CONSENT AND THE LAW

Is cold email legal *where you send?*

Business email law, country by country

CONTENTS

What is *inside*

The 60-second answer	3
Country under review	4
Your plan	5
The card	5
What this means for your send	28
Worked example	30
Words used	30
About Review My Emails	31
Your next step	33

FOR:

anyone asked "are we even allowed to email these people?" about business contacts who never signed up. A shop owner, a sales lead, a new hire handed a list of buyers abroad.

The 60-second *answer*

1 **The law that counts is where your reader is, not where you are.**
A US company emailing a Canadian address falls under CASL, and a German address under GDPR.

2 **The US is the most permissive:**
no consent needed before the first email. Canada and Germany want consent first. The UK allows a company's general address, but not a named person's.

3 **A work address is not exempt.**
GDPR treats it as personal data that needs a lawful basis, and CAN-SPAM has no business exception either.

The US

No consent needed before the first email

The most permissive

Canada and Germany

Consent first

Not without it

The UK

A company's general address, not a named person's

It depends who

COUNTRY UNDER REVIEW

Cold email law, *under review.*

Find the row for each country on your list. The tag gives the card's answer to a first business email.

YES, NO CONSENT FIRST · IT DEPENDS · NOT WITHOUT CONSENT

EU and EEA GDPR, plus each country's own ePrivacy rules — IT DEPENDS

A FIRST BUSINESS EMAIL, ALLOWED?

It depends on the country. Each member state decides whether business email needs consent

Germany GDPR, plus Germany's own rules — NOT WITHOUT CONSENT

A FIRST BUSINESS EMAIL, ALLOWED?

Not without consent. Germany requires prior consent for business email

United Kingdom PECR, with UK GDPR — IT DEPENDS

A FIRST BUSINESS EMAIL, ALLOWED?

Yes to a company's general address, such as `info@`. A named person's address needs consent, even at a company

United States CAN-SPAM — YES, NO CONSENT FIRST

A FIRST BUSINESS EMAIL, ALLOWED?

Yes. No consent needed first. There is no business exemption, so every rule applies

Canada CASL — NOT WITHOUT CONSENT

A FIRST BUSINESS EMAIL, ALLOWED?

Not without consent. There is no general business exemption

Brazil LGPD — IT DEPENDS

A FIRST BUSINESS EMAIL, ALLOWED?

High risk to individuals without consent. Business contacts are treated more leniently in practice, but it is not a free pass

Australia Spam Act 2003 — NOT WITHOUT CONSENT

A FIRST BUSINESS EMAIL, ALLOWED?

Not without consent

Singapore, Japan, India PDPA, the Act on Specified Electronic Mail, the DPDP Act 2023

NOT WITHOUT CONSENT

A FIRST BUSINESS EMAIL, ALLOWED?

Not without consent. All three are opt-in

YOUR PLAN

Your countries, and *what each one asks*

YOUR READERS ARE IN	
THEIR ROWS	
A FIRST BUSINESS EMAIL, ALLOWED?	
WHAT EVERY MESSAGE MUST CARRY	
CHECKED WITH SOMEONE WHO PRACTISES EMAIL LAW	

THE CARD

The *card*

EU and EEA

LAW	GDPR, plus each country's own ePrivacy rules
A FIRST BUSINESS EMAIL, ALLOWED?	It depends on the country. Each member state decides whether business email needs consent
ON WHAT BASIS	A lawful basis under GDPR, such as legitimate interest, passed on three tests and written down before you send
WHAT EVERY MESSAGE MUST CARRY	Who you are, a clear opt-out in every message, and the ability to say where you got the address if asked. A privacy notice on first contact when the address did not come from the person
OPT-OUT DEADLINE	Without unreasonable delay, read as days, not weeks. A person can object at any time
TOP FINE	Up to €20 million or 4 percent of global turnover, whichever is higher

Germany

LAW	GDPR, plus Germany's own rules
A FIRST BUSINESS EMAIL, ALLOWED?	Not without consent. Germany requires prior consent for business email
ON WHAT BASIS	Prior consent. Regulators in Germany and France have pushed back hard on legitimate interest for cold email
WHAT EVERY MESSAGE MUST CARRY	As the EU row, since GDPR applies on top
OPT-OUT DEADLINE	As the EU row
TOP FINE	GDPR's, as the EU row. Fines under Germany's own rules are not in the Almanac yet

United Kingdom

LAW	PECR, with UK GDPR
A FIRST BUSINESS EMAIL, ALLOWED?	Yes to a company's general address, such as `info@`. A named person's address needs consent, even at a company
ON WHAT BASIS	Companies, LLPs and government bodies are corporate subscribers and need no consent first. Sole traders, private people and Scottish partnerships are individual subscribers and do
WHAT EVERY MESSAGE MUST CARRY	Who you are, valid contact details, a way to opt out, and UK GDPR for the data you hold
OPT-OUT DEADLINE	Not in the Almanac yet
TOP FINE	Not in the Almanac yet

