CONSENT AND THE LAW

Email consent laws *compared*

GDPR, CAN-SPAM, CASL, LGPD and more

YANNA-TORRY ASPRAKI

CONTENTS

What is *inside*

The 60-second answer	3
Consent under review	4
Your plan	5
The card	5
What this means for your send	47
Worked example	48
Words used	49
About Review My Emails	50
Your next step	52

FOR:

anyone emailing people in another country, or checking a list before a send. A shop with buyers abroad, a newsletter with readers everywhere, a team asked "are we allowed to email these people?"

The 60-second *answer*

1 **The law follows the reader, not you.**

A US business emailing someone in the EU must meet GDPR. One send can fall under several laws at once.

2 **There are two models.**

The US lets you send until someone opts out. The EU, Canada and the Asia Pacific laws on this card want consent first.

3 **Meet the strictest and you meet the rest.**

Applying GDPR or CASL rules to everyone is the simpler path, and it fits most programs. GDPR compliance satisfies CAN-SPAM, but not the other way round.

Send until they stop

The US lets you send until someone opts out

Honor every opt-out

Consent first

The EU, Canada and the Asia Pacific laws on this card

Ask before the first email

Meet the strictest

Applying GDPR or CASL rules to everyone

The simpler path

CONSENT UNDER REVIEW

Email consent, *under review.*

Find the row for each country on your list. The tag gives the card's answer to what you need before the first email.

CONSENT FIRST · A LEGAL BASIS · OPT-OUT ALLOWED

EU and EEA GDPR — CONSENT FIRST

BEFORE THE FIRST EMAIL

Opt-in. A clear action, freely given, specific and informed. Pre-ticked boxes and silence do not count

United Kingdom PECR, with UK GDPR — CONSENT FIRST

BEFORE THE FIRST EMAIL

Consent for people, with a soft opt-in for your own customers about similar products, if they could opt out when you took the address. Company addresses such as info@ can be mailed without consent first, but a named person's work address counts as a person

United States CAN-SPAM — OPT-OUT ALLOWED

BEFORE THE FIRST EMAIL

No consent needed first. You may send until someone opts out

California CCPA, as amended by CPRA — OPT-OUT ALLOWED

BEFORE THE FIRST EMAIL

No consent needed to send. It governs what you do with the data afterwards

Canada CASL — CONSENT FIRST

BEFORE THE FIRST EMAIL

Express consent, or implied consent for 24 months after a purchase or 6 months after an inquiry

Brazil LGPD — A LEGAL BASIS

BEFORE THE FIRST EMAIL

A legal basis, usually consent or legitimate interest. Consent means a positive action for a specific purpose, never a pre-ticked box

Australia Spam Act 2003 — CONSENT FIRST

BEFORE THE FIRST EMAIL

Consent, express or inferred. Inferred consent does not expire while the relationship lasts

Singapore PDPA — CONSENT FIRST

BEFORE THE FIRST EMAIL

Consent, and a check of the national Do Not Call Registry before you send

Japan Act on Regulation of Transmission of Specified Electronic Mail — CONSENT FIRST

BEFORE THE FIRST EMAIL

Opt-in for most commercial messages

India DPDP Act 2023 — CONSENT FIRST

BEFORE THE FIRST EMAIL

Consent, with notice and a stated purpose

YOUR PLAN

Your countries, and *what each one asks*

YOUR READERS ARE IN _____

THEIR ROWS _____

BEFORE THE FIRST EMAIL _____

PROOF OF SIGN-UP KEPT IN _____

CHECKED ON _____

Clean your first 1,000 addresses free at reviewmyemails.com/get-started.

The *card*

EU and EEA

LAW	GDPR
BEFORE THE FIRST EMAIL	Opt-in. A clear action, freely given, specific and informed. Pre-ticked boxes and silence do not count
UNSUBSCRIBE	Without unreasonable delay, read as days, not weeks. Leaving must be as easy as joining
WHAT YOU MUST PROVIDE	Proof of when and how each person agreed
TOP FINE	Up to €20 million or 4 percent of global turnover, whichever is higher, for consent failures

United Kingdom

LAW	PECR, with UK GDPR
BEFORE THE FIRST EMAIL	Consent for people, with a soft opt-in for your own customers about similar products, if they could opt out when you took the address. Company addresses such as info@ can be mailed without consent first, but a named person's work address counts as a person
UNSUBSCRIBE	An easy unsubscribe in every message
WHAT YOU MUST PROVIDE	Who you are, contact details that work, and a valid opt-out
TOP FINE	Not in the Almanac yet

United States

LAW	CAN-SPAM
BEFORE THE FIRST EMAIL	No consent needed first. You may send until someone opts out
UNSUBSCRIBE	Honored within 10 business days, and the link must work for 30 days after the send
WHAT YOU MUST PROVIDE	Honest headers and subject line, a note that it is an advertisement, a physical postal address, a working unsubscribe
TOP FINE	Up to $53,088 per email

California

LAW	CCPA, as amended by CPRA
BEFORE THE FIRST EMAIL	No consent needed to send. It governs what you do with the data afterwards
UNSUBSCRIBE	Not in the Almanac yet
WHAT YOU MUST PROVIDE	A Do Not Sell or Share link if you share data with ad networks, and real deletion when someone asks, not only suppression
TOP FINE	Not in the Almanac yet

Canada

LAW	CASL
BEFORE THE FIRST EMAIL	Express consent, or implied consent for 24 months after a purchase or 6 months after an inquiry
UNSUBSCRIBE	Processed within 10 business days
WHAT YOU MUST PROVIDE	Who is sending, contact details that work for 60 days after the send, a working unsubscribe
TOP FINE	Up to $10 million CAD per violation for a business

Brazil

LAW	LGPD
BEFORE THE FIRST EMAIL	A legal basis, usually consent or legitimate interest. Consent means a positive action for a specific purpose, never a pre-ticked box
UNSUBSCRIBE	Consent can be withdrawn at any time, as easily as it was given
WHAT YOU MUST PROVIDE	A plain privacy notice in Portuguese, and a way to honor each person's rights
TOP FINE	Up to 2 percent of Brazilian revenue, capped at 50 million reais per violation

Australia

LAW	Spam Act 2003
BEFORE THE FIRST EMAIL	Consent, express or inferred. Inferred consent does not expire while the relationship lasts
UNSUBSCRIBE	A working unsubscribe
WHAT YOU MUST PROVIDE	Who is sending
TOP FINE	Up to AUD 2.22 million a day for serious breaches

Singapore

LAW	PDPA
BEFORE THE FIRST EMAIL	Consent, and a check of the national Do Not Call Registry before you send
UNSUBSCRIBE	Not in the Almanac yet
WHAT YOU MUST PROVIDE	Who is sending
TOP FINE	Up to $1 million SGD for organisations

Japan

LAW	Act on Regulation of Transmission of Specified Electronic Mail
BEFORE THE FIRST EMAIL	Opt-in for most commercial messages
UNSUBSCRIBE	Not in the Almanac yet
WHAT YOU MUST PROVIDE	Who is sending
TOP FINE	Can include criminal liability for individuals

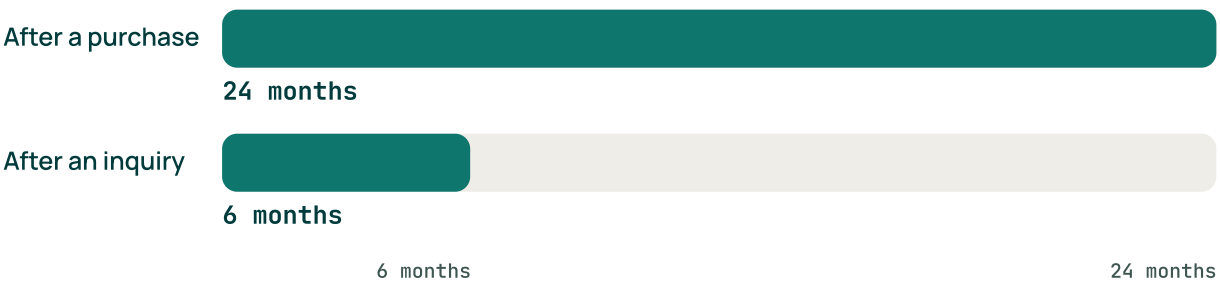
India

LAW	DPDP Act 2023
BEFORE THE FIRST EMAIL	Consent, with notice and a stated purpose
UNSUBSCRIBE	Not in the Almanac yet
WHAT YOU MUST PROVIDE	Rights to access, correction and erasure
TOP FINE	Still being defined

Data requests: under GDPR a person can ask what you hold about them, and you answer within one month, free of charge. That can stretch by two more months for complex cases if you tell them in the first month. UK GDPR is the same. CCPA allows 45 days, plus 45 more.

This card is about email, not legal advice. Email law is complex and varies by country. If you are unsure about your own setup, talk to someone who practises email law where you send.

CANADA'S IMPLIED CONSENT CLOCK



Every row on the card rests on the same starting point, so it comes first.

What is “consent” in email marketing?

You're about to send a marketing email, but you hit a mental speedbump: do you have permission to send it? That’s consent in action. It’s the permission someone gives you to receive marketing emails from your business. Seems straightforward, but consent sits at the center of laws like GDPR, CASL, and CAN-SPAM. These laws define and enforce consent differently, which matters for your sender reputation and your subscribers' trust.

Consent exists on a spectrum. On one end, you've got explicit consent: someone actively checks a box or types their email to subscribe. That’s powerful. On the other end, implicit consent: someone buys from you, so you infer they want order updates and promotional mail. Explicit consent almost always wins for building engaged lists. The stronger your consent, the fewer complaints you get. The fewer complaints, the better your sender reputation.

Here’s the truth: consent isn’t just a legal checkbox. It’s the foundation of a real relationship with your subscribers. When someone explicitly agrees to get your emails, they're expecting value. Meet that expectation consistently, and they'll stay. Ignore it, and they'll mark you spam. Even compliant, explicit consent can backfire if your content doesn’t match what they thought they'd get. Take a look at your current consent practices and make sure the words you use match what you actually send.

Do I need to comply with laws in every country I email?

Yes. Email compliance is determined by where your recipient is, not where you are. When a US company emails a German resident, **GDPR** applies. When an Australian company emails a Canadian resident, **CASL** applies. Your headquarters location doesn’t change that.

This means a single campaign to an international list can need to satisfy multiple laws simultaneously: **GDPR** for EU recipients, **CASL** for Canadian ones, **CAN-SPAM** for US ones, **LGPD** for Brazilian ones, and various APAC laws on top. Each recipient is covered by their own jurisdiction’s rules.

Ignoring foreign laws because you’re based elsewhere doesn’t protect you. It just means violations go unnoticed until enforcement action or blocked mail makes them visible. If you send to a global list, the easiest path to coverage is applying the strictest standard to everyone and documenting your consent practices accordingly.

The next two answers compare GDPR and CAN-SPAM directly.

Is CAN-SPAM the same as GDPR?

> No, CAN-SPAM and GDPR are not the same. CAN-SPAM is a US federal opt-out law (15 U.S.C. 7701) requiring honest sender identification, a physical postal address, and unsubscribe honored within 10 business days. GDPR is an EU regulation (2016/679) requiring a lawful basis, typically explicit prior consent, before sending marketing email. GDPR follows the recipient's location, so any EU subscribers on a US list still require GDPR-level treatment.

