Here, Boots gives the law under which this product is regulated. This serves both as a disclaimer and a marketing tactic.

Boots then gives a lot of information and warnings about how to take the product, including this:

Hazards and Cautions

Do not take Hunger Buddy during pregnancy or whilst breastfeeding, or if your BMI (Body Mass Index) is below 18.5. It is recommended that you calculate your BMI before and during use.

Hunger Buddy must be taken as a whole capsule with a full glass of water (approximately 250ml). Do not open the capsule and avoid taking it in powder form to avoid choking.

Please consult your healthcare professional before taking Hunger Buddy:

- If you are diabetic, as Hunger Buddy may flatten plasma glucose levels that consequently reduce insulin secretion. Diabetic patients may have to adjust their daily anti-diabetic treatment to avoid hypoglycaemic attacks
- If you are taking any cholesterol-lowering medication
- If you are taking any Angiotensin-converting enzyme (ACE) inhibitors, Angiotensin receptor blockers (ARBs), potassium-sparing diuretics
- If you have renal function impairment, as this product contains a source of potassium
- If you are on a low iodine diet, as this product contains trace amount of iodine
- If any medical condition exists

Image: Boots Hunger Buddy hazards and cautions

Alternative medicines, including alternative weight loss products, still require warnings and disclaimers.

In the U.S., the Federal Trade Commission ([FTC](#)) and Food and Drug Administration (FDA) rigorously enforce the law on advertising such products.

In the UK, the [Advertising Standards Authority](#) (ASA) regulates the alternative medicines market (and all advertising), enforcing laws such as the Consumer Protection from Unfair Trading Regulations and Food Safety [Act](#). The agency has the power to issue fines against companies who breach the law.

When it comes to medical products or supplements, it's far better to make carefully-worded and honest claims than careless overstatements.

“Results Not Typical” Disclaimers

There are strict rules on using “before and after” pictures and “success stories” to promote your product. For example, in the US, FTC’s [Guides](#) Concerning the Use of Endorsements and Testimonials in Advertising, simply including a “results not typical” disclaimer alongside a misleading testimonial is not sufficient to escape liability.

The effect of the new guidance is to require that where an atypical “success story” is used to promote the effectiveness of a product, it must be accompanied by an explanation of the product’s typical effect.

Here’s how the weight loss program [Noom](#) notes that individual results will vary depending on factors like your starting point, personal goals and effort.

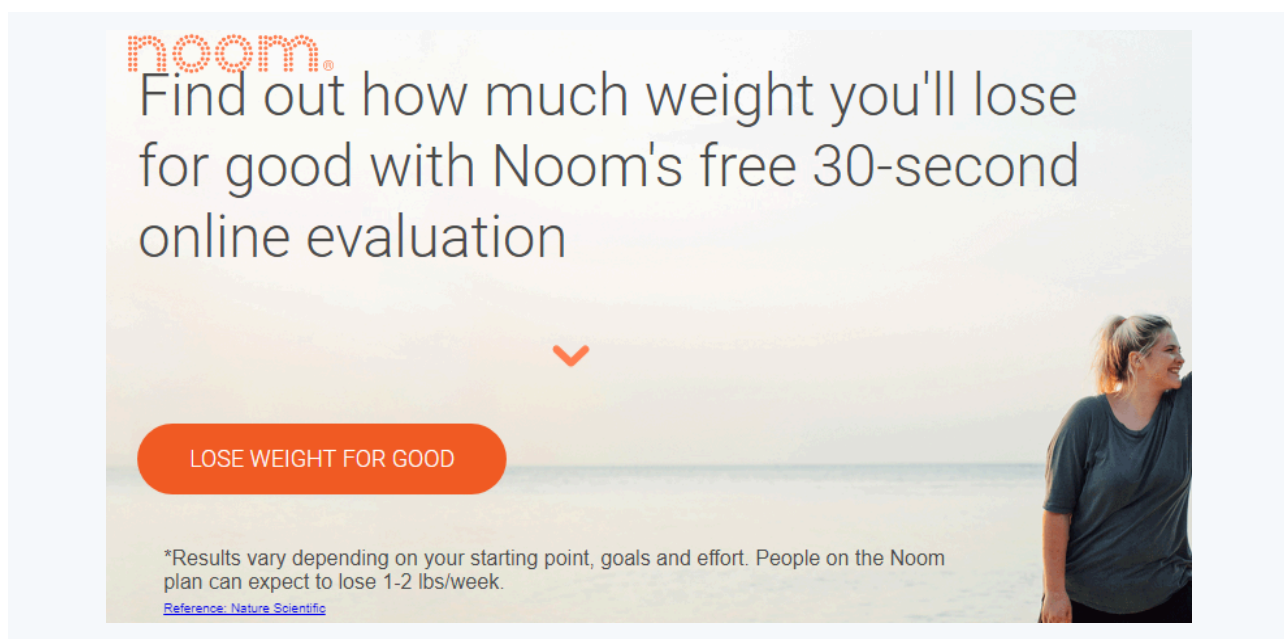


Image: Noom weight loss results disclaimer

Sports Recovery

Some muscle-building supplements carry certain risks when overused, or when combined with other products.

Take a look at this disclaimer that covers a number of the different areas we've looked at so far:

WARNING:

Not for use by individuals under the age of 18 years.

Do not use if pregnant or nursing. Consult a physician before using this product.

Not intended to replace normal food. Watch out when stacking high vitamin or caffeine content supplements.

Contains **185 mg of caffeine** per serving.

Image: Generic supplement warning disclaimer

It reads:

WARNING:

Not for use by individuals under the age of 18 years.

Do not use if pregnant or nursing. Consult a physician before using this product.

Not intended to replace normal food. Watch out when stacking high vitamin or caffeine content supplements.

Contains **185 mg of caffeine** per serving.

Cosmetics

As we've seen, different industries are often regulated by different government agencies and must comply with different laws. There should be no mistaking what kind of product you are selling. It's important that you and your customers are clear on exactly what your products are designed to do.

For example, cosmetics companies make claims about how their products can improve a person's appearance. Sometimes these claims might be mistaken for claims that their products can improve a person's health.

Here's an example of a disclaimer used to distinguish cosmetic products from health products:

DISCLAIMER: Blend & Boost® products described on this website are intended to meet Health Canada's and the FDA's definition of a cosmetic product, an article applied to the human body to cleanse, beautify, promote attractiveness, and alter appearances. These Blend & Boost products are not intended to be drug products that diagnose, treat, cure, or prevent any disease or condition. These products have not been approved and the statements on these pages have not been evaluated by the FDA.

Image: The Compounding Shoppe cosmetics disclaimer

This sort of disclaimer helps manage customer expectations and is also a way to ensure that you aren't falling under the remit of an inappropriate regulatory body. It's another example of how disclaimers can help you avoid accusations of false advertising.

Age-Restricted Items

You might sell some items which are only suitable for adults or people over a certain age.

Here's how [Amazon UK](#) handles this with alcohol products by providing a disclaimer about alcohol not being for sale to people under a certain age:

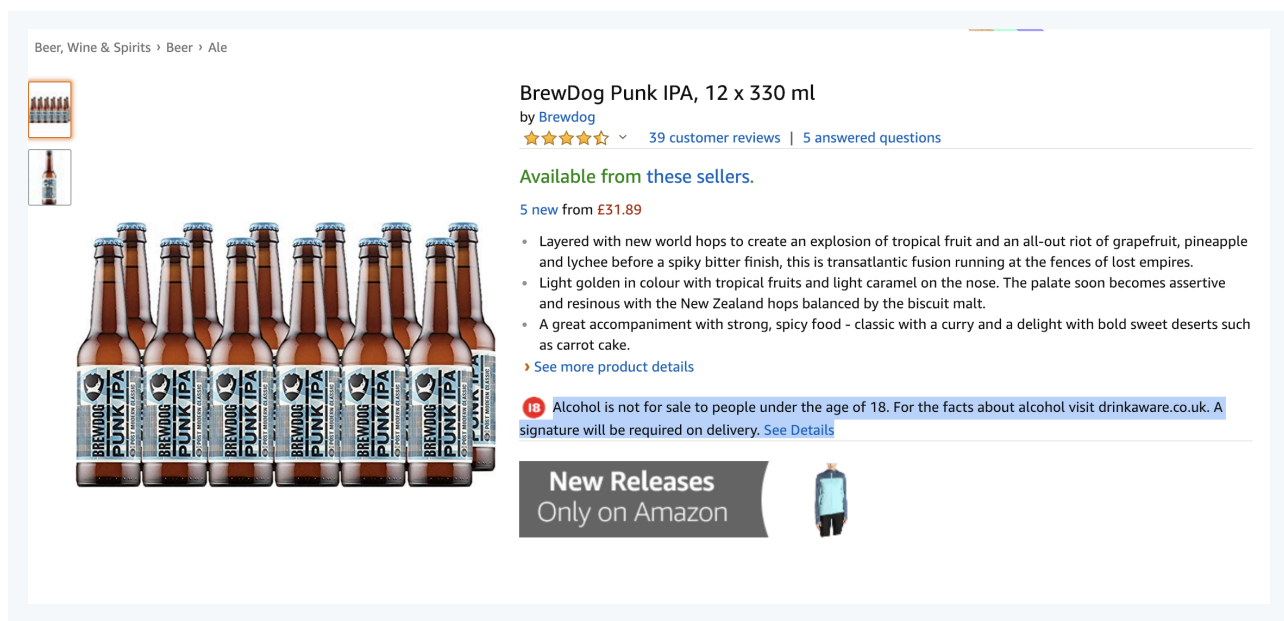


Image: Amazon UK BrewDog Punk IPA product listing with alcohol age disclaimer

You'll notice that Amazon directs its customers to alcohol advice service [Drinkaware](#). This is not a requirement in the UK, but is considered good practice for alcohol producers and retailers.

Of course, you'll have to take further steps to ensure that children aren't buying age-restricted products, such as requiring ID at purchase and/or delivery.

Offers and Promotions

[Promotions and special offers](#) are an essential part of bringing new customers to your ecommerce store. But you must be clear about what you're actually offering people. Misleading offers, such as ones that aren't actually as good as they appear, could damage your reputation and land you in legal trouble.

Here's an example from the UK. An ecommerce business called [Rosee Fine Jewellery](#) was advertising a necklace on Amazon. It advertised the price as follows:

"Price: ~~£129.87~~: Sale: £17.87. You Save: £112.00 (86%)"

The Advertising Standards Authority investigated and could not find any examples of the necklace being sold for more than £25 in the previous 12 months. The offer was obviously misleading. The company was required to remove the ad.

"Money off" promotions need to represent a genuine saving, and any special conditions attached to a promotion must be made conspicuously clear.