United States

LAW	CAN-SPAM
A FIRST BUSINESS EMAIL, ALLOWED?	Yes. No consent needed first. There is no business exemption, so every rule applies
ON WHAT BASIS	Opt-out. You may send until someone says stop
WHAT EVERY MESSAGE MUST CARRY	Honest sender details, an honest subject line, a physical postal address, a working unsubscribe, and a clear note that it is an advertisement
OPT-OUT DEADLINE	10 business days, and the link must keep working for 30 days after the send
TOP FINE	Up to $53,088 per email, and each email can count as its own violation

Canada

LAW	CASL
A FIRST BUSINESS EMAIL, ALLOWED?	Not without consent. There is no general business exemption
ON WHAT BASIS	Express consent, which does not expire, or narrow implied consent: an existing business relationship (2 years), a purchase inquiry (6 months), or an address published openly and used for a message directly relevant to it
WHAT EVERY MESSAGE MUST CARRY	Your name or business name, a physical mailing address, a working unsubscribe, and contact details that keep working for 60 days after the send
OPT-OUT DEADLINE	10 business days
TOP FINE	Up to $10 million CAD per violation for a business, $1 million CAD for a person

Brazil

LAW	LGPD
A FIRST BUSINESS EMAIL, ALLOWED?	High risk to individuals without consent. Business contacts are treated more leniently in practice, but it is not a free pass
ON WHAT BASIS	A lawful basis, usually consent or legitimate interest
WHAT EVERY MESSAGE MUST CARRY	Not in the Almanac yet
OPT-OUT DEADLINE	Not in the Almanac yet
TOP FINE	Up to 2 percent of Brazilian revenue, capped at 50 million reais per violation

Australia

LAW	Spam Act 2003
A FIRST BUSINESS EMAIL, ALLOWED?	Not without consent
ON WHAT BASIS	Express consent, or consent inferred from an existing business relationship or an address published openly. Inferred consent does not expire. Harvested lists are not allowed
WHAT EVERY MESSAGE MUST CARRY	Accurate sender identification and a working unsubscribe
OPT-OUT DEADLINE	Honored promptly. A set number of days is not in the Almanac yet
TOP FINE	Up to AUD 2.22 million a day for serious breaches

Singapore, Japan, India

LAW	PDPA, the Act on Specified Electronic Mail, the DPDP Act 2023
A FIRST BUSINESS EMAIL, ALLOWED?	Not without consent. All three are opt-in
ON WHAT BASIS	Consent. Singapore adds a check of the national Do Not Call Registry. Japan has limited exceptions for existing business relationships
WHAT EVERY MESSAGE MUST CARRY	Clear sender identification, as with every law in the region
OPT-OUT DEADLINE	Not in the Almanac yet
TOP FINE	Singapore up to $1 million SGD for organisations. Japan can include criminal liability for individuals. India still being defined

Cold email here means email to someone who has had no contact with you and never opted in. This card answers whether that is allowed. It is not a guide to sending it.

One send can fall under several of these laws at once, because each reader is covered by the law where they are.

Emailing people who signed up? Marketing consent by country is on its own card, "Email consent laws compared".

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.

Consent does not transfer *with a sale.*

THE 60-SECOND ANSWER

The whole picture first, region by region, then the card row by row.

Is cold email legal?

> Cold email is legal in most countries, but the rules vary by jurisdiction. The US (CAN-SPAM) permits unsolicited commercial email if you include accurate sender details, an honest subject, a physical postal address, and a working unsubscribe link. The EU (GDPR plus ePrivacy) generally requires prior consent, with B2B legitimate-interest exceptions varying by member state. Canada (CASL) requires express or implied consent. UK PECR treats corporate and individual subscribers differently.

Short answer: yes, cold email is legal in most countries, but the rules vary a lot depending on where your recipients are. Getting this wrong isn't just a legal risk. It also tanks your deliverability.

Here's how the major frameworks break down.

United States (CAN-SPAM)

The US is the most permissive. You don't need prior consent to send a cold email. You do need accurate sender information, an honest subject line, a physical mailing address, and a working unsubscribe link. No deceptive tactics. That's it. It's a low bar compared to the rest of the world.

European Union (GDPR + ePrivacy Directive)

Now this is where it gets complicated. The EU generally requires consent before sending marketing to individuals. B2B cold email exists in a grey zone. Some member states allow it when you can show legitimate interest as your legal basis, meaning you have a genuine business reason to contact that specific person. This isn't a loophole you can abuse. You need to document it, and the contact's interests can override yours if there's no clear professional relevance.