They're not the same, and mixing them up can get you in real trouble. CAN-SPAM is a US federal law. GDPR is a European regulation. Both govern email, but they work from completely opposite starting assumptions.

CAN-SPAM is an opt-out framework. You're allowed to email people first and give them a way to stop hearing from you. As long as you identify yourself honestly, include a physical address, and honor unsubscribe requests within 10 days, you're technically compliant. It's a low bar.

GDPR is an opt-in framework. Before you send anything to someone in the EU, you need a lawful basis for doing so. For marketing email, that almost always means explicit consent, meaning the person actively agreed to receive emails from you. Pre-ticked boxes don't count. Implied permission doesn't count. "They're a customer" sometimes counts, but only under specific conditions.

Here's the part that trips people up. If you send to a mixed audience (some US subscribers, some EU), you can't just meet CAN-SPAM and call it a day. Your EU recipients need GDPR-level treatment regardless of where your company is based. GDPR follows the recipient, not the sender.

In practice, most senders with any EU audience end up building to GDPR standards across the board. It's simpler to run one consent-based list than to segment by geography and apply different rules to each group. (And honestly, consent-based lists tend to perform better anyway.)

If you're unsure whether your current signup process and suppression practices actually satisfy both frameworks, that's worth a real look. The consent rules vary by country more than most senders realize, and the EU isn't the only region with strict opt-in requirements.

How do GDPR and CAN-SPAM differ in enforcement?

The core difference is whether you need permission to send. **GDPR** is opt-in: you can't send marketing email to an EU resident without prior explicit consent. **CAN-SPAM** is opt-out: you can send to anyone as long as you include accurate sender info, a physical address, a non-deceptive subject line, and a working unsubscribe that you honor within 10 business days. That philosophical difference shapes everything else.

Penalties reflect the different philosophies. GDPR fines can reach €20 million or 4% of global annual revenue. Amounts designed to sting even multinationals. CAN-SPAM caps at around $53,088 per email, significant but survivable for large companies.

GDPR also imposes obligations that CAN-SPAM doesn't: individual rights beyond unsubscribe (access to data, deletion, portability), documentation requirements, data protection officers for many organizations, and breach notification. CAN-SPAM has none of these.

For any program with EU recipients, GDPR is the operative standard. Start there, and the rest of your compliance picture becomes clearer.

THE EU AND EEA: GDPR

These answers cover who GDPR reaches, what counts as consent, and what happens when it goes wrong.

Who does GDPR apply to?

Here's what catches US businesses off guard: GDPR applies based on where your subscribers are, not where your company is based. If you have EU residents on your email list, you're subject to GDPR. Doesn't matter if you've never set foot in Europe.

The regulation applies to **data controllers** (the organization deciding what data to collect and why. That's you) and **data processors** (organizations processing data on your behalf, like your ESP). If you're using Mailchimp to send to EU subscribers, both you and Mailchimp have GDPR obligations, though different ones. Your ESP typically handles their side through a Data Processing Agreement.

In practice: if you can't guarantee you have zero EU subscribers, treat GDPR as applicable. Most email lists pick up EU addresses over time, especially if you publish content anyone can find or sell to international customers. The safer default is treating GDPR as the standard, not hoping it doesn't apply.

GDPR has also become something of a global reference point. California, Canada, Brazil, and other regions have their own privacy laws that borrow heavily from the same principles. Building your consent practices around GDPR standards usually means you're well-positioned for most of them.

Not sure if GDPR applies to your specific setup? We can help you figure that out. Free call, no pitch.

What constitutes valid consent under GDPR?

Valid GDPR consent, defined in Article 4(11) and Article 7, requires four cumulative conditions: a freely given, specific, informed, and unambiguous indication of the data subject's wishes via a clear affirmative action. Pre-ticked boxes, silence, or inactivity fail (per Recital 32). Bundled purposes fail specificity. Vague disclosures fail the informed test. Making service access conditional on marketing consent fails the freely-given test. If any one condition fails, the consent is invalid.

Under GDPR, consent isn't just a checked box. It has four specific requirements, and if any one of them fails, the whole thing fails.

Affirmative action. The subscriber has to do something positive: check an unchecked box, click an opt-in button, type their address into a clearly-labeled subscription form. Pre-ticked checkboxes, silence, and inactivity don't qualify. They have to choose yes, not merely fail to choose no.

Specific and granular. Consent for marketing emails is separate from consent for data sharing with partners, and separate from consent for profiling. A bundled "agree to all" isn't valid when multiple purposes are involved. Subscribers should be able to say yes to your newsletter without saying yes to everything else you might want to do with their data.

Informed. Subscribers need to understand who will email them, what they'll send, and roughly how often. Vague language like "occasional updates from our partners" doesn't meet the standard. Clear, specific language does.

Freely given. You can't make access to your core service conditional on accepting marketing consent. If someone has to tick the marketing box to create an account, it's not freely given.

These four conditions work together. A consent that passes three and fails one is still invalid.

What is an "affirmative action" in opt-in?

An affirmative action in opt-in is a deliberate, unambiguous step the subscriber takes to signal consent: ticking an unchecked box, clicking a subscribe button, or submitting an email address into a form. GDPR Article 4(11) requires a clear affirmative act and explicitly disqualifies silence, pre-ticked boxes, and bundled consent (where agreeing to terms of service also subscribes the user to marketing). The default state must always be unsubscribed.

Affirmative action in opt-in means the subscriber has to actively do something to say yes. Check an unchecked box. Click a subscribe button. Fill in their email and hit submit. The key word is *actively*. Consent can't come from silence, inaction, or a pre-selected option they never chose to tick.

GDPR spells this out clearly: consent must involve a "clear affirmative act" and can't be obtained through silence, pre-ticked boxes, or inactivity. That standard has shaped signup practices globally, even in places without identical legal requirements.

A few patterns that fail the affirmative action test:

- Pre-checked subscription boxes the user has to uncheck to opt out
- Bundled consent where agreeing to terms of service automatically adds someone to your marketing list
- Any signup flow where "opted in" is the default outcome unless the user takes extra steps

For your signup forms, this means the subscription should never happen unless the user explicitly made it happen. Marketing consent should be separate from other required actions like creating an account or completing a purchase. If someone ended up on your list without choosing to be there, you don't have valid consent. You have a compliance risk waiting to surface.

What is pre-checked box compliance status under GDPR?

Pre-checked consent boxes are non-compliant under GDPR. Article 7 and Recital 32 require consent through a clear affirmative act, which silence, inactivity, and pre-ticked boxes explicitly fail. The Court of Justice of the EU confirmed this in the Planet49 ruling (October 2019), holding that a pre-selected checkbox cannot establish valid consent for marketing. Subscribers gathered this way need a fresh opt-in via a consent refresh campaign before further sending.

Imagine you're building a signup form and you think: "I'll just pre-check the newsletter box. Anyone who doesn't want it can uncheck it." Under GDPR, that reasoning fails the legal test entirely.

GDPR Article 7 and Recital 32 require that consent be given through a "clear affirmative act." Silence, pre-ticked boxes, and inactivity don't count. The Court of Justice of the EU confirmed this in the Planet49 ruling (2019), making it clear that a pre-checked box can't establish valid consent for marketing communications.

The problem isn't just legal: pre-checked boxes make it impossible to know who actually wanted to subscribe vs. who simply missed the checkbox. GDPR's consent framework is built on deliberate choice. Pre-checked boxes flip that on its head by making opt-in the default rather than the decision.

If you've already collected subscribers through pre-checked boxes, that consent is almost certainly invalid under GDPR. You'd need to run a consent refresh campaign before continuing to email those contacts. Many ESPs now flag or block pre-checked mechanisms outright.

These aren't a gray area. They're a clear violation. If you're unsure whether your signup forms are compliant, we're happy to take a look at reviewmyemails.com/sos.

What are the penalties for GDPR violations?

> GDPR penalties follow a two-tier structure under Article 83. Tier 1 violations (poor record-keeping, late breach notification, missing data processing agreements) cap at €10 million or 2% of global annual turnover, whichever is higher. Tier 2 violations (consent failures, ignoring data subject rights, unlawful international transfers) cap at €20 million or 4% of global turnover. Data Protection Authorities weigh response speed, self-reporting, and actual harm, so most enforcement lands well below ceilings.

GDPR penalties are real, and they're designed to hurt even the biggest players. The regulation uses a **two-tier fine structure** with hard ceilings that scale with company size.

Tier 1 (less serious violations) covers things like poor record-keeping, failing to notify a breach on time, or not having a data processing agreement in place. Fines here go up to **€10 million or 2% of global annual turnover**, whichever is higher.

Tier 2 (more serious violations) covers consent failures, ignoring data subject rights, and unlawful data transfers. These fines go up to **€20 million or 4% of global annual turnover**, whichever is higher.

For a company the size of Google or Amazon, 4% of turnover runs into the billions. For a small business, even a low-end fine can be genuinely damaging. That said, most real-world enforcement actions land well below the ceilings. Data Protection Authorities (DPAs) consider factors like how quickly you responded, whether you self-reported, and how much actual harm occurred.

Beyond the fine itself, there's the surrounding fallout. Regulatory investigations take time and cost legal fees. Public enforcement decisions are published (yes, people read them). Affected individuals can bring private claims on top of any DPA action. The full cost of a violation is almost always higher than the headline fine.

For email marketers specifically, the highest-risk areas are consent practices and how you handle unsubscribe requests and deletion. If you're collecting email addresses from EU residents and you can't clearly show when, how, and why they opted in, you're exposed to Tier 2.

One honest note: GDPR compliance is a legal question, not just a technical one. We can point you toward what to check, but if you're uncertain about your specific situation, a qualified data protection professional is worth talking to.

But if you want to start somewhere practical, check that your email marketing setup has proper consent records, a clear unsubscribe path, and a data processing agreement with your ESP. Those three things cover the most common enforcement triggers. Not sure where to start? We're happy to talk it through at our SOS line.

How to design preference centers for compliance (opt-down vs opt-out)?

Start with the legal floor. Under CAN-SPAM, unsubscribe has to work within ten business days, using no more than a single page and an email address. Under GDPR, pulling consent has to be as easy as giving it. If either of those isn't true on your page, nothing else matters.

For GDPR jurisdictions, split consent by purpose. Checkboxes start unchecked. Label each purpose in plain language ("product emails," "promotions," "research invites"). No bundled consent. Store the timestamp, source, and IP with every choice so you can prove consent later.

THE UNITED KINGDOM: PECR AND UK GDPR

The UK row has two exceptions worth reading closely, one for your own customers and one for company addresses.

What is soft opt-in under EU law?

> Soft opt-in is a narrow exception under the EU ePrivacy Directive (implemented in the UK as PECR) that lets a business email existing customers about similar products without prior explicit consent, provided four conditions are met: the address was collected during a sale or negotiation of a sale, the promotion covers the sender's own similar products, the recipient was offered a clear opt-out at collection, and every subsequent message includes an easy unsubscribe.

Most EU email laws require explicit consent before you can send marketing emails. But there's a carve-out for existing customers, and it's called soft opt-in.

Soft opt-in lets you email a customer about similar products if four conditions are all met: you collected their contact during a sale or service negotiation, you're promoting your own similar products or services (not partner offerings, not unrelated products), you gave them a clear chance to opt out when you first collected their address, and you include an easy opt-out in every subsequent message.