Here's how [AT&T](#) explains the conditions attached to an offer:

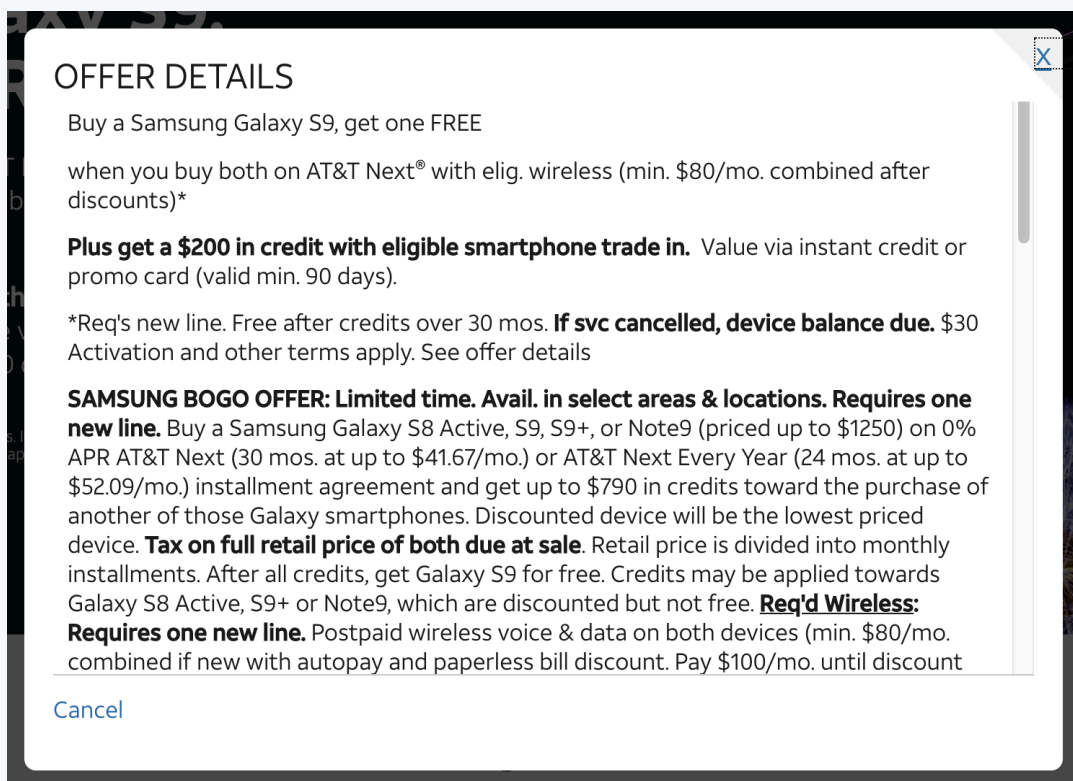


Image: Excerpt of ATT Deals offer details

Restrictions on Normal Service

You also need to be clear where there are restrictions on what your ecommerce store normally offers customers. If your customers have grown to expect a particular service or are subscribing in order to receive certain features, it's important that you let them know about any changes. To put this in context, here's an example of Amazon informing its Prime customers about an exception to its usual one-day delivery option:

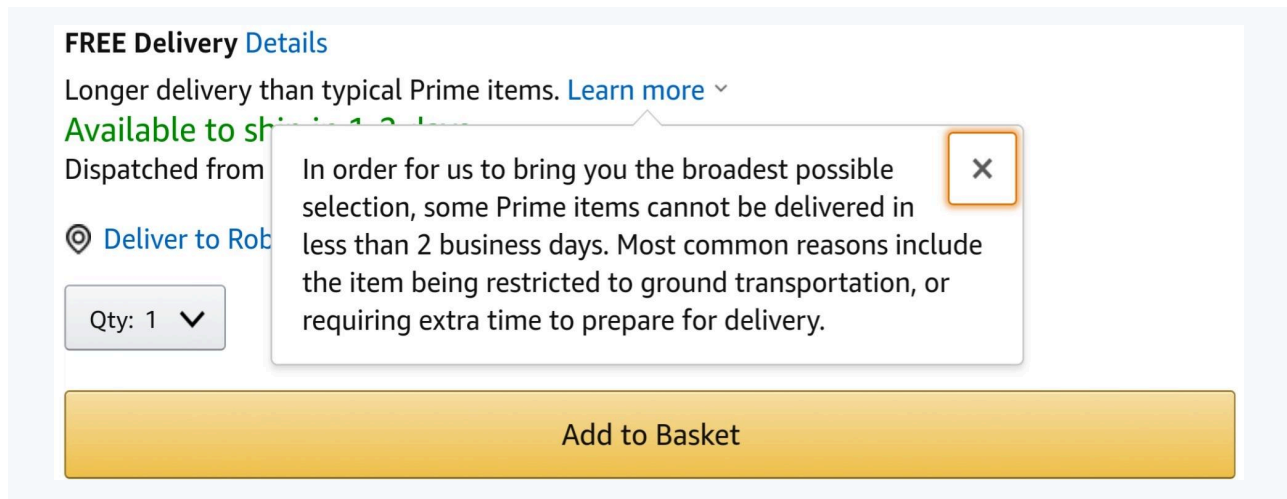


Image: Amazon UK Prime delivery exceptions and restrictions notice

Affiliate Link Disclaimers

If you engage in [affiliate marketing](#), the FTC in the U.S. requires you to include a disclaimer about this. The disclaimer can be short and simply, as long as it discloses that you will earn a commission or some sort of material compensation when someone makes a purchase via your affiliate link.

Many ecommerce stores that have a blog component will engage in affiliate marketing and promote different affiliate products through blog articles. But this isn't the only time you'll see these links.

Here's an example of a short and sweet affiliate disclaimer at the top of a blog entry that will link to products for sale:

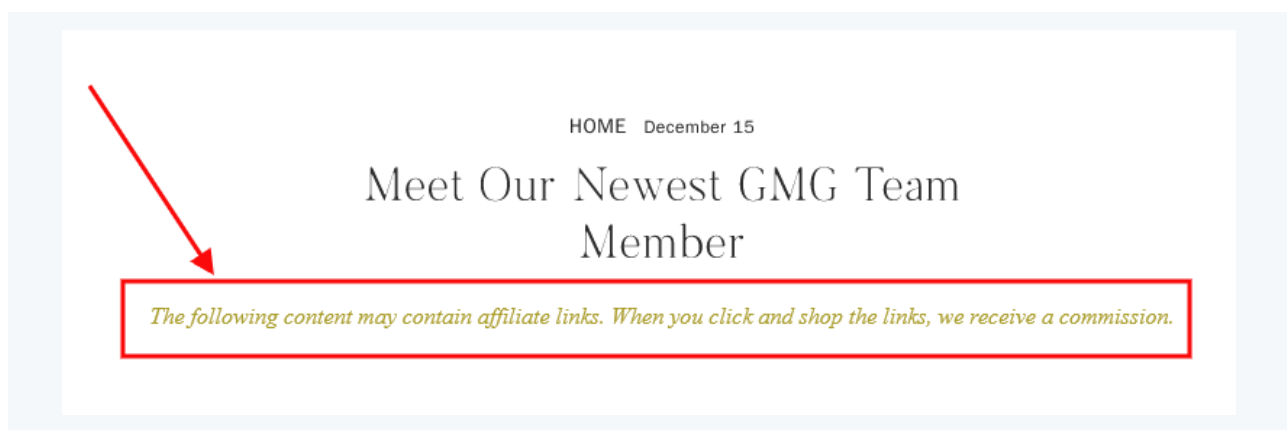


Image: Julia Berolzheimer blog affiliate disclaimer highlighted

Your affiliate disclaimer can also be much longer and more detailed, such as it is here:

Hi. Pat Flynn here. I've always believed in transparency on the web and so I am disclosing that I've included certain products and links to those products on this site that SPI Media LLC will earn an affiliate commission for any purchases you make. My goal with the blog is to help educate you on the possibilities that exist for a blogger in practically any field, but please understand I am doing this as a for-profit business and, frankly, so should you with your site unless you have some charitable endeavor in mind.

The site has grown so big at this point that it is nearly impossible to go back through and list each and every program that I have an affiliate agreement with. Given this, you should assume that any links leading you to products or services are affiliate links that SPI Media LLC will receive compensation from just to be safe. Having said that, there are millions of products and services on the web that relate to blogging and making money online. I only promote those products or services that I have investigated and truly feel deliver value to you. Examples would include the banners for Buzzsprout, Teachable, and Circle. I'm also an affiliate and advisor for companies such as

Image: Pat Flynn Affiliate Disclaimer excerpt

The best approach is to have a short disclaimer as in the first example and place it close to the affiliate links themselves, and also have a longer disclaimer as in the second example as well. The shorter one can even link to the longer one.

Here's an example of combining both styles. This statement would go at the beginning of a post:



Image: Generic affiliate links link screenshot

Results Not Typical Disclaimers

If your ecommerce store sells any product or service that the public can perceive as **promising certain results**, you can protect yourself from legal liability by including a “results not typical” disclaimer. This is also known as a “**results may vary**” disclaimer.

This disclaimer will make it clear to shoppers that their own results may differ from the results of others, and that you make no promise that individual results will be consistent. For example, if you

sell weight loss products, this type of disclaimer helps ensure that people can't hold you accountable if they take your product and still don't lose any weight, or only lose a small amount of it.

Here's an example in action:



Image: Ad disclaimer from Jenny Craig: Results not typical

Consider if any of your products or services could benefit from having this type of disclaimer.

Where to Display Your Disclaimers

You should make sure your customers see any disclaimers before they buy your products. It's no longer common or acceptable practice for business to add disclaimers in the "small print." You need to be clear and transparent or you run the risk of your disclaimers failing to take legal effect.

Where you're selling goods that carry a particular risk, make that risk clear to your customers in your product description.