Canada (CASL)

Canada's anti-spam law is one of the strictest in the world. You need express or implied consent before sending commercial electronic messages. Implied consent can apply if you've had a prior business relationship, but it has a time limit. When in doubt, treat Canada as an opt-in-required market.

Brazil (LGPD)

Brazil's Lei Geral de Proteção de Dados generally requires a legal basis for processing personal data, similar to GDPR. Sending cold email to individuals without consent is high-risk territory. B2B outreach to corporate contacts is treated more leniently in practice, but it's not a free pass.

One thing worth knowing: being legally compliant doesn't mean mailbox providers will deliver your email. Gmail, Outlook, and others filter based on how recipients actually behave with your emails. Low open rates, spam reports, and unengaged lists will hurt your sender reputation regardless of whether your legal boxes are ticked. Legal compliance is the floor, not the ceiling.

How do GDPR, CAN-SPAM, and CASL apply to cold email?

GDPR, CAN-SPAM, and CASL apply to cold email based on recipient location, not sender location. CAN-SPAM (US) permits cold sends without prior consent but requires honest headers, a physical postal address, and opt-out honored within 10 business days. GDPR (EU/EEA) requires a lawful basis (typically legitimate interest for B2B with a documented balancing test) for processing personal data. CASL (Canada) requires express or narrow implied consent before the first send, with penalties up to CAD 10 million per violation.

Three frameworks, three different philosophies. The tricky part: more than one might apply to your list at the same time.

CAN-SPAM (US) is the most permissive. It doesn't require prior consent for cold email, B2B or B2C. It does require honest sender identification, a physical mailing address, no deceptive subject lines, and an opt-out you honor within 10 business days. Fines per violation can exceed $50,000, but enforcement targets repeat offenders, not first-time mistakes.

GDPR (EU/EEA) doesn't regulate email directly. It regulates what you do with personal data. Cold emailing someone using their personal data (which includes most work email addresses) requires a lawful basis. For B2C outreach, that's effectively explicit consent. For B2B, "legitimate interest" can work, but you need a documented balancing test, a clear opt-out on every message, and the ability to explain where you got the address if asked. Segmenting your list by recipient region is often the practical answer here.

CASL (Canada) is the strictest. You need consent *before* sending, not just a way to opt out after. Express consent doesn't expire. Implied consent is narrow and time-limited, usually 2 years for an existing business relationship. After that, it expires and you can't send.

Here's how to figure out which rules apply to you: it's based on where your recipients are located, not where you send from. A US company emailing a Canadian address falls under CASL. The same company emailing a German address falls under GDPR. If your list is mixed, you're juggling all three simultaneously.

EU AND EEA

What are the six lawful bases under GDPR?

GDPR Article 6 defines six lawful bases for processing personal data: consent (freely given, specific, informed, unambiguous opt-in), contract (necessary to perform a contract, fits transactional email like order confirmations), legal obligation (required by law, such as tax records), vital interests (protecting someone's life), public task (government and public authorities), and legitimate interests (your interests outweigh privacy rights, documented via a Legitimate Interest Assessment, common for B2B cold outreach).

Before you process anyone's personal data under GDPR, you need a legal reason. GDPR defines six valid reasons, called lawful bases. Without one, the processing isn't allowed.

Here are the six, with honest notes on which apply to email marketing:

1. Consent: The person clearly agreed to you processing their data for a specific purpose. For marketing emails, this is the most common basis. It must be freely given, specific, informed, and unambiguous. Pre-checked boxes don't count. Silence doesn't count.

2. Contract: Processing is necessary to perform a contract. For transactional emails (order confirmations, account alerts), this is usually the right basis. Not for newsletters.

3. Legal obligation: You're required by law to process the data. Tax records, fraud prevention. Rarely applies to marketing.

4. Vital interests: Necessary to protect someone's life. Not relevant to commercial email.

5. Public task: For government bodies and public authorities. Not applicable to most senders.

6. Legitimate interests: Your interests in processing outweigh the individual's privacy rights. This is the basis most used for B2B cold email and some customer marketing. It requires a Legitimate Interest Assessment (LIA) to document the balancing test.

What is "legitimate interest" and how does it apply to B2B email?

> Legitimate interest is one of six lawful bases for processing personal data under GDPR Article 6(1)(f), allowing senders to process data without prior consent if they pass a three-part test: the purpose test (a specific, defined business interest), the necessity test (email is genuinely required to achieve it), and the balancing test (the recipient's rights and reasonable expectations don't override it). B2B senders must document this in a written Legitimate Interest Assessment before sending.

You've probably heard someone say "legitimate interest" like it's a magic phrase that makes cold email legal under GDPR. It isn't. It's a real lawful basis for processing personal data, but it comes with conditions that most senders don't fully think through.