The word "similar" does real work here. Someone who bought running shoes can reasonably expect to hear about other footwear. Emailing them about your new financial products stretches the exception well past its intent. The connection between what they purchased and what you're promoting has to be obvious, not explained.

Soft opt-in exists because the law (the **ePrivacy** Directive, implemented in the UK as **PECR**) recognized that requiring fresh consent after every transaction creates unnecessary friction. But it's a narrow exception for genuine customer follow-up, not a general license to email your entire customer base. The GDPR still applies to how you handle that data.

Not sure your customer emails qualify? The SOS call is free and we can walk through your specific situation.

What does PECR say about business emails?

The **Privacy and Electronic Communications Regulations (PECR)** in the UK create a distinction between corporate and individual subscribers.

Corporate subscribers: Companies, partnerships, government bodies, and other non-individual entities. You can send unsolicited **marketing email** to corporate subscriber addresses without prior consent. Examples: **info@company.co.uk**, **sales@company.co.uk**.

Individual subscribers: Sole traders, individuals, and partnerships (in Scotland). These require consent before receiving **marketing email**, similar to **B2C** rules.

The critical question: is the email address clearly corporate (**enquiries@business.com**) or does it identify an individual (**john.smith@business.com**)? Named email addresses at businesses are still considered individual subscribers under **PECR**.

Even where **PECR** permits unsolicited email, senders must still:

- Identify themselves
- Provide valid contact details
- Offer opt-out mechanisms
- Comply with **GDPR** for any personal data processing

PECR permissions don't override **mailbox provider** filtering. Legal email can still land in spam.

THE UNITED STATES: CAN-SPAM

Read the requirements and the common misconceptions together.

What are the main requirements of CAN-SPAM?

CAN-SPAM is the US law governing commercial email. It follows an opt-out model, which means you can send without prior consent. But you have to meet these requirements every time.

Accurate header information. Your From name, sending address, and routing information must honestly identify who's sending. Spoofed or misleading headers violate the law, and they're also a fast path to blocklists.

Non-deceptive subject lines. The subject has to match the content. "Your order has shipped" for a promotional email with no actual order is a violation. This sounds obvious until you see how often promotional emails dress up as transactional ones.

Advertisement identification. Commercial emails need to be identifiable as advertising, though the law gives you flexibility in how you do that. No specific language is mandated.

Valid physical postal address. Every commercial email needs a real postal address. Street address, PO Box registered with USPS, or a private mailbox at a commercial mail facility. Virtual addresses that receive mail qualify. Fake ones don't.

Clear unsubscribe mechanism. Easy to find and use. No fees, no login required, no more than one step. The link must stay functional for at least 30 days after sending.

Honor opt-out requests within 10 business days. Once someone unsubscribes, you have 10 business days to stop sending. You can't add them back to a different list or sell their address.

How quickly must unsubscribe requests be honored under CAN-SPAM?

CAN-SPAM gives you 10 business days to process an unsubscribe request and stop sending commercial email to that address. After that window, sending to them violates federal law.

The law also requires your unsubscribe mechanism to stay functional for at least 30 days after you send the email. If someone opens your campaign three weeks later and clicks unsubscribe, the link still has to work. Broken links don't excuse late processing.

Once someone unsubscribes, there are additional constraints: you can't charge a fee, require them to log in, ask for information beyond their email address, or add them back to a different list. You can't route them to a survey first. One step, and they're done.

The 10-day window is a legal ceiling, not a target. Most modern ESPs handle unsubscribes in real time. If yours doesn't, or if you're sending through a custom setup, suppression needs to happen before your next send. People who unsubscribe and then receive another email immediately will file spam complaints. That hurts your deliverability faster than a regulatory penalty.

If your unsubscribe process is broken or delayed, fix it now. The SOS call is free and we can help you diagnose what's going wrong.

What are the penalties for CAN-SPAM violations?

CAN-SPAM violations carry civil penalties of up to $53,088 per non-compliant email (inflation-adjusted from the original $16,000 statutory amount), with each individual message counting as a separate violation. The FTC, state attorneys general, and ISPs can all bring enforcement actions, and liability extends to both the sender and the company whose products are promoted. Aggravated conduct (false header information, dictionary attacks, botnet relays) adds criminal penalties including imprisonment under 18 U.S.C. 1037.

You've heard that CAN-SPAM violations carry fines of "up to $50,000 per email." The actual figure is $53,088 per non-compliant email (adjusted for inflation from the original $16,000), and since each individual email in a campaign can be a separate violation, a single send to a large list can create enormous theoretical liability.

The FTC, state attorneys general, and internet service providers can all bring enforcement actions. Both the company whose products are being promoted and the email sender can be held liable. So if you hire a marketing agency that sends non-compliant email on your behalf, you're exposed too. Not just them.

Aggravated violations carry additional criminal penalties: using false identities to send, hijacking computers to send spam, or harvesting email addresses through automated means can result in fines and imprisonment.

That said: regulators tend to go after systematic violators, not senders making good-faith compliance mistakes. The penalty calculus also includes the fact that enforcement catches relatively few violations. The more immediate risk for most senders is deliverability damage. Spam complaints tank your sender reputation faster than regulatory action shows up.

For anything more involved, the SOS call is free.

What are common misconceptions about CAN-SPAM?

Three things that many senders get wrong about CAN-SPAM.

Misconception: B2B emails are exempt. They're not. **CAN-SPAM** applies to all commercial electronic messages regardless of whether you're emailing a consumer or a business. Same requirements apply: accurate headers, non-deceptive subject lines, a physical address, and a working unsubscribe. No B2B exception exists.

Misconception: You need consent before you can email someone. Under **CAN-SPAM**, you don't. It's an opt-out framework. You can send commercial email without prior permission, as long as you identify who you are, give them a way out, and honor opt-out requests within 10 days. This is what separates CAN-SPAM from GDPR and CASL, which both require consent before sending.

Misconception: CAN-SPAM compliance means your email will reach the inbox. It won't, necessarily. Mailbox providers like Gmail and Microsoft Outlook enforce standards far stricter than what **CAN-SPAM** requires. Engagement rates, authentication (SPF/DKIM/DMARC), and list quality matter far more for inbox placement than **CAN-SPAM** checkboxes.

CAN-SPAM sets the legal floor, not the practical ceiling. Meeting minimum requirements while ignoring deliverability gives you a legally compliant program that lands in spam.

CALIFORNIA: CCPA

California asks a different question from the laws above. It is about what you do with the data, not whether you may send.

What is the CCPA (California Consumer Privacy Act)?

Say you sell software and someone in California signs up for your list. The **CCPA** (California Consumer Privacy Act, effective 2020) gives that person rights over their personal information: the right to know what you've collected, the right to delete it, and the right to opt out of its sale. Unlike **GDPR** or **CASL**, **CCPA** doesn't require consent to send email. It governs what you do with the data.

The practical impact on email programs: a deletion request under **CCPA** means actually deleting the data, not just suppressing the address.

How does CCPA affect email marketing?

> CCPA (and its CPRA amendment) doesn't restrict sending email to Californians, but it gives California residents rights over the subscriber data you hold: access requests, deletion requests (true deletion, not just suppression), and opt-out of sale or sharing. Practical impacts include adding a Do Not Sell or Share My Personal Information link if you share data with ad networks, disclosing data categories and recipients in your privacy notice, and routing deletion requests to actually purge records.

CCPA doesn't regulate whether you can send email. What it does is give California residents rights over the data you hold on them. If someone asks what you've collected, you tell them. If they ask you to delete it, you delete it, not just suppress their address. Those are two different things, and confusing them is one of the most common compliance gaps in email programs.

If you **sell or share personal information** with advertising partners, including email addresses, **CCPA** requires a "Do Not Sell or Share My Personal Information" link. Under **CCPA**/CPRA, sharing data with ad networks for cross-context behavioral advertising can count as "selling" even when no money changes hands. This affects data practices common in email marketing: list sharing, co-registration, and retargeting audiences built from your subscriber data.

Privacy notices must disclose what categories of personal information you collect, why, and which third parties receive them. California residents can't be penalized (denied service or charged different prices) for exercising their **CCPA** rights.

CANADA: CASL

Start with who and what CASL covers, then the two kinds of consent, then what every email has to carry.

Who does CASL apply to?

> CASL applies to any commercial electronic message (CEM) sent to, accessed in, or routed through Canada, based on recipient location rather than sender location. A US or EU company emailing a Canadian subscriber falls under CASL just as a Canadian company would. The law covers any message encouraging participation in commercial activity (newsletters, promotions, brand awareness with commercial intent), with narrow exemptions for transactional messages, employment communications, inquiry responses, and personal-relationship messages.

CASL (Canada's Anti-Spam Legislation) applies based on where your recipients are, not where your company is. If a Canadian receives your commercial email, CASL applies to that send, regardless of whether you've ever done business in Canada or visited the country.

The law covers **commercial electronic messages (CEMs)**: any message that encourages participation in commercial activity. This is intentionally broad. A newsletter promoting your services qualifies. A promotional email about a sale qualifies. Even brand awareness emails that don't sell anything directly can qualify if they could reasonably encourage a transaction. The test is about commercial intent, not explicit selling.

Some messages are exempt: purely transactional messages (order confirmations, account notifications), employment-related messages to employees, responses to inquiries, and messages within personal relationships. But these exemptions are narrow, and most commercial email to Canadian addresses requires CASL compliance.

The practical implication for most senders: if you can't confirm your list has no Canadian addresses, treat CASL as applicable. Unlike GDPR, which requires documented opt-in, CASL at least has implied consent provisions for existing customers. But those expire, and if you can't prove you have consent, you're likely violating the law.

What is “commercial electronic message” (CEM) under CASL?

A commercial electronic message (CEM) under CASL is any electronic message (email, SMS, or certain social media direct messages) where one of its purposes is to encourage participation in a commercial activity, such as promoting a product, service, business, or investment. For mixed content, CASL applies a primary purpose test based on what a reasonable person would conclude. Exemptions include requested quotes, warranty and safety notices, and certain existing-business-relationship communications. Violations reach $10 million CAD per incident for businesses.

Under **CASL**, a **commercial electronic message (CEM)** is any electronic message (email, SMS, or certain social media messages) that encourages participation in a commercial activity. The test: is the message's purpose, or one of its purposes, to promote a product, service, business, or investment opportunity? If yes, it's a CEM and you need **CASL** consent before you send it.

When a message has both commercial and non-commercial content, **CASL** uses a **primary purpose test**. Ask what a reasonable person would conclude the message's main goal is. A newsletter with genuine educational content and one product mention is probably not a CEM. A newsletter where the educational framing is clearly cover for a sales pitch probably is, regardless of what you call it.

Some messages are explicitly exempt from CEM classification: quotes or estimates the recipient requested, warranty or safety information, and certain communications between parties with an existing business relationship. Getting the classification wrong can cost up to $10 million CAD per violation for businesses.

If you're unsure whether a specific message is a CEM, assume it is and get proper CASL consent before sending. It's much easier to have consent you didn't technically need than to defend a message you assumed wasn't a CEM.

What type of consent is required under CASL (implied vs. express)?