Here's an example of this:

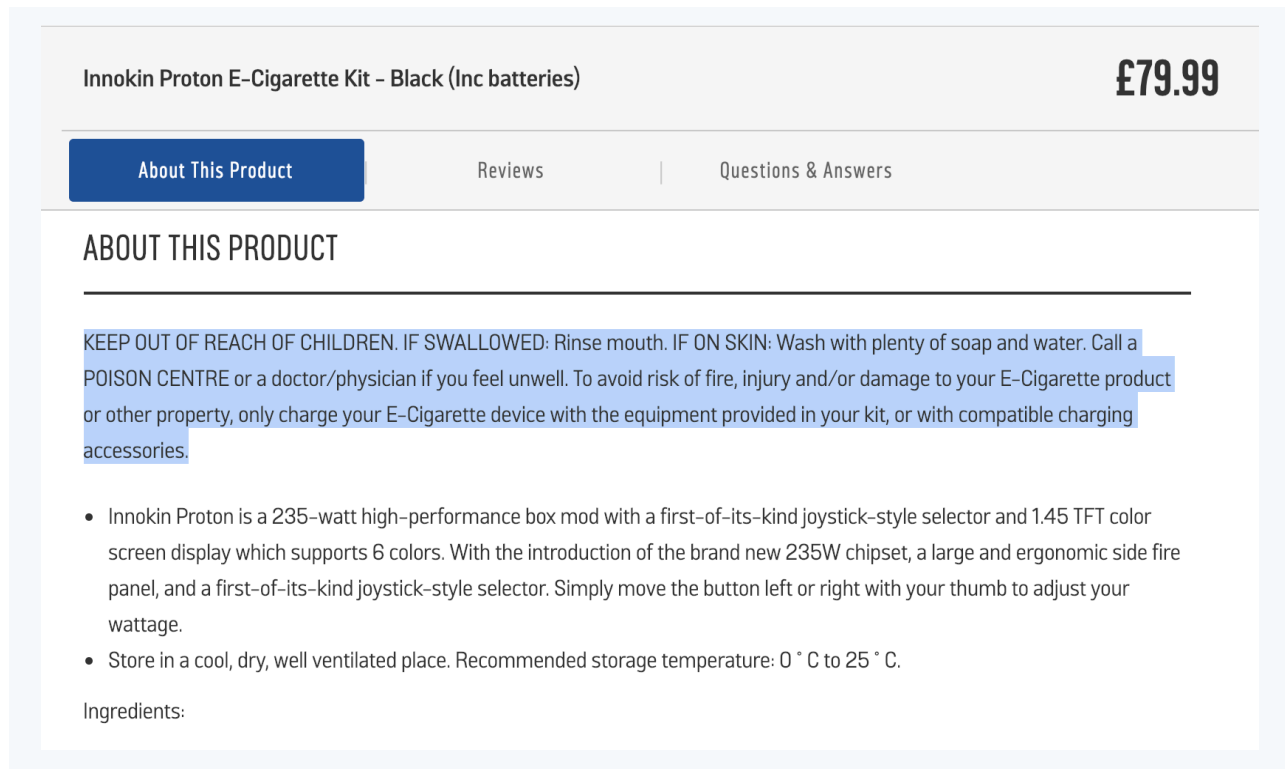


Image: Argos About This Product with disclaimer for children highlighted

And here's a legal disclaimer that Amazon displays on its mobile app under the product description of all medical products and supplements:

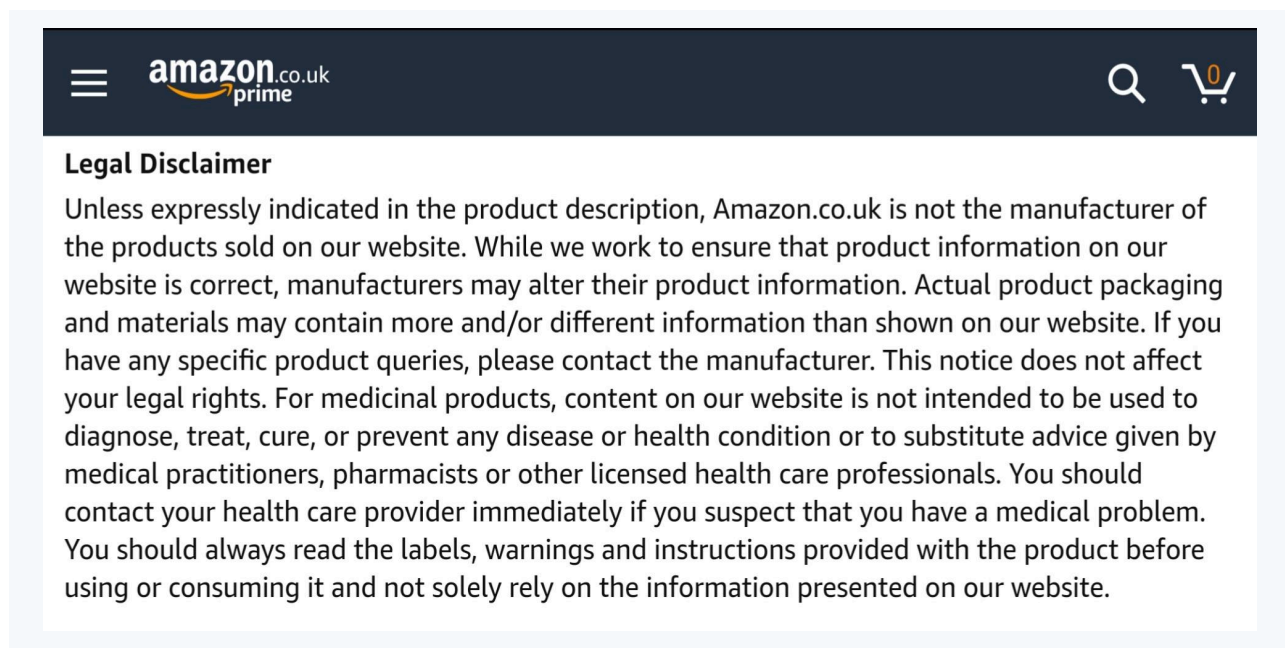


Image: Amazon UK app: medical products and supplements legal disclaimer

Here's how [Verizon](#) provides a disclaimer for one of its promotions. First, the customer sees the "headline" promotion with some basic information about the deal:

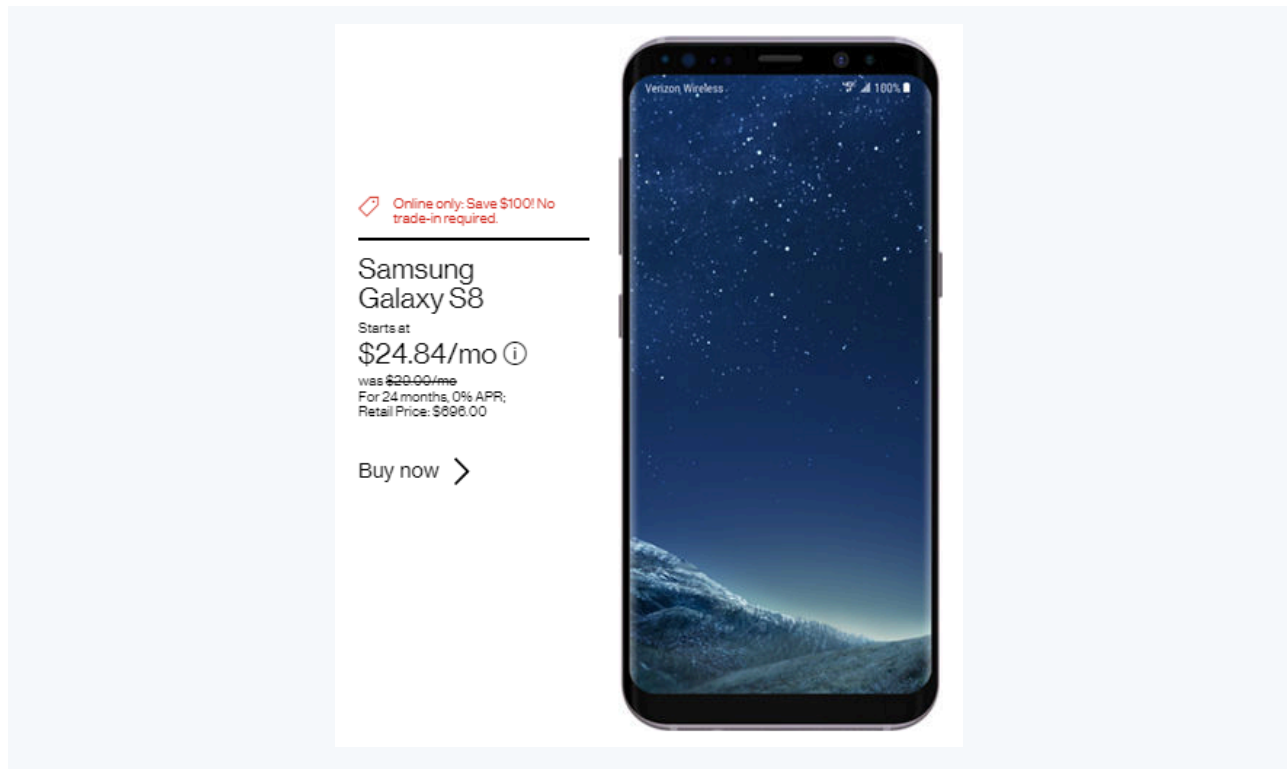


Image: Verizon deal: Samsung Galaxy advertisement

The small circled "i" lets the shopper know that there is additional important information about the deal. Hovering over it reveals the disclaimer and additional information:

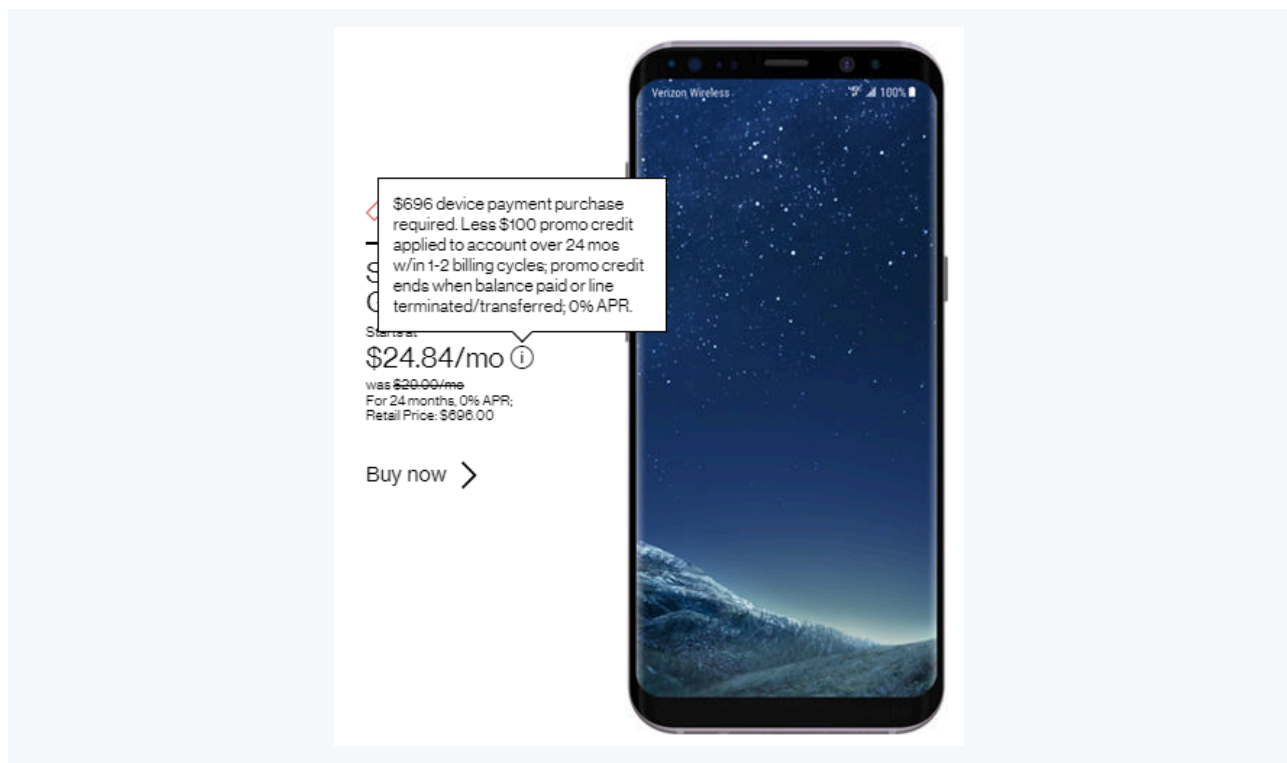


Image: Verizon deal: Samsung Galaxy advertisement with information disclaimer

Case Study

Happiness Herbs is an ecommerce store based in the U.S. that sells essential oils, cosmetics and aromatherapy goods. Its products are not regulated as pharmaceutical products. It ships to the U.S. and Canada.