Legitimate interest is one of six lawful bases for processing personal data under GDPR. Unlike consent, it doesn't require someone to actively opt in. That's why B2B senders reach for it. But "I want more customers" isn't a lawful basis on its own. You have to pass a three-part test first.

The purpose test. What specific interest are you pursuing? Business development can qualify, but it needs to be genuine and clearly defined. "Getting leads" is too vague. "Reaching procurement managers at mid-sized manufacturers who buy the type of software we sell" is closer to defensible.

The necessity test. Is emailing this person actually necessary to achieve that goal? Could you reach them another way? Regulators will ask this. If the answer is "not really," you've got a problem.

The balancing test. This is where most assessments fall apart. You have to weigh your interest against the individual's rights and reasonable expectations. If a professional receives an email that's directly relevant to their job, in a context they'd reasonably expect, the balance can tip in your favor. If it's irrelevant, frequent, or unexpected, it won't.

You're also required to document this reasoning in what's called a Legitimate Interest Assessment (LIA). Not a formality you fill in after the fact. An actual written analysis, done before you send.

For B2B email specifically, a few things work in your favor. Contacting someone at a business address about topics genuinely related to their professional role is more defensible than consumer outreach. Corporate email addresses usually carry lower privacy expectations than personal ones. And GDPR's recitals specifically acknowledge that legitimate interest can apply in a B2B context.

But a few things will sink you quickly. High sending volume, irrelevant content, no easy opt-out, and no record of your assessment are all red flags regulators look for. Recipients still have the right to object at any time, and you need to honor that without friction.

How do "consent" and "legitimate interest" differ in practice?

> Consent and legitimate interest differ in proof, durability, and applicable context under GDPR Article 6. Consent requires an affirmative opt-in with timestamped records of source and wording, and ends the moment the recipient withdraws. Legitimate interest requires a documented Legitimate Interest Assessment (LIA) balancing your purpose against the data subject's rights, doesn't expire, but must honor objections under Article 21 and generally holds up better for B2B prospecting and existing-customer mail than consumer marketing.

If you send marketing emails, you're almost certainly relying on one of these two lawful bases. Here's the practical difference between them.

Consent means the person has actively agreed to receive marketing from you. They opted in through a form, checked an unchecked box, or took some clear affirmative action. The upside: it's the clearest basis and hardest to challenge. The downside: once they withdraw consent, you have to stop. And you need to be able to prove they consented, which means timestamped records with the source and the exact wording they agreed to.

Legitimate interest means you've determined that your interest in sending the communication outweighs the individual's privacy rights, and you've documented that assessment. The upside: it doesn't expire the way consent can, and you don't need an opt-in for every person. The downside: it requires a Legitimate Interest Assessment (LIA), it doesn't override the right to object, and it's under more scrutiny in consumer contexts. It works better for B2B outreach than B2C marketing.

In practice: for consumer newsletters and marketing campaigns, consent is the safer choice. For B2B prospecting or existing customer communications, legitimate interest can work if you've done the LIA properly.

One common mistake: using legitimate interest because you can't get consent. Regulators have rejected this reasoning. Legitimate interest requires a genuine assessment of competing interests, not a workaround for bad consent rates.

How to document the chosen lawful basis?

> Documenting a lawful basis under GDPR means recording, before processing starts, the activity, the basis chosen (consent, legitimate interest, contract, etc.), the reasoning, and the decision date. Consent requires timestamp, source, exact wording agreed to, and the privacy notice version. Legitimate interest requires a written Legitimate Interest Assessment covering purpose, necessity, and balancing. All of this typically lives in your Records of Processing Activities (ROPA), mandated by GDPR Article 30.

Choosing your lawful basis isn't enough. You need to write it down before you start processing, and that documentation needs to hold up if a regulator ever asks to see it.

For each type of processing you do (sending marketing emails, tracking engagement, storing profile data, passing data to your CRM), you should record: the processing activity, the lawful basis you're relying on, why you chose that basis, and the date you made that decision.

If you're using consent, you need consent records too: timestamp, source, the exact wording the person agreed to, and the version of your privacy notice in effect at the time. Most ESPs can export this data, but check that yours does before you need it.

If you're using legitimate interest, you need a Legitimate Interest Assessment (LIA). This is a documented three-step test: purpose (what's your legitimate interest), necessity (is processing necessary for that purpose), and balancing (do your interests outweigh the individual's rights). The LIA should be a real document, not a one-liner.

This documentation typically lives in your Records of Processing Activities (ROPA), which GDPR Article 30 requires for organizations above 250 employees and in many other situations. Even if you're below that threshold, maintaining a ROPA is good practice and shows due diligence.