CASL (Canada's Anti-Spam Legislation) requires either express or implied consent before sending commercial electronic messages. Express consent is an explicit opt-in action (no pre-checked boxes) and does not expire until withdrawn. Implied consent is inferred from an existing business relationship and is time-limited: 24 months following a purchase, contract, or membership, or 6 months following an inquiry. Once the implied window closes, sending must stop unless consent has been converted to express.

Under CASL, you need either express or implied consent before sending commercial email to Canadians. The distinction matters a lot, because they have very different rules.

Express consent is explicit opt-in. The recipient took a positive action to agree to receive commercial messages. No pre-checked boxes, no passive acceptance. Express consent doesn't expire (until the person withdraws it), and it's the strongest legal footing you can have. It's what you're aiming for with every subscriber.

Implied consent is permission inferred from a relationship without an explicit opt-in. It comes in two forms. An **existing business relationship** (purchase, contract, membership within the past 2 years) gives you 24 months of implied consent. An **inquiry** (someone asked for information or a quote but didn't complete a transaction) gives you only 6 months.

The critical thing about implied consent: it expires. When the window closes, you need to stop sending unless you've converted to express consent in the meantime. This is why smart CASL programs run consent conversion campaigns well before the 24-month mark. Nudging customers to explicitly confirm they want to stay on your list.

If you're building a CASL-compliant program from scratch, treat express consent as the default and use implied consent as a short-term bridge for recent customers.

What information must be included in emails under CASL?

> CASL requires three elements in every commercial electronic message sent to Canadians: clear sender identification (your legal or business name, plus any party on whose behalf you're sending), contact information that stays valid for at least 60 days after sending (a mailing address plus a phone number, email address, or URL), and a functional unsubscribe mechanism processed within 10 business days. Missing any one element triggers non-compliance under sections 6(2)(a-c) of the Act.

Every commercial email you send to Canadians needs to include three things. Miss any one and you're out of compliance.

Clear sender identification. Your name (or your organization's name), and the name of anyone on whose behalf you're sending, if that's different. It's not enough to have a legitimate From address. Recipients need to be able to identify who is contacting them without having to dig.

Contact information valid for 60 days. A mailing address, plus at least one of: a telephone number, an email address, or a web address. This contact information needs to stay accurate for at least 60 days after sending. If someone tries to reach you through it in week seven and it's already stale, you're in violation. This is CASL's equivalent of CAN-SPAM's physical address requirement, but it's stricter: you need to provide a way to reach you, not just prove you exist.

A functional unsubscribe mechanism. Clear, prominent, and easy to use. No fees, no login required, nothing beyond providing an email address and unsubscribe preference. The mechanism must stay active for at least 60 days after sending, and you have 10 business days to process requests. That's slightly different from CAN-SPAM's 30-day link requirement and same 10-day processing window.

What are the penalties for CASL violations?

> CASL penalties run up to $1 million CAD per violation for individuals and $10 million CAD per violation for businesses, with each non-compliant email counting as a separate violation. The CRTC enforces the law and can hold directors and officers personally liable when they directed or authorized the violations. A dormant private right of action, if proclaimed in force, would let individuals sue for up to $200 per message received.

CASL has some of the steepest penalties of any email law in the world. Up to **$1 million CAD per violation for individuals** and **$10 million CAD per violation for businesses**. Each non-compliant email can be a separate violation. Do the math on a campaign to a mid-sized Canadian list and it gets alarming fast.

Directors and officers can be held personally liable if they directed, authorized, or participated in violations. Corporate structure doesn't fully protect you. If the company sent non-compliant emails and you were running the email program, your personal exposure is real.

The CRTC (Canada's telecommunications regulator) enforces CASL and has brought cases against both Canadian and international companies. Enforcement tends to focus on lack of consent, missing required information, and false or misleading content. There's also a private right of action provision, though it hasn't been activated yet, that would allow individuals to sue for up to $200 per violation.

The penalties are designed to make compliance cheaper than non-compliance. And they succeed. The good news: senders making good-faith compliance efforts and keeping proper consent records are not typically enforcement targets. The cases that get fined are systematic violators, not accidental ones.

If you're emailing Canadians and you're not sure where your CASL compliance stands, our SOS call is free and we can help you figure out the gaps before they become problems.

If you already work to GDPR, much of this will look familiar. These answers show where to check.

What is the scope of LGPD (Brazil)?

LGPD (Lei Geral de Proteção de Dados, Law 13,709/2018) applies in three territorial scenarios: the processing occurs in Brazil, the processing targets offering goods or services to people in Brazil, or the personal data was collected in Brazil. Your company's location is irrelevant. Email addresses qualify as personal data, and commercial email marketing has no exemption, so any list containing Brazilian subscribers brings the sender into scope as either controller or processor.

If you have any Brazilian subscribers, **LGPD** applies to you. Here's how the scope works.

LGPD covers personal data processing in three situations: the processing happens in Brazil, the processing aims to offer goods or services to people in Brazil, or the data was originally collected in Brazil. Your company's location doesn't matter. A US-based SaaS with Brazilian users is in scope.

"Personal data" means any information that relates to an identified or identifiable person. Email addresses qualify. "Processing" covers basically everything you do with data: collecting it, storing it, using it, sharing it, modifying it, deleting it. Sending a marketing email to a Brazilian subscriber involves multiple processing activities under **LGPD**.

LGPD applies to both data controllers (organizations that determine how data is processed) and data processors (organizations that process it on someone's behalf). Some processing is exempt: purely personal activities, journalistic or academic purposes, and public security uses. Commercial email marketing doesn't qualify for any exemption.

If you have Brazilian subscribers, assume **LGPD** applies and treat them the same way you'd treat EU subscribers under **GDPR**. Start by confirming you have a valid legal basis for processing their data, then check that your individual rights processes cover Brazilian contacts.

What are the key requirements of LGPD for email marketing?

Here's what you need in place to run an LGPD-compliant email marketing program.

Step 1: Establish a legal basis for processing. For email marketing, that's usually **consent** (the subscriber explicitly opted in) or **legitimate interest** (you have a documented, justifiable reason that doesn't override people's privacy interests). Consent is simpler to defend. Legitimate interest is more flexible than under **GDPR** but still requires a written balancing assessment. Pick one and document it.

Step 2: Be transparent. Your privacy notice needs to cover what personal data you collect, why you collect it, how it's used, and who it's shared with. It has to be accessible and written in plain language. When someone signs up, they should understand what they're agreeing to without reading a legal document.

Step 3: Honor individual rights. Brazilian subscribers can request access to their data, correction of errors, deletion, portability, information about third-party sharing, and revocation of consent. You need a process for handling those rights requests. If you're already managing **GDPR** rights requests, extend the same process to your Brazilian contacts.

Step 4: Secure the data and report breaches. Implement appropriate technical and organizational security measures. If a breach occurs that could affect individual rights, it must be reported to ANPD. Maintain records of your processing activities so you can demonstrate compliance if asked.

If you're already **GDPR**-compliant, most of this is familiar territory. The fastest path to **LGPD** compliance is auditing your existing processes and confirming they cover Brazilian subscribers. LGPD's consent standard is nearly identical to **GDPR**'s: free, informed, and unambiguous.

How does LGPD define consent?

> LGPD (Brazil's Lei Geral de Proteção de Dados, Law 13.709/2018) defines consent in Article 5, item XII as a free, informed, and unambiguous indication that the data subject agrees to processing of their personal data for a specific purpose. Consent must be a positive action (a ticked box or clicked button), not a pre-checked option or silence, and must be specific per purpose, documented, and withdrawable as easily as it was given. Sensitive data requires highlighted, explicit consent.

LGPD defines consent as a **free, informed, and unambiguous** indication of an individual's agreement to processing of their personal data for a specific purpose. This mirrors **GDPR**'s approach: consent has to be a positive action, not passive acceptance or a pre-selected option.

Each word carries weight. **Free** means given without coercion: you can't require consent as a condition of service when that consent isn't necessary for the service. **Informed** means the person understood what they agreed to. A clear explanation of who processes their data, what data, and for what purpose. **Unambiguous** requires a clear affirmative action: checking a box, clicking a button. Not merely failing to opt out.

People must be able to withdraw consent as easily as they gave it. You need to document and maintain proof of consent obtained. For sensitive personal data (health information, religious beliefs, genetic data), **LGPD** requires explicit, highlighted consent beyond the standard.

If you're already **GDPR**-compliant on consent, your **LGPD** consent records will likely hold up. Both require the same thing: freely given, specific, informed, unambiguous consent with a clear withdrawal path. Check your consent documentation practices and confirm they cover your Brazilian subscribers.

What rights do individuals have under LGPD?

> LGPD (Lei Geral de Proteção de Dados, Law 13.709/2018) grants Brazilian data subjects nine rights under Article 18: confirmation of processing, access to the data, correction of inaccurate or outdated records, anonymization or deletion of unnecessary or unlawfully processed data, portability in a structured format, deletion of data processed under consent, information about public and private entities the controller has shared data with, information about the option to refuse consent, and revocation of consent at any time.

Under LGPD, people in Brazil have a set of rights over their personal data. Here's what each one means for your email program.

Right to confirmation: People can ask whether you're processing their data at all. **Right to access:** They can get a copy of what you hold on them. **Right to correction:** They can ask you to fix incomplete, inaccurate, or outdated information. These three rights mean you need to know exactly what data you have and be able to retrieve it on request.

Right to anonymization, blocking, or deletion: Data that's unnecessary, excessive, or unlawfully processed can be anonymized or removed. **Right to portability:** People can receive their data in a structured format and transfer it to another provider. **Right to information about sharing:** They can ask which third parties have received their data. **Right to revoke consent:** They can withdraw consent at any time, and you must stop processing based on that consent.

Rights requests must be handled through **simplified procedures** and responded to within reasonable timeframes. You can't charge for responding except in cases of clearly excessive or unfounded requests. If you're already handling **GDPR** rights requests, the processes are similar enough that extending your existing workflow to Brazilian contacts is usually straightforward.

The most operationally important right for email marketers is consent revocation: when someone revokes it, you stop sending. Check that your consent documentation includes a clear trail for each Brazilian subscriber so you can handle revocation and deletion requests accurately.

The four Asia Pacific rows sit together here, starting with the overview.

What are the key email privacy laws in the APAC region?

> Key APAC email privacy laws are Australia's Spam Act 2003 (enforced by ACMA, requires express or inferred consent), Singapore's PDPA with its national Do Not Call Registry check requirement, Japan's Act on Regulation of Transmission of Specified Electronic Mail (opt-in for commercial messages), India's DPDP Act 2023 (consent, notice, purpose limitation), and South Korea's PIPA (explicit consent plus cross-border data transfer restrictions). Unlike CAN-SPAM's opt-out model, all five default to opt-in.

If your list has any APAC subscribers, you're likely dealing with multiple opt-in consent requirements. Unlike **CAN-SPAM**'s opt-out model, most APAC laws require permission before you send.

Australia's Spam Act 2003 is one of the strictest. It requires consent (express or inferred from a business relationship) before sending commercial messages, accurate sender identification, and a working unsubscribe. ACMA (Australian Communications and Media Authority) enforces it actively with significant penalties. **Singapore's PDPA** (Personal Data Protection Act) requires consent for marketing and makes senders check a national Do Not Call Registry before sending. **Japan's Act on Regulation of Transmission of Specified Electronic Mail** requires opt-in for most commercial email, with additional provisions for mobile messaging.

