litmus

FOUNDATIONS OF PRIVACY

Get back to the basics—and build a solid foundation for the future

At its core, marketing is driven by data and as marketers, it's our responsibility to protect that information, whether it's given to us directly or indirectly.

Privacy, in the context of email marketing, is about protecting your subscribers' data and using it in transparent and ethical ways. By explaining your process—what you're collecting, how you plan to use it, and most importantly, how you plan to protect personal information—you'll build trust with your subscribers, which is especially important as privacy measures increase.

And, as our world continues to become more data-driven and privacy-focused, it's imperative to be informed of the privacy laws that apply to email.

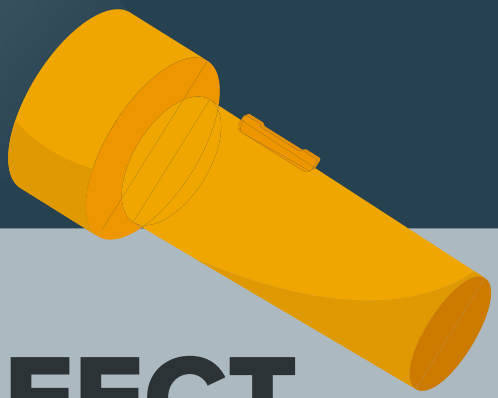
We compiled important points, considerations, and guidelines to help ensure your email campaigns are compliant and equip you with the knowledge you need to handle the ever-changing privacy landscape.

Disclaimer: *This guide provides a high-level overview about privacy laws but is not intended, and should not be taken, as legal advice. Please contact your attorney for advice on email marketing regulations or any specific legal problems.*

FIRST UP: Laws That Affect Email Marketing

LESSON

1



LAWS THAT AFFECT EMAIL MARKETING

First things first: Let's briefly familiarize ourselves with the privacy laws all email marketers should know and understand: CAN-SPAM, CASL, GDPR, and CCPA.

1.1 Anti-Spam Laws

- CAN-SPAM
- CASL

1.2 Data Privacy Laws

- GDPR
- CCPA

Disclaimer: *This guide provides a high-level overview about privacy laws but is not intended, and should not be taken, as legal advice. Please contact your attorney for advice on email marketing regulations or any specific legal problems.*

1.1 Anti-Spam Laws

Anti-spam laws are regulations around unsolicited emails, designed to protect citizens from receiving unwanted commercial or spam emails.

BRIEF HISTORY

Email was founded in 1971. As email became more commercialized as an accessible means of communication, unsolicited emails (or spam) became a serious problem—particularly in the 2000s.

This led to the **Controlling the Assault of Non-Solicited Pornography And Marketing (CAN-SPAM)** act of 2003—America's first federal law designed to combat spam.

CAN-SPAM

Enforced in the U.S.

A law that sets the rules for commercial email, establishes requirements for commercial messages, gives recipients the right to have you stop emailing them, and spells out tough penalties for violations.

Source: Federal Trade Commission

CAN-SPAM requires that businesses and brands:

- Include **a working unsubscribe link** in every marketing email sent
- Honor opt-out requests **within 10 business days**
- Include their **mailing address** in every email they send
- Never use misleading or **deceptive sender names, subject lines, or email copy**
- Never attempt to **conceal their identity or the fact that they're sending advertising**

DIVE DEEPER

Here's more on the impact of CAN-SPAM and how it can be improved.

For a further look into CAN-SPAM, visit the Federal Trade Commission's website.

Another anti-spam law affecting email marketing is **Canada's Anti-Spam Legislation (CASL)**, which came into effect in 2014.

CASL is known as one of the world's strictest anti-spam laws. The law sets clear requirements for sending a marketing email—also referred to as commercial electronic message (CEM).

CASL

Enforced in Canada

A federal law dealing with spam and other electronic threats. It is meant to protect Canadians while ensuring that businesses can continue to compete in the global marketplace.

Source: Office of the Privacy Commissioner of Canada

There are three general requirements for sending a CEM:

- Obtain consent
- Provide identification information
- Provide an unsubscribe mechanism

Source: Canadian Radio-television and Telecommunications Commission (CRTC)

There are two types of consent under CASL: express and implied.

Express consent does not expire, however the recipient has the right to withdraw their consent at any time. *Want to jump ahead?* We cover explicit and implied consent in Lesson 2 ↓

DIVE DEEPER

Here's more on CASL on our blog.

Visit the Office of the Privacy Comissioner of Canada's website for further information on CASL.

In summary

Both CAN-SPAM and CASL focus on transparency and choice around unwanted electronic communication. They both require that all promotional emails include a working unsubscribe link and sender identification.