A simple starting point: document your three main email types (marketing, transactional, automated), the lawful basis for each, and where the consent or LIA records are stored. That covers most of what a regulator will ask for first.

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

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.

What are the penalties for non-compliance with anti-spam laws?

The numbers are real and the regulators do act. Let's go country by country so you know what you're actually risking.

United States (CAN-SPAM): Up to $53,088 per violation, and each individual email can count as a separate violation. The FTC enforces this, as do state attorneys general. In practice, the biggest CAN-SPAM cases involve senders who ignored opt-out requests or used deceptive headers, not senders who forgot a mailing address once.

European Union (GDPR): Up to €20 million or 4% of global annual turnover, whichever is higher. Enforcement has been active since 2018. Meta, Google, and LinkedIn have all faced nine-figure fines. For cold email specifically, the risk centers on not having a valid lawful basis for processing the contact's data.

Canada (CASL): Up to CAD $10 million per violation for businesses. CASL is widely considered the strictest anti-spam law in the world. It requires express or implied consent before sending, not after.

GERMANY

What laws apply to B2B cold email (EU, UK, US, Canada, Brazil)?

B2B cold email is governed by five distinct regimes: in the US, CAN-SPAM permits cold outreach with sender identification, a physical postal address, and a working opt-out (no prior consent required). The EU layers GDPR over the ePrivacy Directive, with member states like Germany requiring prior consent for B2B. The UK's PECR allows unsolicited mail to corporate subscribers but restricts named individuals. Canada's CASL requires consent (express or narrow implied) with no general B2B carveout. Brazil's LGPD requires a lawful basis, typically consent or legitimate interest.

You're planning B2B cold email across five major regions and the legal landscape looks like a patchwork. That's because it is. Here's what applies where.

United States. CAN-SPAM applies to all commercial email, B2B and B2C alike. No consent required, but you've got to follow the rules: identify yourself, include a physical address, and provide a way to opt out. It's an "opt-out" framework, which makes it the most permissive region on this list.

European Union. GDPR applies to any personal data processing. The ePrivacy Directive lets each member state decide if B2B email needs consent. Germany's strict about it. Others are more relaxed. So you've got both GDPR (universal) and member-state-specific ePrivacy rules to consider. This is genuinely the gray zone.

Canada. CASL (Canada's Anti-Spam Legislation) doesn't give B2B special treatment. All commercial messages need consent. There's limited wiggle room for "implied consent" if you're emailing a "conspicuous business contact" where the message relates to their professional role. That's narrow. CASL's the strictest on this list.

Brazil. LGPD (Lei Geral de Proteção de Dados) mirrors GDPR's structure. You need a lawful basis. That's either consent or "legitimate interest," similar to the EU approach. It's not as prescriptive as GDPR yet, but the direction's the same.

Real talk. Regional compliance is complex and varies based on your specific message, recipient role, and regional interpretation. This isn't legal advice. You need qualified legal counsel in your target regions before you launch. They'll map your exact situation to the rules and tell you what's defensible.

Next step. Write down which regions you're targeting and which job roles you're reaching out to. Take that to a compliance lawyer who specializes in email marketing.

UNITED KINGDOM

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.

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

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.

UNITED STATES

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.

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.

What are common misconceptions about CAN-SPAM?

Three misconceptions about CAN-SPAM dominate: that B2B email is exempt (it isn't, the Act covers all commercial electronic messages regardless of recipient type), that prior consent is required (it isn't, CAN-SPAM is an opt-out framework unlike GDPR or CASL, requiring only accurate headers, a physical postal address, and honoring unsubscribes within 10 business days), and that compliance guarantees inbox placement (it doesn't, since Gmail and Microsoft enforce reputation and authentication standards far beyond the legal floor).

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. (Just because cold email is legal doesn't mean it performs well.)

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.

CANADA

What are CASL restrictions on unsolicited messages?

CASL (Canada's Anti-Spam Legislation) prohibits sending a commercial electronic message to a Canadian address without prior consent, either express (explicit opt-in, no expiry) or implied (existing business relationship valid 2 years, purchase inquiry valid 6 months, or a conspicuously published address used in a directly relevant context). Every CEM must include sender identification, a physical mailing address, and an unsubscribe mechanism honored within 10 business days. Penalties reach $1M CAD for individuals and $10M CAD for organizations per violation.

If you're sending cold emails to Canadian addresses, CASL is the law that will catch you off guard. It's stricter than CAN-SPAM and stricter than most people expect.

The core rule: you need consent before sending a commercial electronic message (CEM). A CEM is any message that encourages participation in a commercial activity, which covers essentially all cold sales email.