India's DPDP Act (Digital Personal Data Protection Act, 2023) creates consent requirements with notice, purpose limitation, and individual rights for personal data processing. **South Korea's PIPA** (Personal Information Protection Act) requires explicit consent and has strict rules on cross-border data transfers, which can affect how you use ESPs that process data outside Korea.

APAC laws differ in their specifics, but they all lean toward opt-in. The safe practical approach: treat your entire APAC list as requiring consent and don't assume any commercial relationship counts as permission without checking the specific law. Australia and South Korea are the ones most likely to generate enforcement action.

How does Australia's Spam Act compare?

> Australia's Spam Act 2003 sits between US CAN-SPAM and Canada's CASL: it requires consent before sending (like CASL) but allows inferred consent from existing business relationships or conspicuously published addresses, and unlike CASL that inferred consent does not expire. The law applies to any message with an Australian link (sent to, from, or via Australian infrastructure), and ACMA enforces it with penalties up to AUD 2.22 million per day for serious breaches.

Australia's Spam Act 2003 is tougher than the US approach but different from Canada's. If you're sending to Australian subscribers, it's worth understanding where it sits on the spectrum.

The key difference: Australia requires consent before you send. That's closer to Canada's CASL (which is strict) than to the US CAN-SPAM (which lets you send first and let people unsubscribe). You can get that consent two ways. **Express consent** means the subscriber actively agreed to hear from you. **Inferred consent** exists when there's an existing relationship or when someone's conduct suggests they'd want to hear from you (like publishing their email for business inquiries). Unlike CASL, Australian inferred consent doesn't expire. It persists as long as the relationship continues, though best practice is to get express consent when you can.

The law applies to messages with an "Australian link." That means messages sent to Australia, from Australia, or using Australian infrastructure. If you're mailing Australians, you've got an Australian link, and the rules apply to you.

Enforcement is real. The ACMA (Australian Communications and Media Authority) actively prosecutes violations with penalties up to $2.22 million AUD per day for serious breaches. Australia also partners with other countries on anti-spam enforcement, so violations tend to have international ripple effects.

Here's the practical side-by-side: CAN-SPAM (US) lets you email anyone and they opt out. CASL (Canada) requires permission before you send. Australia's Spam Act sits in the same consent-first camp as CASL but with more flexible inferred consent rules. If your Australian subscribers are on a permission-based list, you're likely compliant. If you bought or rented a list, you've probably violated the law. Start by auditing how you got your Australian addresses.

What are Asia-Pacific frameworks (Singapore, Japan, India)?

Three more countries to know if you're sending to APAC audiences.

Singapore's PDPA (Personal Data Protection Act) requires consent before you collect and use personal data for marketing. It also maintains a national **Do Not Call Registry**: if someone's number is registered, you can't message them even if you have other consent. Organizations in Singapore and those processing Singapore residents' data are both covered.

Japan's Act on Regulation of Transmission of Specified Electronic Mail requires opt-in consent for most commercial messages, with limited exceptions for existing business relationships. Japan also has specific rules for mobile messaging, and penalties can include criminal liability for individuals, not just corporate fines.

India's DPDP Act (Digital Personal Data Protection Act, 2023) requires consent for personal data processing with notice obligations, purpose limitation, and individual rights including access, correction, and erasure. The law is still developing implementing regulations, so some specifics are still being clarified. But the consent requirement is clear.

All three lean toward opt-in. If you're sending to any of these countries, treat them the same as Australia: don't send without consent, and don't assume a commercial relationship counts as permission without confirming what the specific law requires.

What are the key requirements under each?

> Key APAC requirements run country by country. Australia's Spam Act 2003 requires consent (express or inferred), sender identification, and a working unsubscribe, with ACMA penalties up to AUD 2.22 million per day. Singapore's PDPA mandates consent plus a Do Not Call Registry check before messaging. Japan's Act on Specified Electronic Mail requires opt-in consent and carries individual criminal liability. India's DPDP Act 2023 requires consented notice with access, correction, and erasure rights.

Here's what you actually need in place for each major APAC email law, by country.

Australia (Spam Act 2003): Consent (express or inferred from a business relationship) before sending, accurate sender identification, a working unsubscribe honored promptly, and no harvested lists. ACMA enforces aggressively. Penalties up to $2.22 million AUD per day for serious violations. Both the sender and the company whose products are advertised share liability.

Singapore (PDPA): Consent before collecting or using personal data for marketing. Check the Do Not Call Registry before any messaging, even if you have other consent. Document your consent records. Penalties up to $1 million SGD for organizations.

Japan (Act on Specified Electronic Mail): Opt-in consent for most commercial messages before sending. Preserve consent records. Specific rules apply for mobile messaging. Individual criminal liability is possible, not just corporate fines.

India (DPDP Act 2023): Consent with clear notice explaining the purpose. Subscribers have rights to access, correct, and erase their data. Implementing regulations are still being clarified. Default to strong consent practices until the specifics are finalized.

Across all APAC laws: document consent obtained, keep records of unsubscribe processing, and include clear sender identification. Most APAC laws hold both the sender and the company whose products are promoted jointly liable.

The pattern is consent-first, everywhere. If you can check the following, you're well-positioned: valid consent documented for each APAC contact, functional unsubscribe in every message, and clear sender identification. Start by auditing your APAC subscriber list for consent status, then verify your unsubscribe mechanism works across all channels you use to reach them.

The last answer puts the top fines from every region on this card side by side.

What are the penalties for non-compliance?

Email compliance penalties vary dramatically by jurisdiction. Here's what non-compliance can cost you.

GDPR: up to €20 million or 4% of global annual revenue, whichever is higher. **CASL**: up to $10 million CAD per violation for businesses. **CAN-SPAM**: up to $53,088 per email, with criminal penalties for aggravated violations (using false identities, hijacking computers to send spam). **LGPD**: up to 2% of Brazilian revenue, capped at 50 million reais per violation.

Australia: millions in AUD penalties for serious violations. **Singapore**: up to $1 million SGD for organizations. **Japan**: typically smaller fines but includes potential criminal liability for individuals. **India**: still being defined under the DPDP Act, but designed to be significant.

Beyond the direct fines: public enforcement actions damage brand reputation. In some jurisdictions, individuals can sue for statutory damages. Directors and officers can face personal liability. Corporate structure doesn't fully insulate founders or executives. And email delivery itself may be affected, since mailbox providers often act on compliance signals before regulators do.

Compliance is cheaper than the alternative at every scale. If you're not sure which laws apply to your program, start by identifying which jurisdictions your subscribers are in, then work backward to what each requires. Catching the gaps in your compliance coverage before a regulator does is always the better option.

The note under the card gives the deadlines. These answers explain the request itself.

What is a Subject Access Request (SAR) or Data Subject Access Request (DSAR)?

A Subject Access Request (SAR), also called a Data Subject Access Request (DSAR), is a formal request under GDPR Article 15 where an individual asks a data controller to disclose what personal data is held about them. The controller must confirm processing, provide a copy of the data, explain the lawful basis, list recipients, state retention periods, and respond within one calendar month of receipt (extendable by two months for complex cases) free of charge.

For email marketers, a SAR might look like: a subscriber emails you asking "what data do you have about me?" Or you receive a formal written request through your privacy inbox. Either way, it's a SAR, and the clock starts when you receive it.

How quickly do I need to respond to an SAR?

Under GDPR and UK GDPR (Article 12), you have one calendar month from receipt of a Subject Access Request to respond, not 30 business days. The deadline can be extended by up to two further months for complex or numerous requests, but you must notify the requester of the extension within the original month and explain why. CCPA gives 45 days, extendable by another 45 with written notice.

A subscriber emails you on a Monday morning: "I want to see all the data you hold on me." That's a Subject Access Request, and your clock starts the moment you receive it. Under **GDPR** and **UK GDPR**, you've got one calendar month to respond. Not 30 business days. One calendar month from the day the request lands.

You can extend that deadline by up to two more months if the request is complex or you've received several at once. The catch: you have to tell the requester about the extension within the original one-month window, with an explanation of why. Staying silent past month one is a violation even if the complexity is real. Under **CCPA**, you've got 45 days, extendable by another 45 with written notice to the requester.

The response itself is free in almost every case. If a request is genuinely unreasonable (like the same person sending one every week), you can charge a reasonable fee or refuse, but document your reasoning carefully because regulators set a high bar for what counts as excessive. Your response needs to include the personal data itself, why you hold it, how long you'll keep it, and who you've shared it with. Plain language, not legalese.

The practical challenge is that subscriber data lives across multiple systems: your ESP, your CRM, your analytics platform, possibly a data warehouse. Doing that archaeology for the first time under a one-month deadline is stressful. Knowing where your data lives before a request arrives is half the battle. Your data subject rights process should cover SARs as a specific, documented case with an assigned owner.

Start by mapping every system that holds subscriber data and running a mock SAR against yourself. Build a simple response template so you're not starting from scratch each time. That one-month window moves faster than it looks on paper.

How quickly must DSARs be answered?

Under GDPR, you have one month from receiving a Data Subject Access Request (DSAR) to respond. That clock starts the day you receive the request, not the day you verify their identity or the day you start compiling the data.

If the request is complex or you've received multiple requests from the same person at once, you can extend by up to two more months. But you need to tell them within the first month that you're taking more time and why. Missing that notification is treated as a breach of the one-month deadline.

You can ask the person to verify their identity before responding, and that's sensible. But the clock is still running while you do it. Build identity verification into your first response, not as a reason to delay starting the work.

Under UK GDPR the rules are the same. CCPA in California gives businesses 45 days with a possible 45-day extension. CASL doesn't have a formal DSAR framework in the same way, though prompt responses are still best practice.

READERS IN MORE THAN ONE COUNTRY, AND LISTS YOU DID NOT GATHER YOURSELF

Row a is a choice between two approaches. The second answer here covers a question the card cannot answer in one cell: whether permission moves with a list.

How can I manage compliance across different regions?

Two approaches, depending on how complex your list is.

Option 1 (simplest): Apply the strictest standard to everyone. That usually means **GDPR** or **CASL** requirements: explicit opt-in consent, thorough documentation, prompt individual rights handling, and all required disclosures. If you meet those standards for every subscriber, you automatically satisfy every less-strict jurisdiction. You won't be optimizing separately for US vs. Canadian vs. EU recipients, but you won't need to. This is the right call for most email programs that aren't operating at massive scale.

Option 2 (segmented): Apply jurisdiction-specific rules by geography. Tag subscribers by country or region at signup, then apply different rules: EU subscribers get **GDPR** treatment, Canadian subscribers get CASL treatment, US subscribers get **CAN-SPAM** treatment. This is more efficient if you're in a permissive jurisdiction sending mostly to US audiences, but it adds significant operational complexity. Your ESP and CRM both need to support geographic segmentation and rule application.

Either way, you need **detailed consent records** that satisfy the strictest documentation requirements, a process for handling rights requests across jurisdictions within their respective timeframes, and legal review before entering new high-volume markets.

Most email programs are better off with Option 1. The overhead of geographic segmentation only makes sense if the strictest standard would require dropping a significant percentage of your list. If you're not sure which you are, start with Option 1.

Can consent be transferred or inherited (e.g., list purchase)?