The main difference between the two is that CAN-SPAM is an opt-*out* law, while CASL is an opt-*in* law, requiring proof of opt-in. CAN-SPAM mainly requires the ability for anyone to opt-out when they no longer wish to receive a business or brand's emails.

Let's move on to data privacy laws.

1.2 Data privacy laws

Data privacy laws provide a legal framework that specify how an individual's data should be collected, stored, and shared with third parties.

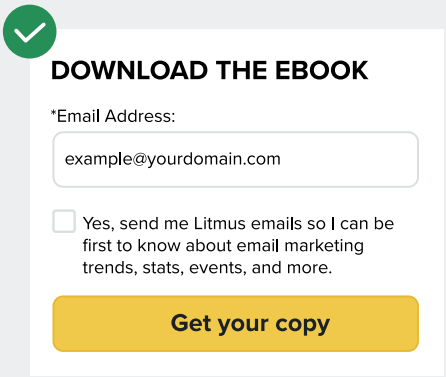
In 2018, the European Union's privacy law, **General Data Protection Regulation (GDPR)** came into effect.

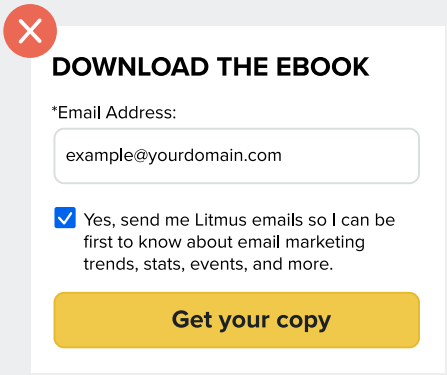
GDPR

Enforced in Europe and the UK*

Enforces the protection of natural persons with regard to the processing of personal data and on the free movement of such data.

Source: European Comission





***Does GDPR include the United Kingdom (UK), post-Brexit?**

After Brexit—the UK's formal departure from European Union (EU)—the UK has created its own UK GDPR. It's pretty much the same as the EU GDPR except that it applies to UK residents only. More details can be found in the Guide to the UK GDPR from the UK's Information Commissioner's Office (ICO).

(For simplicity's sake, we've referred to both as GDPR unless referencing one specifically.) To get a complete review of GDPR visit the European Commission website.

Here's how to keep email consent compliant with GDPR:

- Provide the option to **unsubscribe** in every email
- Get consent from a **positive opt-in** (not pre-ticked boxes)
- Keep consent requests **separate from other terms & conditions**
- Make it easy for people to **withdraw consent**
- Keep **evidence of who consented**, when, and how
- Review your **consent practices** and **existing opt-ins**

DIVE DEEPER

We cover these points in greater detail over on our blog post about GDPR.

Driven by the continued rise in consumer data breaches and growing privacy concerns, the state of California passed the **California Consumer Privacy Act (CCPA)** of 2018, which went into effect in 2020.

CCPA

Enforced in the U.S. in the state of California

The California Consumer Privacy Act of 2018 (CCPA) gives consumers more control over the personal information that businesses collect about them. The CCPA regulations provide guidance on how to implement the law.

Source: State of California Department of Justice

DIVE DEEPER

We explore how CCPA affects marketers along with best practices on our blog.

This landmark law secures new privacy rights for California consumers, including:

- The **right to know** about the personal information a business collects about them and how it is used and shared
- The **right to delete** personal information collected from them (with some exceptions)
- The **right to opt-out** of the sale of their personal information; and
- The **right to non-discrimination** for exercising their CCPA rights.

Learn more about CCPA from the State of California Department of Justice.

Lesson recap

Here's an overview of points, to help you stay compliant with CAN-SPAM, CASL, GDPR, and CCPA. Please contact your attorney for advice on email marketing regulations or any specific legal problems.

- ☐ Include a **working unsubscribe link** in every marketing email sent
- ☐ Include a valid **mailing address, telephone number, email address**, and **web address** in your emails
- ☐ **Make it easy** to withdraw consent
- ☐ Get consent from a **positive opt-in**, not pre-ticked boxes (CASL, GDPR)
- ☐ Honor **opt-out requests promptly** (within 10 business days for CAN-SPAM and CASL and within 15 business days for CCPA)
- ☐ Keep consent requests **separate from other terms & conditions** (GDPR)
- ☐ **Keep evidence** of who consented, when, and how
- ☐ Review your **consent practices and existing opt-ins**

LESSON

2

DATA COLLECTION AND MANAGEMENT

Now that you've got an understanding of the laws and regulations around email marketing, let's look at how to collect, store, and manage subscriber data.