Express consent means the recipient explicitly agreed to receive messages from you. It doesn't expire. **Implied consent** is narrower: it applies in specific circumstances like an existing business relationship (typically valid for 2 years), a purchase inquiry (valid for 6 months), and a publicly listed email address used in a directly relevant context. Once implied consent expires, you can't send.

Every message you send under CASL must include your full name or business name, a physical mailing address, and a working unsubscribe mechanism honored within 10 business days. These aren't optional.

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

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.

BRAZIL

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.

AUSTRALIA

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.

SINGAPORE, JAPAN, INDIA

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.

READING THE CARD

What is cold email?

Cold email is outreach to someone you've had no prior contact with. You're not replying to a conversation. You're starting one. The recipient didn't sign up for anything, doesn't know you, and has no existing relationship with your business.

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.

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

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.

What are data-broker transparency requirements under GDPR?

If you're buying contact data from a data broker to use in your email program, GDPR applies. And it creates obligations for both the broker and you. Understanding who is responsible for what matters before you start sending.

What data brokers must do under GDPR:

Data brokers are data controllers in their own right. That means they need a lawful basis to collect and sell personal data. Under Article 14 of GDPR, when a data broker collects information about someone through indirect means (not directly from the person), they must inform that person within one month of collection, or at the latest, when they first communicate with them, about what data they hold and how it's being used.

Individuals have the right to ask a broker where their data came from, what it's being used for, and to have it deleted. Brokers need to be able to answer these requests.

What you're responsible for as the buyer:

Buying data from a broker doesn't transfer GDPR responsibility to them. You're a data controller too, and you need your own lawful basis for the data you hold and the emails you send. "The broker said it was GDPR compliant" doesn't hold up to regulatory scrutiny if you can't demonstrate your own lawful basis.

Before using broker data for cold email under GDPR, ask: what lawful basis did the broker use to collect this, and does that lawful basis cover your use of it? Can the broker provide documentation? If they can't answer clearly, that's a risk signal.

What qualifies as “publicly available” contact info?

"It's publicly available" is one of the most frequently misused justifications in cold email. Here's where it actually holds up and where it doesn't.

Generally clearer territory: A contact page on a company's website with a listed email address. A press release with a named spokesperson's email. Government registry filings with director details. Professional directory listings where the person voluntarily published their information for business contact. These contexts share a common thread: the person put the information out there specifically for business contact purposes.

Legally murky territory: LinkedIn profile data is publicly visible to other users, but LinkedIn's Terms of Service prohibit scraping it, and automated extraction often violates both ToS and relevant data laws. Social media profiles are similar. Just because something is visible to the public doesn't mean it's available for commercial use. The legal analysis depends on how you collected it and whether the person had a reasonable expectation of contact.

Under GDPR: "Publicly available" isn't a lawful basis on its own. You still need a legal ground to process the data and to send to the person. Legitimate interest may apply in B2B contexts, but only after a documented balancing test. The data being public is just one factor.

The practical question to ask yourself: would this person be surprised to receive an email from you, given where you found their address? If yes, you're probably in murkier territory regardless of how the data was technically accessible.

How to legally process scraped or enriched contact data?

The short answer is that data being public doesn't make it legal to use for email marketing. GDPR requires you to have a lawful basis before processing anyone's data, regardless of where you found it. In the US, CAN-SPAM is less strict about the source, but it still has compliance rules once you start sending.

The real risks with scraped data. Scraping LinkedIn, company websites, or other platforms often violates their terms of service. It can also run afoul of computer fraud laws. The platform tracks scrapers and sometimes pursues legal action. Even if you buy from a broker, you inherit the risk that their scraping was illegal or unauthorized.

What documentation actually matters. Keep records showing where your data came from and how you sourced it. Write down your legitimate interest assessment if that's your legal basis. Be prepared to explain your sourcing if a contact requests it (they have that right under GDPR). If someone asks you to delete their data, do it promptly. This isn't legal advice, but these records are your protection if things go sideways.

Do B2B senders not need consent?

No, B2B senders are not exempt from consent rules. GDPR treats work addresses as personal data and requires a lawful basis (consent or documented legitimate interests) for EU recipients. CASL requires express or implied consent for any Canadian commercial email, B2B included, with implied consent expiring after a set window. CAN-SPAM in the US permits cold outreach without prior consent but still mandates honest identification and a working unsubscribe.

A lot of B2B senders assume that emailing a work address is somehow exempt from consent rules. It's one of the most common misconceptions in email marketing, and it can get you into real trouble.

The short answer is no, B2B doesn't get a free pass. GDPR covers individuals at companies just as much as it covers consumers. If you're emailing someone at their work address in the EU, you need a lawful basis for doing so. Consent is one option, but so is "legitimate interests" (which means you need a documented reason that genuinely holds up, not just "we want their business").