> Consent is not transferable or inheritable under GDPR (Article 7) or Canada's CASL. Permission was granted to a specific sender for a specific relationship, so purchased lists, rented lists, and lists acquired through M&A cannot legally be mailed as if the new sender holds consent. The compliant path after a corporate acquisition is a re-consent campaign from the original sender's domain, notifying subscribers of the change and requiring an affirmative opt-in to continue.

You just acquired a company. Their list has 50,000 subscribers. Can you start emailing it? The short answer is no, and the longer answer involves a lot of legal exposure.

Under **GDPR** and **CASL**, consent is not transferable. When someone subscribed to Company A's newsletter, they gave permission to Company A. That permission doesn't move to Company B, regardless of how the list was acquired. The consent was specific to the original sender, the original brand, the original relationship.

Purchased lists are worse. The people on those lists never agreed to hear from you at all. Their relationship was with whoever originally collected their address. Sending to them without consent violates GDPR (which can mean substantial fines), destroys your sender reputation quickly, and lands your domain on blocklists. Spam complaint rates on purchased lists are brutal.

Corporate acquisitions are more nuanced. If you acquire a company with a subscriber list, the safe path is a **re-consent campaign**: notify subscribers about the new ownership, explain what changes, and give them a clear option to stay or go. Some regulators require this explicitly. It's also just honest. Subscribers who stay after that notification are genuinely yours.

There's no shortcut to a quality list. The only addresses worth having are ones where someone specifically said yes to you. If you've acquired a list and you're not sure where you stand, book a free SOS call and we'll walk through your options. We won't tell you what you want to hear, but we'll tell you what's actually true.

PROVING WHEN AND HOW SOMEONE SIGNED UP

This is the record the row asks you to keep, as a list you can check your own system against.

What records must you keep to prove consent?

> Proving consent requires capturing, for every subscriber: the email address, signup timestamp with timezone, IP address at signup, source URL or form identifier, the exact consent language shown (including privacy policy version), and evidence of affirmative action like the checkbox or button click logged. Double opt-in adds the confirmation email timestamp, click timestamp, click IP, and token. Under GDPR Article 7(1), the controller must demonstrate consent, so retain these records for the life of the subscription plus the applicable limitations period.

If a regulator ever asks you to prove a subscriber consented, you need a paper trail that shows who opted in, when, from where, and what they agreed to. Without it, you can't prove you had permission to email them at all (and "they're on my list" won't cut it).

At minimum, capture these for every subscriber:

- Email address
- Timestamp of signup, including timezone
- IP address at signup
- Source URL or form identifier showing which page or widget they used
- The exact consent language they saw at the time, including the privacy policy version
- Evidence of affirmative action: the unchecked box they checked, the button click logged

If you're using double opt-in, also record the confirmation email timestamp, the click timestamp, the IP address of that click, and the specific token used. That creates an audit trail proving they confirmed from an address they actually control.

Keep these records for as long as the subscriber relationship is active, plus any legally required retention period after. Under GDPR, you hold personal data only as long as you have a legitimate reason. For consent records, that means keeping them until the subscriber is fully off your list and any limitations period has passed.

Most major ESPs capture some of this automatically. But not all of it. Check what your platform actually stores and whether you can export it. If you've never looked, now is a good time. Not sure what you're capturing? Our SOS line can help you map it out.

The law, the evidence and the trade-off, in that order.

Does GDPR require double opt-in?

No, GDPR does not explicitly require double opt-in. Articles 4(11) and 7 require that consent be freely given, specific, informed, unambiguous, and demonstrable, but they don't mandate a confirmation email as the mechanism. Single opt-in with a timestamped record of an unchecked box being ticked can satisfy the standard. Double opt-in is the practical default for EU senders because the confirmation click produces stronger evidentiary proof if a supervisory authority challenges consent.

No, GDPR doesn't explicitly require double opt-in. But there's a meaningful gap between what's technically required and what's actually smart.

GDPR requires **valid consent** and the ability to demonstrate it. It doesn't specify the mechanism. Single opt-in with proper documentation, a timestamped record of when someone checked an unchecked box, could technically satisfy GDPR's consent requirements. The regulation cares about the fact of consent, not the confirmation email.

That said, double opt-in creates significantly stronger evidence. The confirmation click proves three things at once: the email address is real and accessible, the person who controls it actively confirmed intent, and you have a timestamped record of both the original signup and the confirmation. If consent is ever challenged, that's a much easier position to defend.

Regulators haven't issued binding guidance making DOI mandatory, but enforcement patterns suggest preference for it as best practice. When fines can reach €20 million, the friction of a confirmation email looks like excellent risk insurance.

The practical answer: if you have EU subscribers, treat DOI as your default. It improves your consent records, filters out typos and bot signups, and gives you a cleaner list to start with. The short-term list growth hit is worth it.

Is DOI required by any laws?

No law explicitly requires double opt-in (DOI), but several consent regimes make it the safest defensible choice. German courts consistently require senders to prove consent if challenged, and DOI produces the cleanest evidence trail. GDPR Article 7 requires demonstrable consent, achievable with detailed single opt-in logs but easier to defend with a confirmation click. CASL mandates express consent in Canada. CAN-SPAM in the US requires no prior consent, only honored opt-outs.

Short answer: no law explicitly writes "you must use double opt-in" into its text. But several jurisdictions have consent standards that make double opt-in the safest practical choice.

Germany is the clearest example. German courts have consistently ruled that senders must prove consent if challenged, and DOI provides the most reliable evidence trail. The legal requirement isn't "use DOI." It's "be able to prove consent." DOI is just the cleanest way to do that. Sending to German subscribers without verifiable proof opens you to legal challenges and potential injunctions.

GDPR takes a similar approach. It doesn't name DOI specifically, but it requires that consent be demonstrable. A single opt-in signup can satisfy this if you keep detailed logs (IP address, timestamp, form version), but those records are harder to defend than a confirmation click from the actual inbox owner. DOI's verification step proves the email address belongs to the person who consented.

CASL in Canada requires express consent for commercial messages. DOI isn't mandatory, but it's strongly recommended. **CAN-SPAM** in the US doesn't require prior consent at all. You just have to honor opt-outs.

In practice, most sophisticated email programs use DOI regardless of legal minimums. It keeps spam complaints down, keeps your list clean, and gives you a defensible record if anyone ever asks. If you want to check how your current consent records hold up, our SOS line at reviewmyemails.com/sos is a good starting point.

What is double opt-in (DOI)?

> Double opt-in (DOI) is a list-building flow where a new subscriber submits their address, receives an automated confirmation email containing a unique verification link, and is added to the active list only after clicking that link. The unconfirmed state is held in a pending bucket and expires if never clicked. DOI produces a timestamped consent record for GDPR and CASL, filters out typos and fake addresses, and often loses somewhere from 10 to 40 percent of signups at the confirmation step, depending on your offer, your industry and your readers.

Someone signs up for your newsletter. Instead of going straight onto your list, they get an email with a confirmation link. They click it, and now they're in. That extra step is double opt-in, and it's the reason some lists are measurably cleaner than others from day one.

The confirmation email acts as a filter. Typos and fake addresses either bounce the confirmation or never click it, so they never make it onto your list. Most role accounts like `info@` never click either, though some get confirmed by whoever reads them. What you're left with is a set of addresses where someone actively verified access. That's a meaningful quality signal. Double opt-in lists tend to have lower bounce rates, higher engagement, and fewer spam complaints out of the gate, all of which strengthens your sender reputation with inbox providers over time.

From a compliance angle, double opt-in gives you strong footing under **GDPR**, **CASL**, and other consent-based frameworks. The confirmation email creates a timestamped record that the subscriber both provided their address and took deliberate action to confirm it. If you're sending into the EU or Canada, that documentation matters, and some senders in regulated industries treat DOI as the default rather than an option.

The tradeoff is drop-off at the confirmation step. Anywhere from 10 to 40 percent of people who sign up won't complete confirmation, whether they forgot, got distracted, or the confirmation email landed in spam. That range does not mean much on its own. How many confirm depends on your offer, your industry, the person and where they are in their journey with you, so read it as a rough guide, not a target. To minimize that leakage, send the confirmation within 60 seconds of signup, keep it short and clear, and consider a single follow-up reminder if they haven't confirmed within 24 hours.

If you're deciding between DOI and single opt-in, the cleaner list you get from DOI is usually worth the smaller size, especially if you're building for long-term deliverability rather than short-term volume. Most major ESPs, including Klaviyo, Mailchimp, and HubSpot, let you enable DOI at the form level. Turn it on, make sure your confirmation email renders well across clients, and watch your bounce rate over the next 60 days.

CANADIAN CONTACTS ON IMPLIED CONSENT

These answers show how the clock runs, and how to keep track of it across a whole list.

How long does implied consent last under CASL?

> Implied consent under CASL (Canada's Anti-Spam Legislation, S.C. 2010 c.23) lasts 24 months from the date of a purchase, contract, or paid membership, or 6 months from the date of an inquiry or quote request that did not result in a transaction. The clock runs continuously and cannot be reset by sending email. After expiration, the sender must stop mailing unless express consent (a documented explicit opt-in) was obtained in the interim.

You sold something to a Canadian customer 18 months ago. Under CASL, how much longer can you email them without asking permission? 6 more months. After that, your implied consent window closes.

Here's how the clock works. If someone made a purchase, signed a contract, or became a paying member, you get 24 months of implied consent from their last transaction. If someone only requested a quote or filled out an inquiry form but never bought anything, you get just 6 months. So a purchase window is much longer. An inquiry window is short.

When the clock runs out, you must stop emailing that contact unless you've converted them to express consent (explicit opt-in) in the meantime. And this is the important part: the clock doesn't pause. If you haven't gotten their documented agreement to keep receiving email by month 24 (or month 6), you can't send anything else. Not even a "please stay subscribed" message. Silence means stop.

Best practice is to start your conversion campaigns 3-4 months before expiration, when you still have time to engage them. Ask something straightforward like "Want to keep getting our emails?" Make it obvious they're choosing to stay. Log their response. That documented yes becomes express consent, which doesn't expire.

Is implied consent enough in Canada?

You made a sale last month, so you're safe to email that customer, right? In Canada, that depends on exactly when they bought, what they bought, and whether you're keeping track. **CASL** (Canada's Anti-Spam Legislation) is stricter than most people expect, and implied consent has an expiry date stamped right on it.

Here's how it actually works. CASL allows **implied consent** when a real business relationship exists, but only within defined windows:

- **Purchase, lease, or contract:** 24 months from the date of the transaction.
- **Inquiry or application:** 6 months from the date of the inquiry.
- **Membership in a club, association, or voluntary organization:** 24 months from when membership ends (as long as they haven't asked to be removed).

Once those windows close, implied consent is gone. You need express consent to keep sending, which means a clear, affirmative opt-in where the person knowingly agreed to receive your emails.

Not every business interaction qualifies either. A casual website visit? Not a qualifying interaction. Someone following you on social media? Also no. The relationship needs to be a real transaction or a direct inquiry about your products or services.

The practical problem: tracking this at scale.

This is where most Canadian senders get into trouble. Knowing the rule is one thing. Having a system that actually tracks the consent basis and date for each contact is another (and yes, that's the part regulators will ask about if it ever comes up).