2.1 Forms of Consent

Before sending marketing emails, it's important to understand email marketing compliance—specifically, the difference between explicit and implied opt-in consent.

Here's what each look like, in the context of email marketing.

EXPLICIT CONSENT

also known as express consent

When a person has clearly agreed (orally or in writing) to receive marketing emails from you

- Provides **higher-quality** subscribers but at a **lower quantity**
- **Does not expire**; valid until recipient withdraws their consent
- **Always allowed**

Examples:

- Clicking a checkbox on a form
- Confirming through double opt-in (DOI)
- Opting-in through written consent

IMPLICIT CONSENT

also known as implied or inferred consent

When a person has not directly signified that they want to receive marketing emails from you, but have provided their email address over a course of normal business communication

- Provides a **higher quantity** of subscribers but of **lower quality**
- Typically **expires after a certain amount of time**
- **Banned** or **heavily restricted** under certain jurisdictions

Examples:

- Collecting customer information from checkout
- Collecting emails from a "Contact Us" form
- Signing up for gated content or resources

NOTE: **Implied consent** jurisdiction varies by country. When implied consent is allowed, it is usually restricted to a specific time frame or under a set of circumstances. Please contact your attorney for advice on email marketing regulations or any specific legal problems.

Now that we've covered our basis on types of consent—**how do you collect permission for email?**

2.2 Collecting Email Permission

Let's start by clearly defining the two major approaches to email permission:

Single opt-in (SOI)

A subscription process where a new email address is **added to your mailing list without requiring** the owner of that email address to confirm definitively that they knowingly and willingly opted in

Double opt-in (DOI)

also known as confirmed opt-in (COI)

A subscription process where a new email address is only **added to your mailing list after the email address owner clicks a confirmation link** in an opt-in confirmation request email that's sent after they opt in via a form or checkbox

	SINGLE OPT-IN	DOUBLE OPT-IN
Subscriber Experience	Less friction	More friction
List Growth	Faster	Slower
Engagement	More overall	Better overall
Deliverability	Higher bounce rates and bad addresses	Lower bounce rates and cleaner lists

Here's where we stand on single opt-in vs. double opt-in (hint: it depends).

What does that mean for pre-checked boxes?
Certain laws require action in order to consent to marketing emails—like GDPR and CASL.

- **For GDPR**, opt-in must be explicit. You cannot use a pre-checked checkbox on a form.
- **For CASL**, you will mostly need explicit permission. You cannot use a pre-checked checkbox on a form.
- **For CAN-SPAM**, no explicit opt-in is technically required.

2.3 Opting Out

To comply with anti-spam and privacy laws like CAN-SPAM, CASL, GDPR, and CCPA, you should ensure all marketing emails sent contain an unsubscribe link—aka, the right to opt-out.

CASL, GDPR, and CCPA specify that the unsubscribe process should be easy for the subscriber—and we recommend you make it easy across the board.

HERE ARE SOME DOS AND DONT'S ON UNSUBSCRIBES:

- ✓ Promptly honor unsubscribes
- ✓ Allow subscribers to opt-down or temporarily pause email subscriptions
- ✓ Provide the opportunity to resubscribe
- ✓ Provide options for your ex-subscribers to follow your brand on other channels
- ✗ Send an unsubscribe confirmation email
- ✗ Ask people to log in to unsubscribe
- ✗ Make people fill out a survey before they've unsubscribed
- ✗ Bury the unsubscribe link in your email or override the link styling

DIVE DEEPER

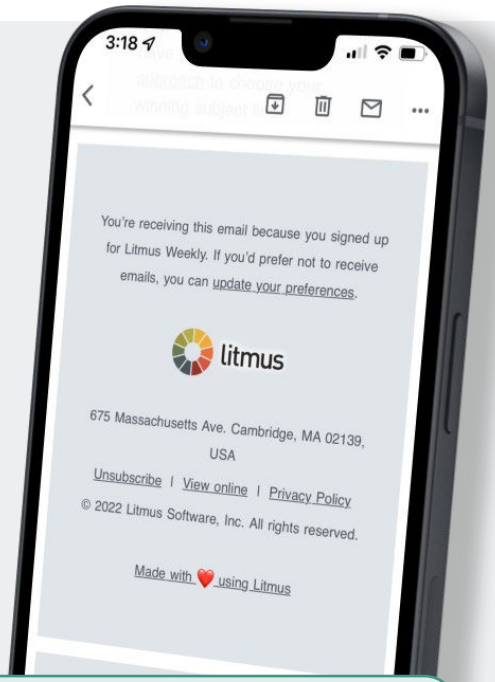
We go over unsubcribe dos and dont's at greater length on our blog.