CASL, Canada's anti-spam law, requires either express or implied consent before you send commercial email to anyone, B2B included. Implied consent exists when there's a prior business relationship, like a recent inquiry or purchase, but it has a time limit and it expires. CAN-SPAM in the US is the most permissive of the three, but it still requires a functioning unsubscribe and honest sender identification. It doesn't require prior consent, which is why so many US-based cold outreach tools cite it, but CAN-SPAM compliance doesn't protect you if your recipients are in the EU or Canada.

A few places do treat B2B more leniently than B2C. The UK's PECR regulation, for example, allows unsolicited email to corporate addresses (not personal ones) in some cases. But "more lenient" is not the same as "anything goes."

There's also a practical argument here, separate from legality. Even where cold B2B outreach is technically allowed, it drives complaints, spam reports, and low engagement. Those signals hurt your sender reputation whether or not you broke a law. Cold outreach still counts as email in the eyes of a spam filter, and filters don't care about your jurisdiction.

So what does good B2B consent actually look like in practice? A few approaches that hold up:

- **Event-based consent:** Someone attends a webinar or downloads a resource and checks a box agreeing to future emails. That's clean, documented consent.
- **Direct opt-in:** A prospect fills out a contact form or signs up for updates. Simple and solid.
- **Implied consent from a business relationship:** You've had a recent commercial exchange. Under CASL this lasts two years from the date of the transaction. Under GDPR it still needs legitimate interest documentation.
- **LinkedIn or event connections:** Meeting someone at a conference doesn't automatically grant email permission. It gives you a reason to reach out once and ask if they'd like to hear from you. That's it.

Whatever your source, document it. If someone files a complaint, "I found their address online" is not a defense. "They filled out our contact form on March 4th" is.

SOMEONE SAYS STOP

How to handle unsubscribe requests in cold outreach?

Handling unsubscribe requests in cold outreach means processing them same-day to a shared suppression list, even though CAN-SPAM allows 10 business days and GDPR effectively requires immediate action. Make opt-out one click with no login or reason-capture form, sync the suppression list across every sending tool (CRM, sequencer, bulk sender) so a removed contact cannot re-enter via a parallel sequence, and log the request timestamp and processing time for audit evidence.

Someone asked to be removed. The law says you have 10 business days (under CAN-SPAM). Best practice says same day. The gap between those two is where sender reputation quietly erodes.

Here's how to set this up properly:

Make opting out frictionless. One click, no login, no "tell us why" form before the removal completes. Any friction here is both a CAN-SPAM violation risk and a complaint waiting to happen. Under GDPR, the standard is effectively immediate.

Add every opt-out to a suppression list immediately. Not a "do not contact" spreadsheet you check manually. A suppression list that your sending tool checks before every send. If you're running campaigns across multiple tools or sequences, that suppression list needs to be shared across all of them, not siloed per campaign.

Keep records. Log when the request came in and when you processed it. If you ever face a complaint or audit, that timestamp is your evidence.

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

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.

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.

What happens when you lose your lawful basis?

> When you lose your lawful basis under GDPR (consent withdrawn via unsubscribe, or a successful Article 21 objection to legitimate interests), you must stop the dependent processing immediately. Practically: halt marketing sends to that address, check whether a separate basis covers retention (legitimate interest justifies keeping the address on a suppression list), delete profile data with no remaining purpose, and notify any third-party processors under Article 19 so downstream systems align.

A subscriber hits unsubscribe. Or they send a formal objection to your marketing emails. Either way, the legal permission that let you contact them is gone. So what happens next?

Under **GDPR**, every piece of data processing needs a lawful basis to be valid. When that basis disappears, you can't just keep going. You need to stop the processing activity that depended on it.

For most email marketers, this comes up in two situations. First, **consent withdrawal**: someone unsubscribes, and if consent was your only basis for sending marketing emails to them, you're done. You can't market to that address anymore. Second, **a legitimate interests objection**: a subscriber formally objects to your processing, and you can't show a compelling reason that overrides their objection. Same result. Stop.

Stopping the emails is just the first step. Here's what you actually need to do when a lawful basis falls away:

- **Stop the processing activity** right away. No more marketing emails to that address.
- **Check if another basis applies.** For example, you can keep an address on a suppression list (the basis there is legitimate interest in not re-contacting someone who opted out). That's different from marketing, and it's valid.
- **Delete data that no longer has a purpose.** If you held profile data only for marketing and that permission is gone, you may need to delete it.
- **Tell any third parties.** If you've shared that contact's data with another processor, you need to inform them of the change so they adjust their own processing.
- **Update your records.** Your consent and processing logs should reflect the change, including the date and what triggered it.

IT IS LEGAL WHERE YOUR READER IS, SO YOU THINK IT IS SAFE

What is the risk of using your main domain for cold campaigns?