And a workable approach looks like this:

- Store a "consent basis" field in your CRM or ESP for every contact. Values might be: express, implied-purchase, implied-inquiry.
- Store a "consent date" so you can calculate when the window closes.
- Set up an automated segment that flags contacts approaching their expiry, say 60 days out.
- Send a re-consent campaign before the window closes. Ask them to opt in properly. Keep it honest and low-pressure.
- If they don't respond, move them to a suppression list before the deadline hits.

That last step is the one most senders skip. Suppressing non-responders feels painful, but emailing a contact whose implied consent has expired is a compliance risk in Canada. The fines under CASL are not symbolic.

How long does consent last?

The answer depends on the type of consent you collected and which laws apply to your audience.

Explicit consent, where someone actively opted in, generally **lasts until the subscriber withdraws it**. When they unsubscribe, consent ends. There's no legal expiration clock running unless they leave. That said, a subscriber who opted in four years ago and hasn't opened anything in eighteen months isn't really on your list in any meaningful sense, legally valid consent aside.

CASL is stricter. It puts hard time limits on implicit consent (consent inferred from a transaction or relationship rather than an explicit opt-in): typically **24 months from the last transaction** for customer relationships, or **6 months from an inquiry**. After those windows close, you need explicit consent or you stop sending. CASL's limits apply when you're emailing Canadians regardless of where you're based.

Beyond legal timeframes, there's a practical reality: list decay happens whether consent is technically valid or not. Long-dormant subscribers eventually generate spam complaints that hurt your sender reputation, regardless of what they agreed to years ago.

Some senders run **consent refresh campaigns** periodically, asking long-term subscribers to confirm they still want to hear from you. You'll lose some names, but the ones who stay are the ones who actually open.

The way back belongs to the reader. These answers cover what that looks like and what stops an accidental re-add.

What happens if someone re-subscribes after opting out?

When someone re-subscribes after opting out, their new consent is valid as long as it came from them through a genuine opt-in action (filling in a sign-up form, ticking a subscription box at checkout, or replying to a labeled re-subscribe prompt). Your ESP must remove the address from the suppression list, log the new subscription event with timestamp and source, and retain the full history (original opt-in, unsubscribe, re-subscribe) for GDPR and CAN-SPAM audit purposes.

People change their minds. Someone who unsubscribed six months ago might genuinely want back on your list today. That's completely fine, and you can absolutely re-add them. You just need to do it the right way.

When a previously unsubscribed contact goes through a real opt-in process again, their new consent is valid and you can start sending to them. Think of it as a fresh start. The old opt-out doesn't block them forever. What matters is that the re-subscription came from *them*, not from you deciding they probably want to hear from you again.

Valid re-subscription looks like this: they found your sign-up form and filled it in, they checked a subscription box during checkout, or they replied to a clearly labeled re-subscribe prompt. Any of those work. What doesn't work is re-importing their address from a third-party source, assuming a purchase counts as consent, or finding their email somewhere else and adding them back without their knowledge. That's not re-subscription. That's just re-adding someone who opted out.

On the technical side, here's what your system needs to do when a valid re-subscription comes in:

- Remove the address from your active suppression list (or flag it as overridden by new consent)
- Log the new subscription event with a timestamp and source
- Keep the full history: original subscription, unsubscribe, and re-subscription all on record

That history matters. If questions come up later about whether you had permission to send, you want a clear record showing exactly when and how they opted back in. Some ESPs require manual confirmation before reactivating a suppressed address, which is actually a helpful safeguard against accidental re-enabling.

One thing worth considering: if you're operating under GDPR, CASL, or similar regulations, the re-subscription needs to meet the same consent standard as the original sign-up. In practice, that often means double opt-in for re-subscription is a smart move (it gives you cleaner evidence that the intent was real). Check what your specific legal obligations are for your audience's location.

The short version: yes, re-subscriptions are valid. Just make sure they're genuinely voluntary, properly documented, and processed through a real opt-in. If you're unsure whether your current setup handles re-subscription events correctly, our SOS hotline is free and we're happy to take a look with you.

What is a suppression list?

> A suppression list is the set of email addresses your sending system will never contact, functioning as a master override that blocks sends even when a suppressed address appears in a fresh import, purchased data, or CRM sync. It typically holds four categories: unsubscribes, hard bounces, spam complaints (recipients who hit the this-is-spam button), and manual removals. Honoring it is required under CAN-SPAM, GDPR, and CASL, and ESPs like Mailchimp, Klaviyo, and SendGrid maintain account-level suppression automatically.

Picture this: someone unsubscribes from your newsletter, and a week later you import a fresh list that happens to include their address. Do they get your next campaign? If you don't have a suppression list, the answer is yes. That's exactly the kind of mistake it prevents.

A **suppression list** is a set of email addresses your sending system will never contact, no matter what. It acts as a master override. Even if a suppressed address shows up in a new import, a purchased data set (not that you'd do that), or a synced CRM segment, the suppression check catches it before anything goes out.

Suppression lists typically hold four types of addresses. **Unsubscribes** are people who opted out through your unsubscribe mechanism. **Hard bounces** are addresses that permanently failed delivery. **Spam complaints** are addresses where the recipient hit the spam button. **Manual removals** are addresses you've added yourself for legal requests, customer service situations, or anything else that warrants it.

Keeping this list accurate isn't just good practice. CAN-SPAM, GDPR, CASL, and similar regulations all require you to honor opt-outs, and that means maintaining real suppression data. From a sender reputation standpoint, mailing people who've already complained or unsubscribed is one of the fastest ways to damage your standing with mailbox providers.

Your ESP almost certainly maintains its own suppression list for your account. Mailchimp, Klaviyo, Twilio SendGrid, and most others handle this automatically. But you should also keep your own master suppression file separately. If you ever switch platforms or run campaigns across multiple tools, your own copy is the only thing that helps ensure consistency across all of them.

One more thing worth knowing: some senders maintain global versus list-specific suppression. A global suppression stops all contact. A list-specific one only applies to a particular campaign type. For most compliance situations, global is the safer default.

If you're not sure whether your suppression data is clean or consistent across platforms, it's worth auditing. A messy suppression list is often the first thing that surfaces when deliverability goes sideways.

SOMEONE ASKS TO BE DELETED

Three words get mixed up here: delete, suppress and opt out. These answers separate them.

How to handle requests for deletion vs suppression?

> Handling deletion versus suppression means running them as two linked steps in the erasure workflow: delete the subscriber's profile data (name, behavioral history, preferences) from your ESP, CRM, and sub-processors, then add the email address alone to a suppression list so a future signup-form re-entry doesn't restart sending. Under GDPR Article 17, the suppression record is the lawful minimum retained specifically to honor the erasure, not marketing data.

Deletion and suppression aren't the same thing, and you often need both. This is one of the most common compliance mistakes email marketers make.

Deletion means removing a subscriber's personal data: their name, email, behavioral history, preferences. After deletion, they shouldn't have a profile anywhere in your stack.

Suppression means keeping the minimum data necessary to prevent you from contacting them again. Usually that's just their email address, stored in a list your ESP checks before every send.

Why you need suppression even after deletion: if you delete everything and they later resubscribe through your signup form, you'll email them again. Under GDPR and CAN-SPAM, that could be a compliance failure.

The correct workflow for an erasure request: delete the profile data, then add the email to a suppression list. The suppression record doesn't need personal data beyond the address. Many ESPs maintain this as a global unsubscribe list automatically.

A standard unsubscribe is different from an erasure. When someone unsubscribes, you suppress them from that list. You might still be able to contact them about transactional matters. An erasure request under GDPR's right to be forgotten is broader: they want to be gone entirely.

If you use multiple sub-processors, erasure requests need to cascade to those systems too. Check that your process covers all of them, not just your main ESP.

What is the right to erasure ("right to be forgotten")?

> The right to erasure, set out in GDPR Article 17 and often called the right to be forgotten, lets a data subject require a controller to delete personal data held about them within one month of the request. For email senders, correct compliance means deleting the profile and adding the address to a suppression list so future signups don't re-enroll them. Exceptions are narrow (legal obligation, contract performance, defense of legal claims), and any processors holding copies must be notified.

When someone asks you to delete their data under GDPR Article 17, they're exercising the right to erasure. It's sometimes called the "right to be forgotten," and for email marketers it's one of the most important data subject rights to understand correctly.

There's a nuance that trips people up: deleting and suppressing aren't the same thing, and you often need to do both.

If someone asks you to delete their data, you delete their profile: their name, email address, behavioral data, everything you hold on them. But if you delete without suppressing, there's nothing to prevent you from accidentally collecting their email again through a signup form and emailing them. That would be a compliance failure.

So the correct process is: delete the personal data and add the email address to a suppression list that prevents future contact. The suppression list doesn't need to store their full profile, just enough to prevent re-entry.

The right to erasure isn't absolute. You don't have to delete data if you have a legitimate reason to keep it, such as a legal obligation (like tax records), a contract that requires it, or where the data is necessary for legal claims. These exceptions are narrow and should be applied carefully.

You have one month to comply. When you do, you should notify any sub-processors who hold a copy of that person's data as well.

What's the difference between “unsubscribe” and “opt-out”?

> Unsubscribe and opt-out overlap in everyday usage but differ in scope. Unsubscribe describes ending a prior subscription relationship, the action of leaving a list someone joined, typically via a List-Unsubscribe header (RFC 8058) or footer link. Opt-out is broader regulatory language covering unsubscribes plus declining mail you never agreed to, objecting to data processing, or removal under CAN-SPAM, which permits sending until the recipient opts out rather than requiring upfront consent like GDPR.

You've probably used both words without thinking twice about it. "Hit unsubscribe" and "opt out" feel like the same thing, and in most day-to-day email marketing contexts, they are. But the distinction does matter when you're writing privacy policies, consent flows, or trying to figure out which compliance framework applies to you.

"Unsubscribe" refers to a specific action. Someone joined your list, and now they're leaving it. They click a link, visit a preference center, or reply asking to be removed. There was a prior subscription relationship, and they're ending it. The word implies a two-way agreement that one party is walking away from.

"Opt-out" is broader. It covers unsubscribing, but it also covers declining communications you never agreed to in the first place, objecting to how your data is being used, or requesting removal from a list you ended up on without actively signing up. That last scenario is exactly what CAN-SPAM was designed around. Under CAN-SPAM, you can email people commercially until they opt out, because the law doesn't require an upfront opt-in. So the regulation uses "opt-out" deliberately.

GDPR works differently. It requires consent before you send. When someone withdraws that consent, the regulation calls it "withdrawing consent" or exercising their "right to object," not just opting out. If you're processing email addresses under legitimate interest rather than explicit consent, a subscriber can object to that too. That's also a form of opting out, even though the person may have never clicked a subscribe button.

Where this gets practically important is in how you word things. Your privacy policy and consent records should match the framework you're actually operating under. If you're in the US, "opt-out" works. If you're working with EU contacts under GDPR, "withdraw consent" or "right to object" is more precise language for your documentation (even if your email footer still just says "unsubscribe").

In your actual email footer, just say "unsubscribe." It's what people recognize, it's what they click, and it does the job regardless of jurisdiction. The legal language lives in the privacy policy, not the footer link.

Either way, once someone asks to stop receiving your emails, the process is the same. Stop sending and add them to your suppression list. The word you use to describe it doesn't change what you're required to do.