Happiness Herbs should:

- Display a general legal disclaimer that sets out the risks associated with using its products
- Disclose any potentially dangerous ingredients in its products, particularly if they are covered by California's Prop 65 law
- Be careful about any claims it makes about the effectiveness of its products:
 - When citing any customers' testimonials or "success stories," Henry's Herbs must be careful to explain that the results are not typical, and cite the source for any claims
 - Henry's Herbs must be clear that its products are not medical products and not intended to improve the health of its customers
- Display warnings about how to safely use its products, including:
 - Advising its customers to consult with their doctor where necessary
 - Making note of any age restrictions
 - Disclosing any health considerations that might be relevant to using these products
- Ensure any discounts are genuine savings based on the actual normal price of the product

Chapter 7:

Email Marketing and Ecommerce Businesses

Despite the rise of social media advertising, email marketing remains the primary way for many businesses to promote their products, bring in new customers, and ensure customer loyalty.

In some ways, successful email marketing campaigns have never been easier:

- Customers are making more of their personal information and preferences available online
- Technology allows you to accurately measure the impact of your campaigns
- Third-party direct email marketing services are available to help businesses target their customers in the most effective way

But there are a lot of new challenges, too:

- Email spam filters are increasingly vigilant
- Customers have access to tools which allow them to instantly unsubscribe from email lists en masse
- Privacy and data protection laws are imposing ever-stricter requirements and restrictions on businesses

The importance of that last point can hardly be overstated. Failing to comply with the [laws around email marketing](#) could have disastrous consequences for your business, resulting in fines, litigation, and severe reputational damage.

Laws on Email Marketing

In [Chapter 3](#), we looked at how important it is for your ecommerce store to maintain a Privacy Policy. We're now going to look at the effect privacy law has on your email marketing campaigns.

Remember that you aren't necessarily only affected by the laws of the country in which your ecommerce store is based. You should get to know the laws of your customers' countries, too.

[Privacy laws](#) very often have an extra-territorial scope. This means that the law will be enforced even against foreign businesses if they do business within the country where the law is enacted.

United States



Image: United States Flag

Although there is no general privacy law in the United States at the federal level, there is a national law that regulates the sending of email marketing.

The [Controlling the Assault of Non-Solicited Pornography and Marketing](#) (CAN-SPAM) Act was introduced in 2003, and surely ranks among America's more misleading legislative puns. "Can" is supposed to mean "stop."

CAN-SPAM doesn't "can" unsolicited email altogether. You can still send marketing emails to a person without their consent under this law. But the Act sets out several requirements for the sending of marketing emails.

It provides three broad requirements for marketing emails:

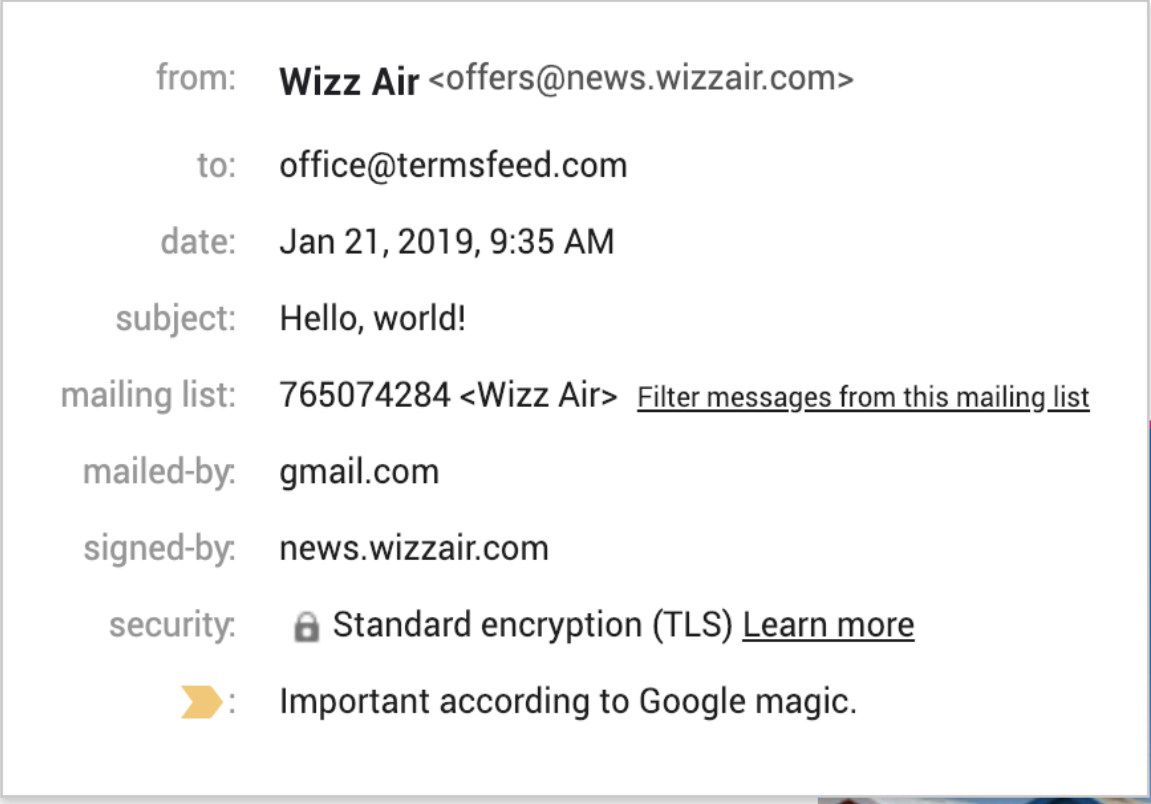
1. Be clear about who is sending the email
2. Be honest about your reasons for sending it, and
3. Make it easy to unsubscribe from future marketing emails

At the Top of Your Email

CAN-SPAM requires that your emails have accurate headers and subject lines.

The header is the part of the email that tells the recipient who the email is to, and who it is from. CAN-SPAM requires that the "from" line "*accurately identifies any person who initiated the message.*"

Here's a compliant example:





from: **Wizz Air** <offers@news.wizzair.com>
to: office@termsfeed.com
date: Jan 21, 2019, 9:35 AM
subject: Hello, world!
mailing list: 765074284 <Wizz Air> [Filter messages from this mailing list](#)
mailed-by: gmail.com
signed-by: news.wizzair.com
security:  Standard encryption (TLS) [Learn more](#)
 Important according to Google magic.

Image: Screenshot of Wizz Air email header

The “from” field shows that the email was sent from a domain associated with the business, as expected. Note that the definition of “person” isn’t limited to an individual, and can mean a business.

CAN-SPAM requires you to be honest in your subject lines. Rather than forbidding particular phrases or giving examples, the Act states that the sender must not use subject lines that: *“would be likely to mislead a recipient, acting reasonably under the circumstances, about a material fact regarding the contents or subject matter of the message.”*

At the Bottom of Your Email

CAN-SPAM requires your marketing emails to:

- Give a **physical address** for your business
- Let the recipient know that they are receiving a **marketing email** (*unless* they have consented), and
- Offer the recipient the **opportunity to unsubscribe**

Here’s a footer from a marketing email that covers all three bases:

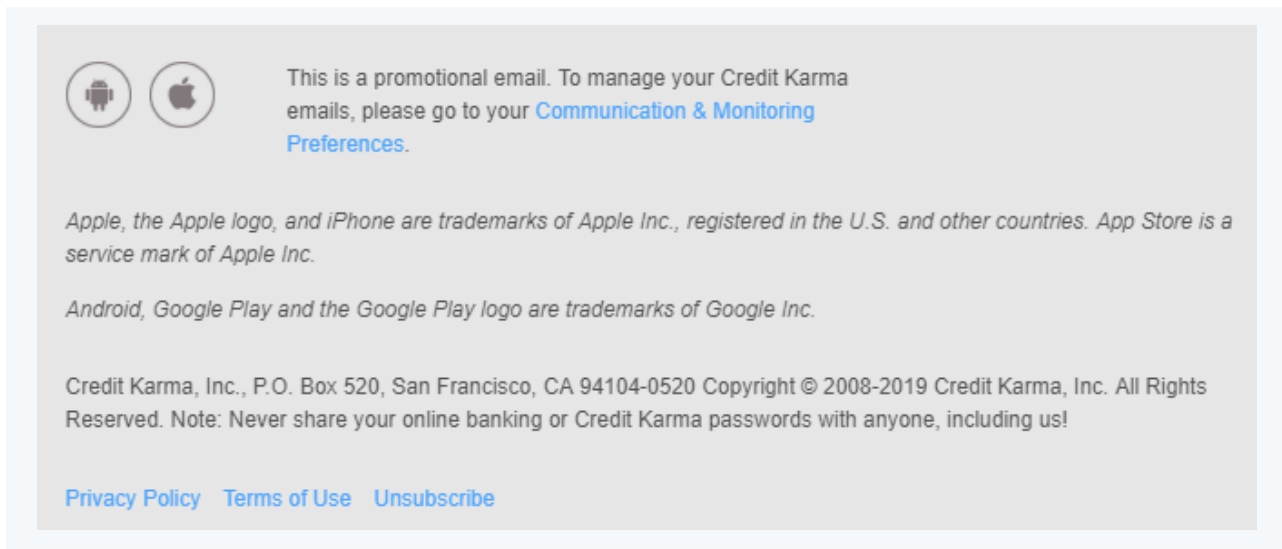


Image: Screenshot of Credit Karma email footer

Credit Karma provides its postal address. This is to comply with the requirement in CAN-SPAM that the marketing emails contain *"a valid physical postal address of the sender."*

The recipient is told that the email is a promotional email.