INSIDE LOOK - LITMUS' PREFERENCE CENTER

Preference centers are a great way to meet the wants of your subscribers and to ensure they're *not* getting unsolicited emails.

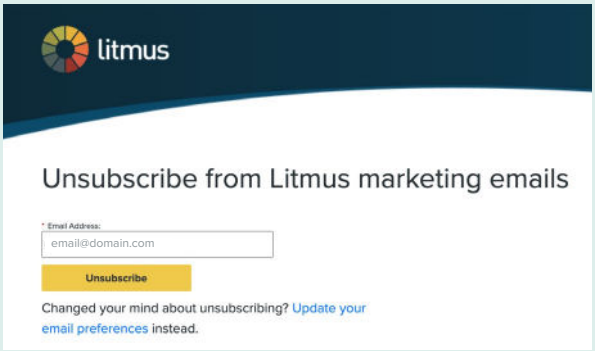
If your brand or business has multiple newsletters, preference centers are key for keeping your subscribers happy. Not only do they help you build first-party data, but also more personalized email experiences.

At Litmus, our email footers contain both a link to "unsubscribe" and one to "update your preferences."



OPTION 1: Update your preferences

OPTION 2: Unsubscribe*



*The key is to provide a universal unsubscribe button that makes it simple and easy to opt-out. Offer a way for people to unsubscribe from all of your emails—and make it easy for them. This helps you stay compliant with laws now (and in the future).

DIVE DEEPER

Learn more about email preference center best practices with examples for inspiration.

2.4 Storing and Deleting Subscriber Data

Data privacy laws define other common consumer rights—including the right to access and the right to be forgotten.

RIGHT TO ACCESS

GDPR and CCPA give your subscribers the right to see all personal identifiable information (PII) you've collected on them—so you'll need to have a process in place for compiling and delivering that information to them.

RIGHT TO BE FORGOTTEN

This is more than removing someone from your email list—it means deleting every data point you have on that individual.

To comply, you'll need to delete their data completely, as if they never existed in your database (including any third-party databases that you may use).

Opting out or unsubscribing is not the same as exercising the right to be forgotten. Individuals will need to contact your brand or business and make a request, and you will need to make sure have at least one official way for individuals to request data deletion (according to the CCPA).

Lesson recap

- ☐ Implied consent jurisdiction **varies by country**.
- ☐ Certain laws require **action** in order to consent to receive marketing emails—like GDPR and CASL.
- ☐ CASL, GDPR, and CCPA specify that the unsubscribe process should be **easy for the subscriber**—and we recommend you make it easy to do so across the board.
- ☐ Data privacy laws define other common consumer rights—including the **right to access** and the **right to be forgotten**.

LESSON

3

PRIVACY-PROOFING

Privacy-proofing means setting up your email program for longevity and success, with privacy top of mind.

In this lesson, we'll cover privacy as it stands today, and how to prepare for an ever-changing landscape:

3.1 State of Data Privacy

The rules around privacy are changing—and ever-evolving. Recent shifts in marketing—like the introduction of Apple's Mail Privacy Protection (MPP) in 2021 and the death of third-party cookies from Google in 2024—has email marketers putting consumer privacy in focus now more than ever before.

HOW DID WE GET HERE?

> *"For most of its existence, the data economy was structured around a 'digital curtain' designed to obscure the industry's practices from lawmakers and the public.*
>
> *Data was considered company property and a proprietary secret, even though the data originated from customers' private behavior. That curtain has since been lifted and a convergence of consumer, government, and market forces are now giving users more control over the data they generate."*
>
> — Harvard Business Review

In short, power is going back into consumer's hands, causing a ripple effect into our roles as marketers. A new rule—or standard—that brands and businesses should work toward is "trust over transactions." Data collected with meaningful consent will become the most valuable data of all, because it's the only data companies will be permitted to act upon, down the line.

Three distinct pressures driving change in the personal data industry:

1. Consumer mistrust
2. Government action
3. Market competition

Challenges ahead for the future of privacy

The loss of third-party cookies

In March 2021, Google announced that its ad tools would no longer support individual tracking of users across websites. This phase out is set for the second half of 2024.

While this seemed shocking, it wasn't a surprise, as Google Analytics—which relies on cookies—isn't GDPR compliant by default.