An unsubscribe has to reach every flow and every system. The first answer covers automations, the second covers everything else.

How to prevent accidental resends after unsubscribes?

> Preventing accidental resends after unsubscribes requires three controls working together: real-time suppression sync (the unsubscribe webhook updates the suppression list immediately, not on an hourly or nightly batch), send-time consent checks at each individual email fire rather than only at flow entry, and explicit automation exits configured on every active sequence so an unsubscribe event yanks the contact out of all queued steps. Audit by unsubscribing a test address mid-sequence and confirming the next scheduled send drops.

Picture this: someone clicks unsubscribe from your welcome series on a Tuesday afternoon. By Thursday, they've received two more emails from the same flow. That's not a glitch. It's a gap in how your system handles suppression, and it happens more often than most senders realize.

The core problem is timing. An unsubscribe event and your email queue don't always talk to each other fast enough. Some platforms process suppression in batches rather than in real time. Others check consent only at the moment a contact enters a flow, not at the moment each individual email fires. So if someone unsubscribes while they're mid-sequence, every email already queued behind them can still go out.

Here's what you actually need to prevent this.

Real-time suppression sync. The unsubscribe event should trigger an immediate update to your suppression list, with no batch delay. If your ESP processes suppressions on a schedule (say, every hour or every night), that window is your risk zone. Check your platform's documentation or ask support directly how quickly an unsubscribe propagates.

Send-time consent checks, not just entry-time. This is the one that catches most senders off guard. Your automation might check whether someone is subscribed when they first enter a flow, then never check again. You want the system to verify consent status right before each individual email goes out, not just at the start. That way, an unsubscribe that happens between steps in a long sequence still stops the next email cold.

Automation exit triggers. Most modern platforms (like Klaviyo, ActiveCampaign, or Customer.io) let you set an exit condition on any flow: if a contact unsubscribes, they leave the automation immediately, and any queued messages for that contact get cancelled. If you haven't set this up, it's usually a one-time config change per flow, and it's worth doing now.

Queue purging for scheduled sends. Broadcast campaigns scheduled in advance are a separate risk. If you schedule a newsletter to go out next Monday and someone unsubscribes on Sunday, your ESP should automatically exclude them at send time. Most do this well, but it's worth confirming. Some older setups or third-party integrations generate a static send list at the time of scheduling, which means suppressions that happen after that snapshot don't apply. If your setup works that way, you need to refresh the audience right before send.

Test it before you trust it. The only way to know your suppression flow actually works is to test it. Create a test contact, enter it into a multi-step automation, trigger an unsubscribe mid-flow, and check whether subsequent emails stop. Takes ten minutes. Do it at least once per platform you use, and again after any significant platform update.

One accidental post-unsubscribe email can trigger a spam complaint (and in some jurisdictions, a legal obligation). It's worth treating suppression as infrastructure, not an afterthought.

But if you're not sure whether your suppression updates in real time, that's the first thing to check.

How must unsubscribe requests be processed (timing, confirmation)?

Unsubscribe requests must be honored within 10 business days under CAN-SPAM and CASL, and without unreasonable delay under GDPR (regulators interpret this as days, not weeks), but operational best practice is immediate processing to avoid spam complaints. Processing means adding the address to a global suppression list, canceling queued campaigns, halting automated sequences, and blocking silent re-adds from future CRM imports. A confirmation email is not required and is usually skipped.

Someone just clicked your unsubscribe link. What happens next matters more than most senders realize.

The legal timelines vary by regulation. **CAN-SPAM** gives you up to 10 business days to process opt-out requests. **CASL** matches that with a 10-business-day maximum. **GDPR** doesn't name a specific number of days, but regulators have consistently interpreted "without unreasonable delay" to mean days, not weeks. If you're sending to EU subscribers and waiting eight days to honor an unsubscribe, that's a compliance risk.

In practice, the regulatory ceiling doesn't matter much. Your real deadline is immediate. Every hour someone keeps receiving emails after they opted out is another hour they might report you as spam. ISPs notice that. Your sender reputation notices that.

Before the unsubscribe-from-all link, offer a preference center with real choices, like fewer emails or only some topics, and stick to what people pick. If the only choice you give is unsubscribe, people will unsubscribe, hit the spam button, or ignore you. What they pick in the preference center also tells you what they want, so learn from it.

What "processed" actually means

Removing someone from a single list isn't enough. When you process an unsubscribe, you need to do all of this. Add the address to your suppression list right away. Cancel any scheduled campaigns they're included in. Stop all automated sequences they're enrolled in. Make sure the suppression sticks, so if their address shows up in a future import or list sync, they don't get re-added silently.

That last point catches a lot of senders off guard. You import a refreshed CRM export next month, and suddenly an unsubscribed address is active again. Your ESP should block re-adds automatically, but it's worth checking that your suppression list is configured to work that way.

You also need to make sure the unsubscribe travels across every system that touches that address. Your primary ESP, your transactional email platform, any third-party tools with their own sending capabilities. A suppression that lives in only one system isn't really a suppression.

Confirmation pages vs. confirmation emails

And a confirmation page is good practice. Showing a clear "you've been removed" message reassures the person that it worked and reduces the chance they'll hit the spam button out of frustration.

Now a confirmation email is a different story. The person just asked you to stop emailing them. Sending them an email to confirm you've stopped is legally risky and, honestly, a bit tone-deaf. If you do send one (some senders argue it helps with re-subscribe rates), it must be purely informational. Nothing promotional. No discount codes. No "we'll miss you" upsell. Some regulations explicitly prohibit using the unsubscribe step as a marketing touchpoint.

The simpler move is a clean confirmation page, no email. It's less risk and just as effective.

If you're not sure whether your current unsubscribe flow is airtight, our SOS hotline is free and we'll walk through it with you.

YOUR ANSWERS

What this means *for your send*

YOUR SITUATION	DO THIS FIRST
Your list has readers in more than one country	Either apply the strictest rules (GDPR or CASL) to everyone, or split the list by country at signup and apply each country's rules. The first is simpler and fits most programs

YOUR SITUATION	DO THIS FIRST
You only have US-style opt-out on file, and you mail people in the EU, Canada or Brazil	The EU and Canada want consent before the first email, and Brazil wants a documented legal basis, usually consent. Meeting CAN-SPAM does not meet GDPR
You cannot show when and how someone signed up	From now on, keep for every signup: the address, the time and its time zone, the IP, the form or page, the exact words shown with the privacy policy version, and the tick or click itself. Under GDPR you must be able to show consent
You are choosing single or double opt-in	GDPR does not require double opt-in. Single opt-in with a timestamped record of the person ticking an unticked box can meet it. Double opt-in gives stronger proof if consent is ever challenged
Canadian contacts on implied consent	Check each clock: 24 months from a purchase, 6 months from an inquiry. Sending email does not reset it. Ask for express consent before it runs out
Someone unsubscribed and you want them back	Waiting does not refresh consent. Only they can opt in again, through a new signup. Keep a permanent suppression list so an upload never re-adds them
Someone asks to be deleted	An unsubscribe is not a deletion request. Keep the address on your suppression list to honor the opt-out, with only the address, the date and the reason. A deletion request is separate and has its own deadline
Your automations run off a different list from your campaigns	Sync unsubscribes at once, not hourly or nightly, check consent at each send rather than only when someone enters a flow, and make every flow exit on an unsubscribe

Worked *example*

Skipper Mako runs Pearl Diver Travel (`pearl-diver.example`) and emails past and future travellers in the US, Canada, Germany and Brazil. Skipper reads the Americas and Europe rows of the card. A Canadian who asked for a quote eight months ago and never booked is past the 6-month implied consent window, so Skipper does not mail them unless they opt in. The old German signup form had a pre-ticked box, which is not valid consent under GDPR. Skipper switches every form to an unticked box, starts keeping the signup records, and applies the GDPR rules to the whole list rather than running four sets of rules.

GLOSSARY

Words *used*

Consent

permission a reader gives a sender to receive commercial email. Its required form depends on the country

Opt-in and opt-out

asking first, or sending until someone says stop. Opt-out is the broader legal word for any way of saying no

Soft opt-in

the UK and EU exception for your own customers about similar products

Implied consent (CASL)

consent inferred from a purchase or inquiry, for a limited time

Double opt-in

a signup that only counts once the person clicks a confirmation link

Data access request (DSAR)

a person asking what data you hold about them

Suppression list

the addresses your sending system will never contact, even if they turn up in a new import

WHO WE ARE

About *Review My Emails*

You never opted in to this page, so feel free to leave. If you stay, here is who we are.

Review My Emails is email list cleaning and validation that tells you which addresses to keep, which to watch and which to stop sending to, and why.

Most checkers answer one question: does this address exist? We answer the next one: should you send to it? An address can be perfectly valid and still be quietly damaging your sender reputation. Valid is not safe.

Valid is not safe.

The company was founded in 2020 and is based in Bolton, United Kingdom. Our founder is Yanna-Torry Aspraki, an email deliverability specialist who has worked in deliverability since 2015.

WHAT THE APP DOES

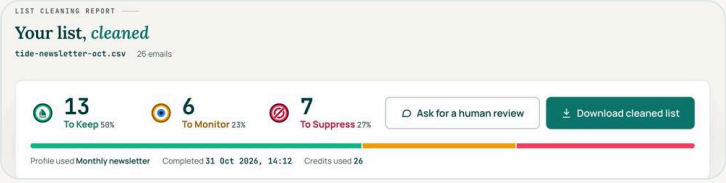
What the *app does*

You sign up, upload your list and get every address back with one decision and the reason, in plain English. Big lists take a while, so we email you when yours is ready.

To Keep. Send to it.

To Monitor. Send carefully and watch what happens.

To Suppress. Stop sending to it, and keep the record of who you stopped emailing.





We delete your list after 60 days, or sooner if you delete it yourself.

If you want a person to look, ask for a Human Review from your report, and Yanna-Torry goes through your list herself.

1,000

Your first 1,000 *are free*

Create an account and your first 1,000 addresses are free. No card is needed to sign up. After that you pay for the size of your list, from $0.0080 an address down to $0.0026 at volume, with an $8 minimum. There is no subscription and no monthly minimum.

What cleaning does not fix

List cleaning does not fix SPF, DMARC, MX or blocklist problems. Those live in your sending setup, and they are a different job. A blocklist listing measures your sending, so it is never a reason to suppress anyone on your list. And nobody can promise you the inbox, so we do not.

SOS

For those problems there is the Email SOS Hotline, our free help line. Tell Yanna-Torry what is going on and she will tell you what she would do. She reads every message herself and replies within 48 to 72 hours, with no pitch.

`reviewmyemails.com/sos`

The Email Almanac

Every explanation in this PDF comes from the Email Almanac, our own library of more than 4,000 answers about email. You do not have to buy anything to read it.

YOUR NEXT STEP

Clean your first 1,000 *addresses free*

Consent tells you that you may email someone. It does not tell you the address still works or is safe to send to. Once you know who gave you consent, upload the list and clean your first 1,000 addresses free at reviewmyemails.com/get-started. Cleaning never turns a list without consent into one with consent.

Questions about a send or where a list came from? Ask the free SOS line at reviewmyemails.com/sos. A real person answers, with no pitch.

reviewmyemails.com/get-started

Yanna-Torry Aspraki, Review My Emails