Credit Karma provides an unsubscribe link. This is to comply with the requirement that the sender provides *"clear and conspicuous notice of the opportunity [...] to decline to receive further commercial electronic mail messages from the sender."*

A recipient must be able to unsubscribe by sending one reply to your email, or via a link that takes them to one webpage. It mustn't be any more complicated than that. Unsubscribe requests must be honored within 10 working days.

Canada



Image: Canada Flag

Canada's Fighting Internet and Wireless Spam Act, known as [Canada's Anti-Spam Act](#) (CASL), came into effect in 2014.

CASL applies to you if you're planning on sending any marketing email to anyone in Canada, whether your business is based in Canada or not.

One of the most important sections of CASL states that it's illegal to send a marketing email to someone unless you have their consent to do so. There are **two broad types of consent** under CASL.

Implied Consent

CASL allows you to earn consent without explicitly asking for it. It's possible to argue that you have a person's implied consent if:

1. **You share an active business relationship.** This might mean that the person has made a purchase from you within the past two years, or expressed an interest in your products in the past six months.
2. **You share an active non-business relationship.** This applies in a similar way to type 1 but to clubs, charities and other nonprofits. The "purchase" in this scenario might refer to a donation.
3. **The person's email address was publicly available or disclosed to you.** In this case, you can only send marketing emails that are related to that person's business or interests. You can't send the person marketing material if they've made it clear that they don't want to receive it. For example, if they've published their email address on their website with an accompanying message, such as "no spam please."

You must be able to prove that you have implied consent on these terms.

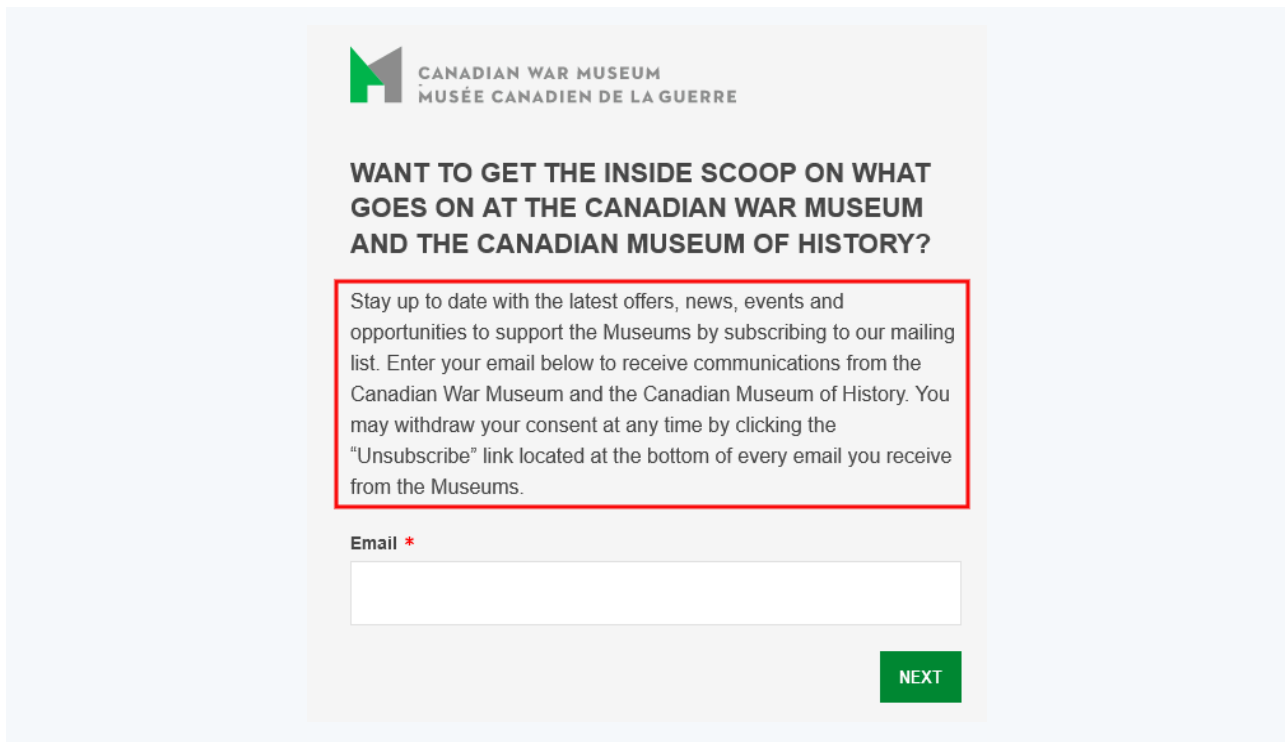
There was a three-year transition period which ended on 1 July 2017. Before this date, businesses could rely on implied consent formed from existing relationships formed before CASL passed in 2014. Now that the transition period is over, the two-year time limit applies to implied consent arising from existing business relationships.

Express Consent

If you don't have implied consent, you can ask for consent. This is called express or explicit consent. For a request for consent to be valid, it must include:

1. The reason you're asking for consent. For example "please give us your email address so we can send you information on our products."
2. The identity of your company

Here's an example from the [Canadian War Museum](#):

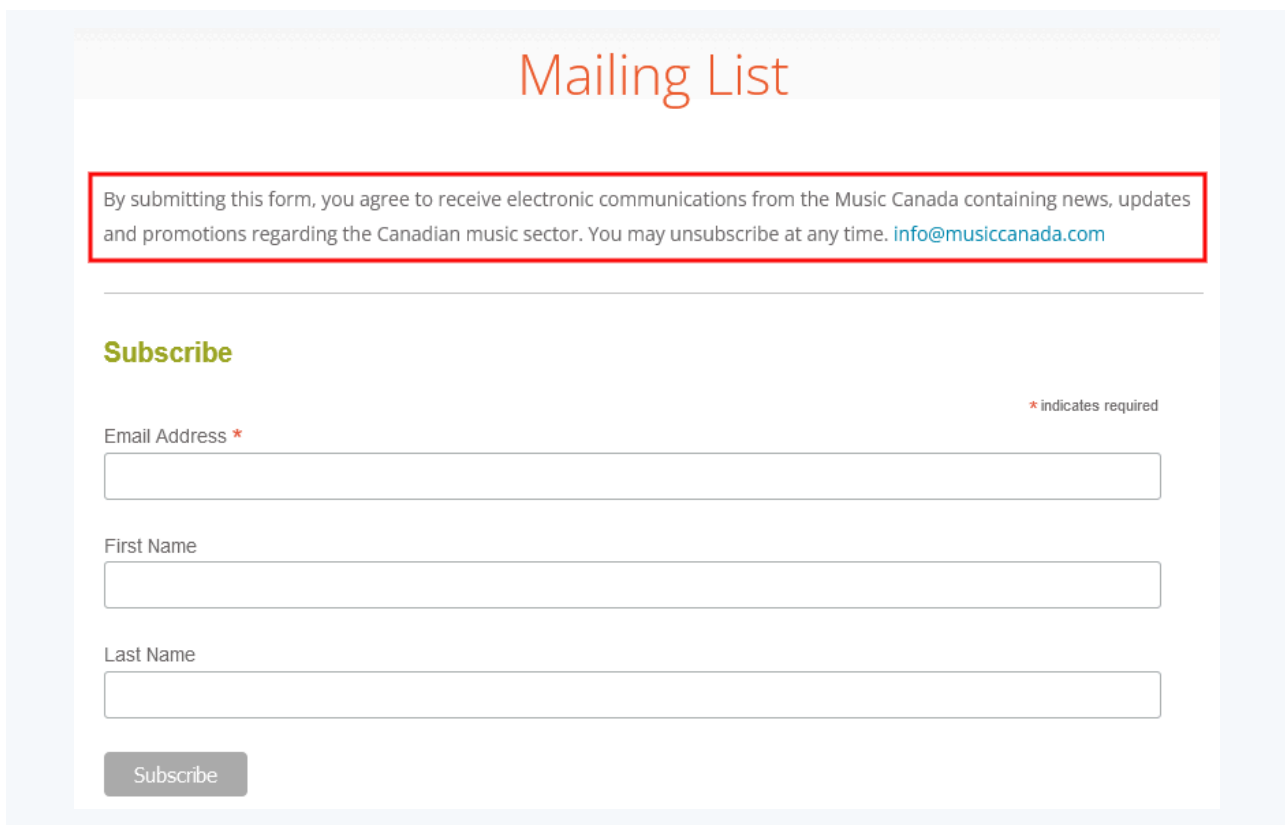


The image shows a web form for the Canadian War Museum. At the top is the museum's logo and name in English and French. Below this is a heading: "WANT TO GET THE INSIDE SCOOP ON WHAT GOES ON AT THE CANADIAN WAR MUSEUM AND THE CANADIAN MUSEUM OF HISTORY?". A red-bordered box contains the following text: "Stay up to date with the latest offers, news, events and opportunities to support the Museums by subscribing to our mailing list. Enter your email below to receive communications from the Canadian War Museum and the Canadian Museum of History. You may withdraw your consent at any time by clicking the 'Unsubscribe' link located at the bottom of every email you receive from the Museums." Below the text is a text input field labeled "Email *" and a green button labeled "NEXT".

Image: Canadian War Museum email subscribe form

The Canadian War Museum provides very comprehensive information about its organization and the purposes of joining its mailing list.

Here's another example of a valid express consent request from [Music Canada](#):



The image shows a web form titled "Mailing List" for Music Canada. A red-bordered box contains the following text: "By submitting this form, you agree to receive electronic communications from the Music Canada containing news, updates and promotions regarding the Canadian music sector. You may unsubscribe at any time. info@musiccanada.com". Below the text is a section titled "Subscribe" in green. To the right of this section is a note: "* indicates required". There are three text input fields: "Email Address *", "First Name", and "Last Name". At the bottom is a grey button labeled "Subscribe".

Image: Music Canada email subscribe form

Compliant Emails

Even when you have a person's consent under CASL, there are certain rules about the content of your marketing emails. These requirements are broadly similar to those made by CAN-SPAM.

You must include:

- Clear information about who you are and how you can be contacted
- An unsubscribe mechanism. This must allow the recipient to unsubscribe by reply email, or by visiting a web page. The reply email address or web page link must be valid for at least 60 days. Unsubscribe requests must be honored within 10 working days.