The GDPR ruling means that websites can no longer rely on implicit opt-in, and must not capture opt-in consent before any analytics or web tracking cookies are placed on a browser.

> *"If your organization generates any value from personal data, you will need to change the way you acquire it, share it, protect it and profit from it."*
>
> — Harvard Business Review

> *"23% of marketing experts plan on investing in email marketing software due to Google's new policy."*
>
> — HubSpot

3.2 Privacy-Proof Your Email Program

As privacy measures continue to increase, it's imperative for email marketers to think about the long-term health of their email program—and that means prioritizing privacy.

Our tip: If you aren't doing it now, you should be taking action to privacy-proof your email program. **Here's how:**

1. INCREASE COLLECTION OF ZERO-PARTY DATA

Zero-party data is individual-level data explicitly given to you, directly from an individual. It's a key component for future-proofing because it's reliable data.

DIVE DEEPER

Familiarize yourself with the four types of data.

By increasing your efforts to collect more zero-party data, you'll set yourself up for success down the line as privacy measures change. Subscription preference centers can be a great place to tap into to gather zero-party data, like topics of interest.

2. ENSURE CONFIRMATION CAMPAIGNS ARE IN PLACE

Stay on top of your list hygiene and ensure you have confirmation campaigns in place that gather explicit opt-in from existing subscribers.

You can do this in a few ways: re-permission campaigns as part of your regular practice and DOI (double opt-in), if you aren't doing it already.

3. TRACK ENGAGEMENT WITH METRICS *OTHER* THAN OPEN RATES

As adoption of MPP increases, open rates will become less reliable due to perceived inflation. Shift your focus to engagement metrics instead, such as click-through rates, conversion rates, and unsubscribe rates.

4. REDEFINE HOW YOU RE-ENGAGE CUSTOMERS, *OUTSIDE* OF EMAIL

Take an omnichannel approach: The real key for measuring engagement is looking beyond email.

Look at your other platforms and incorporate attribution metrics that demonstrate customer engagement—such as offline purchases, account activity, website visits, mobile app activity, and SMS engagement. Think of email as a touch point for engagement.

5. STEER AWAY FROM DEPENDENCE ON OPENS AND GEOLOCATION

MPP has impacted email marketers' ability to track geolocation. That's why it's a good idea to start adjusting how you measure your program's performance, outside of these metrics.

Audit your email program(s) and check for instances where you rely on open rates and geolocation. Then, discuss new ways to move forward with your team. These may include:

- Trigger automated nurture flows
- Content for emails based based on open tracking
- Re-engagement campaigns (if based on opens)
- A/B tests (if winners are determined by opens)
- Send time optimization (if based on geolocation)

6. CONSIDER REMOVING PERSONALLY IDENTIFIABLE INFORMATION (PII)

How does PII apply to email marketing? A person's account information is usually linked to an email address for a product or service. If there were ever a security breach, that information would be tied to the subscriber.

Personally identifiable information (PII)

Information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual.

Source: U.S. General Services Administration

To privacy-proof: Remove PII to protect your subscribers' sensitive information. Instead of PII, a subscriber ID number can be used. By assigning an ID, you can connect information to an individual user and protect their information from being passed to other systems, in case of a breach.

DIVE DEEPER

Get more on these six privacy-proofing tips on our blog.

Lesson recap

- [ ] Increase collection of zero-party data
- [ ] Ensure confirmation campaigns are in place
- [ ] Track engagement with metrics other than open rates
- [ ] Redefine how you re-engage customers, outside of email
- [ ] Audit your email programs and steer away from dependence on opens and geolocation
- [ ] Consider removing PII

Foundations of Privacy—complete.

Want to stay in touch?

Get how-tos, inspiration, and more from our newsletters—for email pros, by email pros.

Subscribe today

A little about about us

Litmus provides the leading email personalization, optimization, and collaboration software for marketers. From pre-Send campaign development, testing, and AI-driven content recommendations through Kickdynamic, to post-send insights for future content optimization, Litmus improves marketing performance and boosts customer engagement. Drive conversion and revenue with Litmus' suite of solutions that enable users to efficiently build, test, and collaborate on large volumes of emails, while simultaneously creating highly personalized email experiences at scale. With offices in Boston, San Mateo, and London and backed by Spectrum Equity, Litmus is used by major global brands across every industry, including 80% of the Fortune 100, the top 10 retailers, 9 of the top 10 ecommerce brands and U.S. banks, and 23 of the top 25 U.S. advertising agencies. Learn more about Litmus at litmus.com, subscribe to the Litmus blog, or follow us on social media - Twitter, LinkedIn, Instagram, and Facebook.