Your main domain is your business's identity online. It handles password resets, invoices, support replies, and every campaign you send to subscribers who opted in. Cold outreach puts all of that at risk.

The core danger is reputation spillover. Cold campaigns generate higher complaint rates and more bounces than warm sends. That damage doesn't stay contained. It drags down your sender reputation for everything sent from that domain, including transactional mail your customers actually need.

A blocklist hit is the worst case. Delisting takes time, isn't always fully successful, and can shut down your entire email program while you wait. Even without a blocklist event, accumulated negative signals quietly push more mail into spam over time.

YOUR ANSWERS

What this means *for your send*

YOUR SITUATION	WHAT THE LAW SAYS
Your readers are in more than one country	Each reader brings their own country's law, so check the row for every place on your list. The approach most cautious senders take is to meet the strictest rules for everyone

YOUR SITUATION	WHAT THE LAW SAYS
You are counting on legitimate interest in the EU or UK	It is not a magic phrase. It needs a purpose test, a necessity test and a balancing test, written down before you send, and the person can object at any time. Regulators have rejected it as a workaround when consent is hard to get
The list was bought, or the seller says it is compliant	Consent does not transfer with a sale. You need your own lawful basis, and the seller's claim does not move the liability to them. Under GDPR and CASL, a purchase cannot establish consent or legitimate interest
The addresses were scraped, or found "in public"	Public is not a lawful basis under GDPR. Scraping LinkedIn breaks its terms and can risk computer fraud laws in the US. Harvesting addresses by automated means can bring criminal penalties under CAN-SPAM
The address belongs to a named person, not a role like `info@`	In the UK a named address is an individual subscriber and needs consent, even at a company. Under GDPR a named work address is personal data and needs a lawful basis
Someone says stop	Honor it within the deadline for their row. Taking someone out of one campaign while another still emails them is a violation. Re-adding people who unsubscribed gets you in trouble even where business email is allowed
It is legal where your reader is, so you think it is safe	Legal is not the same as safe. Unsolicited email brings legal exposure, deliverability damage and harm to your domain's reputation that lasts months after the sending stops. Sent from your main domain, it drags down everything else that domain sends, invoices and password resets included
Someone else sends for you	Both the sender and the company whose products are promoted can be held liable under CAN-SPAM. Most Asia Pacific laws hold both jointly liable too

Worked *example*

Gil Brinewater runs Brinewater Brewing (`brinewater.example`). A new sales hire brings Gil a list of bar buyers in the UK, Germany, Canada and the US, bought from a directory, and asks if they may email them. Gil reads the card. In Germany and Canada the answer is no without consent. In the UK, a bar's general `info@` address at a limited company is a corporate subscriber, but a named manager, or a bar run by a sole trader, needs consent. The US allows a first email with the rules in its row, but the list was bought, and consent does not transfer with a sale. Two rows of "What this means for your send" settle it: the bought list, and legal is not the same as safe. The same domain sends Brinewater's invoices, and unsolicited mail would drag down all of it. The list stays unused. The hire puts a sign-up box at the next trade event instead, where buyers who tick it give documented consent.

GLOSSARY

Words *used*

Cold email
email to someone who has had no contact with you and never opted in

Lawful basis
the legal reason GDPR asks for before you use anyone's personal data. There are six, consent and legitimate interest among them

Legitimate interest
a lawful basis that needs no opt-in, only a written three-part test showing your reason outweighs the person's rights

Corporate and individual subscriber
the UK split between a company's general address and a named person or sole trader

Implied consent (CASL)
consent Canada infers from a business relationship, an inquiry or an openly published address, for a limited time

Opt-out
the legal word for any way of saying no, including declining mail you never agreed to

Privacy notice (Article 14)
the GDPR notice owed on first contact when you got someone's data from somewhere else

WHO WE ARE

About *Review My Emails*

This one is not a cold introduction. You came to us, so 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

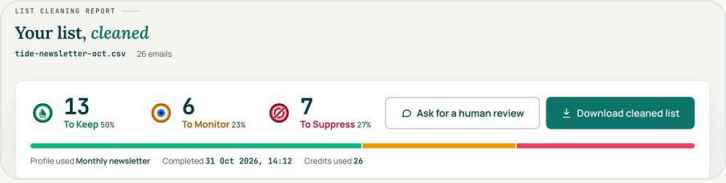
What the *app does*

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

Not sure about a list? Ask, *free*

Cleaning a list never makes an unsolicited list lawful. It can tell you an address works, never that you may email it.

Emailing people who did sign up? The consent card shows what each country asks for: Email consent laws compared, at reviewmyemails.com/resources/email-consent-laws-compared.

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/sos

Yanna-Torry Aspraki, Review My Emails