Australia



Image: Australia Flag

The Spam Act [2003](#) regulates marketing emails sent to and from people in Australia. The Act is quite similar in its effects and language to CASL. It also effectively bans the use of email-harvesting software in Australia.

Australian Link

The Spam Act refers to marketing emails with an “Australian link.” This includes any emails that are sent from Australia or might reasonably be expected to be opened in Australia.

There is some scope for a business to argue that it did not expect its marketing email to be opened in Australia. But to be safe, it's better to take a few steps to comply with the Act than to risk violating it.

The Spam Act is quite clear that it generally applies “extraterritorially” - outside of Australia.

The Spam Act bans unsolicited marketing email. Sending “unsolicited” emails effectively means sending emails without consent. The Spam Act recognizes two types of consent: inferred and express consent.

Inferred Consent

You can infer that you have consent to email a person if:

1. You have an existing business relationship with the person. There is little guidance in the Act about what constitutes an existing business relationship. The Australian Communications and Media Authority ([ACMA](#)) suggests it would be a relationship where *“there is a reasonable expectation of receiving commercial electronic messages.”*
2. The person has conspicuously and publicly published their email address. This doesn't apply if the person has stated that they don't wish to receive marketing emails. The emails you send must be relevant to their industry or profession.

This is very similar to the model of implied consent we looked at under CASL.

Express Consent

Express consent means that the person has actively agreed to receive marketing emails from you. Again, the Act is a little thin on the details here. But the ACMA provides the following advice:

- **A double opt-in is good practice.** For example, once your customer has subscribed to your marketing newsletter, send an initial welcome email to ask them to confirm their subscription.
- **You cannot use a pre-ticked box** to gain consent
- **Silence** (e.g. not unsubscribing) doesn't constitute consent

Compliant Emails

The requirements around the content of marketing emails under the Spam Act 2003 are very similar to those under CAN-SPAM and CASL.

1. **The sender must be clearly identified.** The information must include the name of the person or company sending the email, and their Australian Business Number (if applicable). If you're having a third party send emails on your behalf, they must identify your company as the originator of the email.
2. **Include information about how the recipient can contact you.** This can simply be a matter of replying to the email, depending on what's in the “From” field.
3. **Always include an unsubscribe facility, in every email.**

All this information must be valid for at least 30 days. Unsubscribe requests must be honored within 5 working days.

European Union



Image: Flag of EU

The EU has the strictest privacy laws around. There's no EU-wide law specifically related to the regulation of spam, but a patchwork of rules can be inferred from laws such as the [ePrivacy Directive](#) and the [GDPR](#). Each EU country will implement these rules in a slightly different way, but there is an accepted minimum set of standards that they must adhere to.

There is a lot to be done in order to comply with the GDPR. Much of this has to do with creating a Privacy Policy, which we covered in Chapter 3. When it comes to sending marketing emails, the main thing to remember is that when the EU says “consent,” it really means it.

Again, if you're seeking EU customers, you'll need to comply with the EU's privacy laws even if you aren't based in the EU.

Affirmative Consent

One of the myths of the GDPR is that processing someone's personal information *always* requires consent. This is not true. If you wish to process someone's personal data (this includes sending them marketing emails), you won't have to ask for consent in *every* case. This *even* applies to email marketing [in some circumstances](#).

But in many contexts, consent will be the way to go, especially if you're hoping to gain new customers with your email marketing campaign.

Canada and Australia's anti-spam laws say that they require consent, but this includes “implied” or “inferred” consent. The GDPR doesn't recognise this type of consent. Consent must be freely given, via a clear, affirmative action.

Always “opt-in,” never “opt-out.”

Here's a bad (and since updated) example from [Walmart](#). When creating an account, the customer is presented with a pre-ticked box which allows Walmart to send them marketing information:

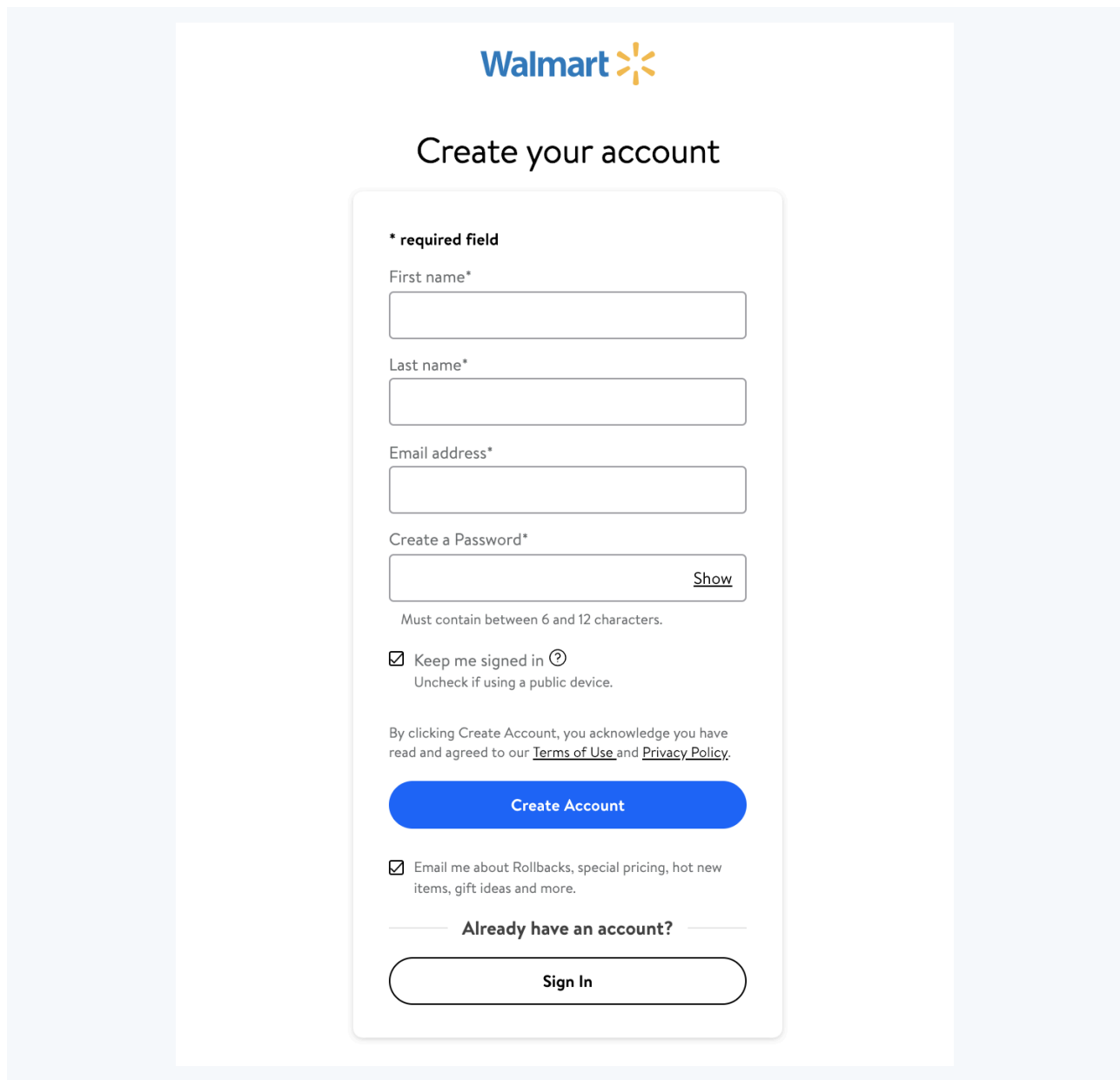
The image shows a screenshot of the Walmart account creation page. At the top is the Walmart logo. Below it is the heading "Create your account". The form is enclosed in a light gray border. It starts with a "* required field" label. The fields are: "First name*", "Last name*", "Email address*", and "Create a Password*". The password field has a "Show" link on the right. Below the password field is a note: "Must contain between 6 and 12 characters." There is a checkbox labeled "Keep me signed in" with a help icon and a note "Uncheck if using a public device." Below this is a paragraph: "By clicking Create Account, you acknowledge you have read and agreed to our [Terms of Use](#) and [Privacy Policy](#)." This is followed by a large blue "Create Account" button. Below the button is another checkbox labeled "Email me about Rollbacks, special pricing, hot new items, gift ideas and more." which is pre-checked. At the bottom, there is a link "Already have an account?" and a "Sign In" button.

Image: Walmart account sign-up form with pre-checked email consent box

The customer can't be said to have given clear, affirmative consent here. They're clicking a button that says "Create Account," and they might not even realize that they're also signing up to marketing emails. You shouldn't "piggyback" consent for marketing in this way.

Granular Consent

Getting consent for one type of communication doesn't mean you have consent for all types of communication. You should break down your consent requests so that your customers know exactly what they're agreeing to and are presented with choices and options.

Let's take a look at an example from [Logitech](#):

Privacy Policy'. At the bottom is a blue 'REGISTER' button and a link 'ALREADY REGISTERED? [SIGN IN >](#)'." data-bbox="93 117 900 419"/>

Image: Logitech account registration page with consent checkbox for communications

Logitech is using one consent statement to ask its customers to consent to receive several different types of communication here.

Ideally this would be broken down so that the customer could, for example, consent to receiving the Logitech newsletter, but decline to receive information about “exclusive offers.”

Here's an example of how something like this could look, with multiple options and opportunities to give consent:

privacy policy'." data-bbox="93 610 900 899"/>

Image: Time to Change email updates preferences checkboxes to get granular consent

Compliant Emails

It almost goes without saying that it should be easy for your EU users to unsubscribe. Even the least demanding of the spam laws we've looked at, CAN-SPAM, requires this.

The guiding principle comes from [Article 7](#) of the GDPR, which states that "*it shall be as easy to withdraw as to give consent*." Including a facility in your marketing emails that will allow a customer to withdraw by visiting a single webpage should satisfy this requirement.

You should also **link to your Privacy Policy in the footer of all automated emails**.

Laws Across the EU

EU law is implemented slightly differently in different EU countries, with laws setting a minimum level of protection. The GDPR demands clear consent. Some individual countries lay further protections on top of this, or make small changes as permitted under the GDPR's exemptions.

Other Major Economies

Email marketing laws vary significantly around the world. Generally speaking the strictest are found in Europe. Here are the laws of some other major economies.

Argentina

The Personal Data Protection [Act](#) and Regulatory [Decree 1558/01](#) regulate marketing emails. There has also been data protection [reform](#) in 2023.

Allows opt-outs and recognizes implied consent.

The subject line of a marketing email [must read "advertisement"](#) and nothing else.

Brazil

There is effectively no anti-spam law in Brazil.

The [Civil Rights Framework for the Internet](#) ("Marco Civil") provides the right for individuals to request deletion of personal information but does not mention spam specifically.

The [Self-Regulation Code for E-mail Marketing](#)

[Practices](#) is a voluntary code for email marketers in Brazil.

The Brazilian Data Protection Law ([LGPD](#)), known as “Brazil’s GDPR” went into force in 2020.

China

The [Regulations On Internet Email Services](#) cover marketing emails. Broader internet censorship laws are also relevant.

Marketing emails must contain the word “Ad” (or the Chinese equivalent) in the subject line. Explicit consent is required.

Hong Kong

Under the Unsolicited Electronic Messages [Ordinance](#), marketing emails must contain:

- Accurate sender information
- An unsubscribe facility
- Honest subject lines

Unsubscribe requests must be honored within 10 working days.

Indonesia

Marketing emails are not regulated by law in Indonesia.

[Law 11 Concerning Electronic Information and Transactions](#) covers internet privacy.

Israel

The [Communications Law \(Telecommunications and Broadcasting\) 1982](#) was amended in 2008 to include some provisions about email marketing.

The law recognizes informed “opt-out” consent where a customer provides their email address at the point of a previous sale. The marketing material must be connected to the type of product sold. Consent can be easily withdrawn.

Marketing emails must contain:

- The word “Advertisement” in the subject line
- The contact details of the business
- An unsubscribe facility

Japan

The [Act on Regulation of the Transmission of Specified Electronic Mail](#) requires businesses

	to gain express, opt-in consent before sending marketing emails, and to keep records that can prove that they have done this.
Malaysia	The Communications and Multimedia Act (1998) forbids “ <i>intent to annoy, abuse, threaten or harass</i> ” via email.
New Zealand	<p>The Unsolicited Electronic Messages Act 2007 recognizes express, inferred and “deemed” consent (implied consent via conspicuous publication of an email address).</p> <p>Marketing emails must contain: the contact details of the business and details of how to unsubscribe. Unsubscribe requests must be honored within five working days.</p>
Singapore	<p>The Spam Control Act regulates marketing emails with a “Singapore link” (this language can also be seen in Australia’s Spam Act 2003).</p> <p>Marketing emails must begin with the characters <ADV>, and not contain misleading headers or subject lines. They must contain an unsubscribe facility.</p>
Switzerland	<p>Marketing email is regulated by the Federal Law against Unfair Competition 2007 and Telecommunications Act. The law is very strictly enforced and only recognizes express consent.</p> <p>Businesses must state a clear legal basis for sending marketing emails. Marketing emails must be clearly identified as such, and contain accurate sending information and an unsubscribe facility.</p>
South Africa	<p>The Electronic Communications and Transactions Act 2002 allows marketing email to be sent on an opt-out basis.</p> <p>The Protection of Personal Information (POPI) Act 2013, a privacy law very similar to the GDPR, has been gradually coming into force but has yet to take full effect. Email marketing rules will be much stricter once it has.</p>

Table 2. Email marketing laws of some other major economies

Case Study

Plastic Pipes is a plumbing company based in the UK. It ships all over the EU. It is compiling a mailing list of existing customers and website sign-ups. It plans to distribute a weekly newsletter and regular promotional emails.

Plastic Pipes needs to do the following:

- Ensure customers are **actively consenting** to receiving marketing email:
 - Via a form on its website
 - Via a unticked consent boxes when making a purchase
- Give customers an honest representation of what they'll be receiving, and **offer a choice** over which sorts of marketing correspondence they receive, for example:
 - *"Tick here if you would like to receive marketing materials and information about our new products."*
 - *"Tick here if you would like to receive our weekly newsletter, which will sometimes contain information about promotions and offers."*
- Ensure it sends emails via an email address that can be **easily associated with its company**, for example `abdul@plasticpipes.com`
- Write **subject headers that are an honest representation** of what's contained in the email, for example "Weekly Newsletter and Special Offers," or "Exclusive Discount on Our New Pipes Range"
- **Include the company's address and contact details** in every email
- Provide a facility by which **recipients can unsubscribe** - for example a link that leads to a single web page that automatically removes the customer from its mailing list

Chapter 8:

Growing Your Ecommerce Store

In previous chapters, we've looked at some of the privacy implications of operating an ecommerce store. Many of these will be relevant to practically any internet business - for example, creating a Privacy Policy, processing customers' personal information in a secure way, and earning the necessary consent to send marketing emails.

Privacy runs through every aspect of ecommerce. Alongside the more conventional ways of promoting your ecommerce store, you might decide to use innovative marketing tools such as analytics, session recording and remarketing. There are additional, more complex privacy implications when it comes to using these tools.

Analytics

Analytics is a broad term encompassing a number of different techniques used to measure and analyze data about your website. This data may or may not constitute personal information, depending on:

- The nature of the data you collect
- How personal information is defined under the relevant privacy laws
- The steps you take to ensure that individuals are not personally identifiable from the data you collect from them

There are **two important principles** that you should try to remember at all times:

1. You must maintain control over what you're collecting, and
2. You must be transparent with your customers about it

It's possible to end up collecting personal information "by accident" if you aren't careful. Make sure you know what you're collecting and what you need it for. And make sure you disclose anything you're collecting that might be personal information in your Privacy Policy.

Analytics and Privacy Law

Analytics platforms use [third-party cookies](#). It's essential that you're upfront about this, and seek consent where necessary.

One of the most popular analytics services, [Google Analytics](#), requires that websites running the service operate a Privacy Policy that explains how Google uses their personal information. Here's the relevant part of Google's Terms:

7. Privacy.

You will not and will not assist or permit any third party to, pass information to Google that Google could use or recognize as personally identifiable information. You will have and abide by an appropriate Privacy Policy and will comply with all applicable laws, policies, and regulations relating to the collection of information from Visitors. You must post a Privacy Policy and that Privacy Policy must provide notice of Your use of cookies that are used to collect data. **You must disclose the use of Google Analytics, and how it collects and processes data.** This can be done by displaying a prominent link to the site "How Google uses data when you use our partners' sites or apps", (located at www.google.com/policies/privacy/partners/, or any other URL Google may provide from time to time). You will use commercially reasonable efforts to ensure that a Visitor is provided with clear and comprehensive information about, and consents to, the storing and accessing of cookies or other information on the Visitor's device where such activity occurs in connection with the Service and where providing such information and obtaining such consent is required by law.

Image: Google Analytics Terms of Service Privacy clause with disclosure requirements highlighted

Here's how you can implement this:

We use Google Analytics, which uses cookies and similar technologies to collect and analyze information about use of the Site and report on activities and trends. This service may also collect information regarding the use of other websites, apps and online resources. You can learn about Google's practices by going to <https://www.google.com/policies/privacy/partners/>, and opt out of them by downloading the Google Analytics opt-out browser add-on, available at <https://tools.google.com/dlpage/gaoptout>.

Image: Amunix Privacy Policy: Google Analytics clause

It reads:

We use Google Analytics, which uses cookies and similar technologies to collect and analyze information about use of the Site and report on activities and trends. This service may also collect information regarding the use of other websites, apps and online resources. You can learn about Google's practices by going to <https://www.google.com/policies/privacy/partners/>, and opt out of them by downloading the Google Analytics opt-out browser add-on, available at <https://tools.google.com/dlpage/gaoptout>.

It's best to get consent to use Google Analytics if you have EU customers.

Here's how [TrendMD](#) does this:

I consent to the use of Google Analytics and related cookies across the TrendMD network (widget, website, blog). [Learn more](#)

No

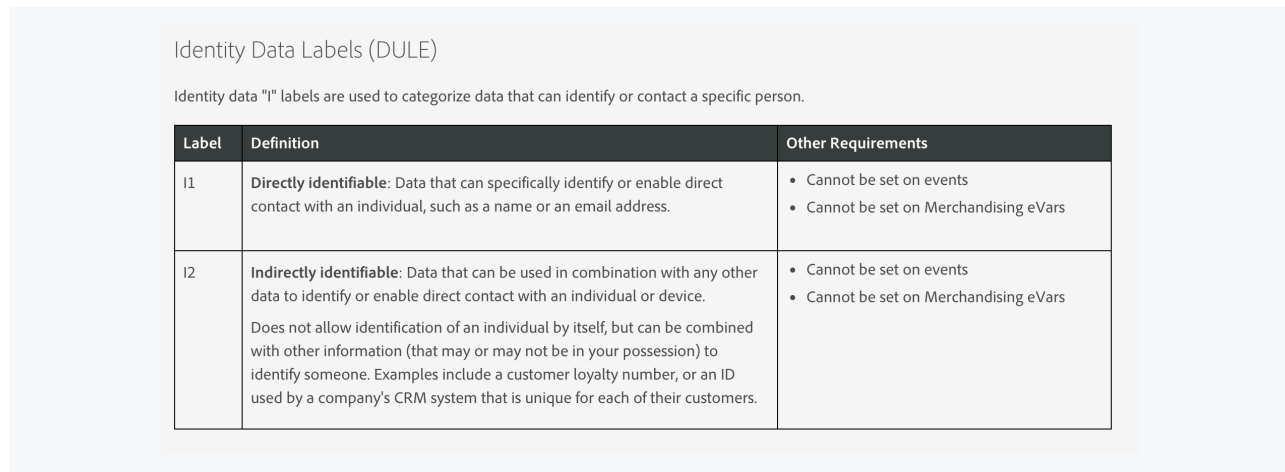
Yes

Image: TrendMD Google Analytics and cookies consent banner notice

Note that it's just as easy to select "Yes" as it is to select "No." This is a really good practice under the GDPR.

It's also possible to make various adjustments to how you collect analytics data in order to minimize the amount of personal information you're collecting. Under [Article 25](#) of the GDPR, you must keep the amount of personal information you collect to an absolute minimum.

Analytics software provider [Adobe Analytics](#) allows users to label the different types of data they collect so as to maintain control over how it is used:



The image shows a screenshot of the 'Identity Data Labels (DULE)' section in Adobe Analytics. It includes a title, a brief explanation of the labels, and a table with two rows: 'I1' for 'Directly identifiable' data and 'I2' for 'Indirectly identifiable' data. Each row has a 'Definition' and 'Other Requirements' column.

Label	Definition	Other Requirements
I1	Directly identifiable: Data that can specifically identify or enable direct contact with an individual, such as a name or an email address.	<ul style="list-style-type: none">• Cannot be set on events• Cannot be set on Merchandising eVars
I2	Indirectly identifiable: Data that can be used in combination with any other data to identify or enable direct contact with an individual or device. Does not allow identification of an individual by itself, but can be combined with other information (that may or may not be in your possession) to identify someone. Examples include a customer loyalty number, or an ID used by a company's CRM system that is unique for each of their customers.	<ul style="list-style-type: none">• Cannot be set on events• Cannot be set on Merchandising eVars

Image: Adobe Analytics GDPR Labels for Analytics Variables: excerpt of Identity Data Labels chart

Session Recording Tools

Session recording is a type of analytics technology which allows you to view your customers' activity on your website in detail by actually recording and replaying their session as they move their mouse pointer around, click links and enter information into forms.

This can allow you to see exactly where visitors might get "stuck" on your website, shows which areas of your website might be difficult to find, and helps you put analytics data into context.

As you can imagine, there are serious implications here for your customers' privacy. If the proper safeguards aren't put in place, it will seem like you are "spying" on people as they move around your site.

Session Recording Tools and Privacy Law

The companies offering session recording tools are very conscious of this potential privacy threat, and many pride themselves on apparently being GDPR-compliant. EU privacy law is seldom straightforward, but many of these services have clearly done their homework.

First, we'll look at how a Privacy Policy can disclose the different types of information it collects on behalf of businesses:

Information We Collect on Behalf of Third Parties.

Cookies And Tracking Technologies: Technologies such as: cookies, beacons, tags and scripts are used by our partners, affiliates, analytics or service providers. These technologies may be used in analyzing trends, administering the Sites, tracking your movements around the Sites and to gather demographic information about our userbase as a whole. We may receive reports based on the use of these technologies by such companies on an individual as well as aggregated basis.

Image: Mouseflow Privacy Policy: Information We Collect on Behalf of Third Parties clause

Note that "third parties" here refers to third parties *other than the company itself* - which is, of course, a third party in relation to your customers.

You can provide some instructions to your clients in a way that ensures they are using the software in a legally compliant way:

	EU/EEA ACCOUNTS	REST-OF-WORLD ACCOUNTS
Website Audit	You need to audit your website(s) to ensure Personal Data is excluded from tracking -- across all page content and form fields (which should be blocked automatically).	You need to audit your website(s) to ensure Personal Data is excluded from tracking -- across all page content and form fields .
IP Addresses	No action is required. We anonymize or exclude IP addresses automatically, according to local law. You can contact us to have IP exclusion enabled (stricter) if your country only requires anonymization.	You may wish to anonymize IP addresses (just click Settings > Anonymize IPs). This removes the last tuple of IP address data. You can contact us to have IP exclusion enabled (stricter) for added protection.

Image: Excerpt of Mouseflow GDPR compliance instructions chart for clients: Website Audit and IP Addresses

You can also explain such things like all IP addresses being anonymized or excluded automatically within the EU. For businesses operating outside of the EU, IP address anonymization is optional.

Explicit Consent	You may need to obtain active and explicit consent to track users on your site. We recommend checking the laws and regulations that apply to your website(s) and obtaining legal advice.	You may need to obtain active and explicit consent to track users on your site. We recommend checking the laws and regulations that apply to your website(s) and obtaining legal advice.
------------------	--	--

Image: Excerpt of Mouseflow GDPR compliance instructions chart for clients: Explicit consent

When EU courts rule on what constitutes personal information, they tend to make very broad interpretations. Monitoring your customers' behavior on your site can render them identifiable under certain circumstances, even where safeguards are in place. Therefore, it is safest to earn your customers' consent for session recording technology.

Different session recording services approach GDPR compliance in different ways. Tracking tool [Hotjar](#), which also offers session recording, has drawn up a Data Processing Agreement:

Data Processing Agreement

This Data Processing Agreement ("DPA"), together with Our [Terms of Service](#), [Privacy Policy](#) and [Acceptable Use Policy](#), forms part of the ("Agreement") entered into by and between Hotjar "We", "Our" or "Us") and the natural or legal person agreeing to it (together with Affiliates of such person which ordered Platforms for such Affiliate as provided in this Agreement, each "Customer", "You" or "Your") to reflect the terms on which Hotjar will process Personal Data in connection with Your use of Our Platform and pursuant to the Agreement. Hotjar and You may each be referred to as a "Party" or collectively as the "Parties."

All capitalized terms in this DPA shall have the same meaning as defined in the Agreement and in the Applicable Law.

Image: Hotjar Sign Data Processing Agreement page

It's necessary under [Article 28](#) of the GDPR for a data controller to have a legally binding agreement with any data processors. Hotjar has set this out very explicitly for its clients.

Another similar service, [Inspectlet](#), has conducted a Privacy Impact Assessment in order to ensure GDPR compliance. This is a requirement under [Article 35](#) of the GDPR for processing involving new technology.

Here's part of Inspectlet's Privacy Impact Assessment where it discusses the measures it takes to anonymize IP addresses:

Technical and security measures

All data is encrypted during transmission and collected data is stored encrypted at rest using AES encryption. If the Customer has enabled IP address anonymization, the last two octets of the IP address will be removed and not be available to the user nor Inspectlet. Backups of data collected are made routinely and tested occasionally to verify restore procedure functionality. All data is physically stored only in AWS data centers meeting ISO 27001 compliance.

Image: Inspectlet Privacy Impact Assessment for GDPR: Technical and security measures section

It reads:

Technical and security measures

All data is encrypted during transmission and collected data is stored encrypted at rest using AES encryption. If the Customer has enabled IP address anonymization, the last two octets of the IP address will be removed and not be available to the user nor Inspectlet. Backups of data collected are made routinely and tested occasionally to verify restore procedure functionality. All data is physically stored only in AWS data centers meeting ISO 27001 compliance.

Inspectlet has decided that removing the last two octets of IP addresses will help ensure that users' personal information is not revealed. This is one of the methods suggested by the Internet Engineering Task Force's Internet Area Working Group ([IntArea](#)) for anonymizing log data in a GDPR compliant way:

3. Recommendations for Internet-facing servers

This section is intended to replace [Section 2 of \[RFC6302\]](#).

Providers of internet-facing servers

SHOULD only store entire incoming IP addresses for as long as is necessary to provide the specific service requested by the user.

SHOULD keep only the first two octets (of an IPv4 address) or the first three octets (of an IPv6 address) with remaining octets set to zero, when logging.

SHOULD NOT store logs of incoming IP addresses from inbound traffic for longer than three days.

Image: IntArea Working Group Logging Recommendations for Internet-Facing Servers - Providers section

Session recording technology does represent a considerable privacy risk if not used carefully. However, the examples above show that companies offering such tools do take privacy seriously.

Remarketing

[Remarketing](#) (retargeting) is a method of using cookies to display ads to your users *after* they've left your site.

If you've ever added a product to your cart and then abandoned the purchase, you might have spent the next few weeks noticing ads for that product pop up in unexpected places. This is no coincidence. The ecommerce store most likely placed a cookie on your device that followed you around the ad network to tempt you into completing the sale.

This is a highly effective marketing technique, but your customers might find it a little creepy. However, with the right privacy protections in place you should be able to put their minds at rest.

Remarketing and Privacy Law

[Google Ads](#) is one of the more popular ad networks to offer a remarketing service. It makes clear that anyone wishing to use the service must disclose that they are doing so in their Privacy Policy, and explain the implications.

Here's how [Clickseed](#) fulfills this requirement:

This website uses Google AdWords & Facebook Remarketing Tags

This website uses Google AdWords & Facebook remarketing service to advertise on third party websites to previous visitors to our site. It could mean that we advertise to previous visitors who haven't completed a task on our site, for example using the contact form to make an enquiry. This could be in the form of an advertisement on the Google search results page, a site in the Google Display Network, or somewhere on Facebook. Third-party vendors, including Google & Facebook, use cookies to serve ads based on someone's past visits to the ClickSeed website. Of course, any data collected will be used in accordance with our own privacy policy, as well as Google & Facebook privacy policies.

You can opt-out of remarketing by visiting the links below:

For Google: <https://support.google.com/ads/answer/2662922?hl=en>

For Facebook: https://www.facebook.com/ads/website_custom_audiences/

Image: Clickseed Privacy Policy - Google AdWords and Facebook Remarketing Tags clause

It reads:

This website uses Google AdWords & Facebook Remarketing Tags

This website uses Google AdWords & Facebook remarketing service to advertise on third party websites to previous visitors to our site. It could mean that we advertise to previous visitors who haven't completed a task on our site, for example using the contact form to make an enquiry. This could be in the form of an advertisement on the Google search results page, a site in the Google Display Network, or somewhere on Facebook. Third-party vendors, including Google & Facebook, use cookies to serve ads based on someone's past visits to the ClickSeed website. Of course, any data collected will be used in accordance with our own privacy policy, as well as Google & Facebook privacy policies.

You can opt-out of remarketing by visiting the links below:

For Google: <https://support.google.com/ads/answer/2662922?hl=en>

For Facebook: https://www.facebook.com/ads/website_custom_audiences/

You should give your customers a choice about whether they want to be subject to remarketing. You can do this by seeking their consent in the same way that you've sought their consent for other types of cookies.

You then can use a tool such as [Google Tag Manager](#) to ensure that you're excluding customers from remarketing where they have not opted in (or perhaps where they have opted *out*, if they're outside of the EU).

Case Study

Perfect Pasta is an Italian food company that sells dried pasta through its ecommerce store. It hopes to promote its business and improve its website through the use of analytics and tracking technologies.

Perfect Pasta should be sure to:

- Make absolutely sure that any third-party services it uses to provide this service are GDPR-compliant
- Only conduct business with such third parties under a clear and legally-binding contract
- Give a clear explanation of the tracking and targeting technologies it uses and the reasons that it uses them in its Privacy Policy
- Earn its customers' consent to be subject to such marketing techniques
- Offer any customers that have opted in a clear method by which to opt out
- Use such technologies in a responsible way that keeps the amount of personal information collected to a minimum

Note From the Editors

We hope this has been a helpful overview of the legal implications of running an ecommerce store. As you can see, there are a number of different legal policies you'll need, and some you'll benefit greatly from having. There are also a variety of laws that you'll need to be aware of that affect the ecommerce landscape. From your Privacy Policy to handling returns, these seemingly small details can truly transform the way the public perceives your ecommerce store as trustworthy and compliant.

As your business grows and changes, and as you enter into new business relationships, your company's policies will remain the backbone of your dealings with the public and with legal authorities. Paying attention now and creating the most compliant policies in line with legal requirements will help you consistently save time, effort and money in the future so you can focus on the more enjoyable, exciting aspects of running your unique business.

We wish you the best in your business endeavors, and want to remind you that you can return to the relevant chapters of this book at any time to make sure you're getting it right. And you can always visit our [TermsFeed blog](#) for the most up-to-date and relevant information on the ever-changing legal and regulatory landscape.



TermsFeed