

The Outbound Sequence Compliance Cookbook

How to build outbound email and LinkedIn sequences that respect CAN-SPAM, work with CASL and GDPR-style rules, honour suppression, and log every reply in the CRM, with AI drafting kept under human review.

Contents

01 Start with who may be contacted

02 What CAN-SPAM requires of every email in a sequence

03 Suppression lists: one list, checked twice

04 Message structure and cadence that earn replies without pressure

05 Reply handling and CRM logging

06 AI-assisted drafting with a human gate

07 Build checklist

Key Takeaways & Sources

01

Start with who may be contacted

Before anyone writes a subject line, decide what list the sequence is allowed to touch. The rules differ by where the recipient is, and the person doing the targeting is usually the one who knows least about them. The US CAN-SPAM Act sets an opt-out model: you may send commercial email without prior permission, provided you follow the content and opt-out rules. Canada's anti-spam law (CASL) is built on consent, either express or implied under specific conditions, and it covers commercial electronic messages generally. Under the EU and UK regimes, rules on electronic marketing sit alongside data protection law, which asks for a lawful basis for processing personal data; GDPR Article 6 lists the bases, and legitimate interest is one of them. The UK Information Commissioner's Office publishes separate guidance on direct marketing and electronic communications.

We are not lawyers and this cookbook is not legal advice. What it can do is show where the decisions sit. Whether a given prospect in Ontario, Germany or the UK can be emailed cold, and on what basis, depends on facts about the recipient and the message, and on rules that change. The practical step is to have counsel write a short regional policy: which countries you contact, which basis you rely on in each, and what must be recorded. Then build that policy into the enrolment rules of the tool, so a rep cannot add a contact from an excluded region.

Record the source of every contact. If a prospect asks "how did you get my address?", the answer should be one field away: where the data came from, when, and on what basis you are contacting them. A list with no provenance is a list you should not be sequencing against.

- Define permitted regions and the basis you rely on in each, in writing, with counsel
- Block enrolment for contacts in regions outside that policy
- Store source, date and basis on the contact record
- Review the policy when you enter a new market or add a new data provider

The practical step is to have counsel write a short regional policy: which countries you contact, which basis you rely on in each, and what must be recorded.

02

What CAN-SPAM requires of every email in a sequence

The FTC's compliance guide sets out the requirements, and each one applies to every step in a sequence, not only the first. Do not use false or misleading header information, including the From name, reply-to address and routing. Do not use a deceptive subject line. Identify the message as an advertisement where that is not otherwise clear. Include a valid physical postal address. Give a clear, conspicuous way to opt out. Honour opt-out requests within ten business days, and do not charge a fee, require more than an email address or make the person do more than reply or visit a single page to opt out.

Two operational consequences follow. The first is that the opt-out has to work across the whole sequence and across every tool. If a contact unsubscribes from step two, the tool must stop steps three and four, and your other platforms must also know. The second is that outsourcing does not move the liability. The FTC guide states that a company whose product is promoted in a message, and the company that sends it, can both be responsible. If you use an agency, a data vendor or a lead-gen partner to send for you, the contract should say how opt-outs are shared and who checks them, and you should test it.

Mailbox provider rules sit on top of the statute. Google's sender guidelines require senders of more than 5,000 messages a day to Gmail accounts to authenticate their mail, support one-click unsubscribe for marketing messages, and keep spam rates low. Other mailbox providers publish their own rules. See the email authentication and deliverability playbook for the technical setup. A compliant sequence that gets complained about will still be blocked, so low-volume, well-targeted sending is the safer design for both the law and the inbox.

The first is that the opt-out has to work across the whole sequence and across every tool.

03

Suppression lists: one list, checked twice

A suppression list is the set of addresses and people you must not contact: unsubscribes, complaints, hard bounces, do-not-contact requests, existing customers where sales has a separate relationship, competitors, and anyone a legal or contractual rule excludes. A common failure is not that a list is missing, but that there are several, held in different tools, and none of them agree.

The design that avoids this is simple to state. Keep one master suppression list in the system of record, usually the CRM. Sync it to every sending tool and sequencing platform, and sync changes back from them, so that an unsubscribe in one place becomes a suppression everywhere. Check the list at two moments: when a contact is enrolled, and again before each scheduled step goes out, because the

contact may have opted out, replied or become a customer in between. Match on email address and, where you have it, on person, because the same individual may have two addresses. A suppression record should hold the reason, the date and the source, and should never be deleted when someone asks you to stop contacting them, because the record is what lets you keep that promise. Where privacy law gives someone the right to erasure, take counsel's advice on keeping a minimal suppression entry for exactly that reason.

Suppression reason	Source of the signal	Action
Unsubscribe request	Link or one-click header, or a reply asking to stop	Suppress across all tools immediately; confirm within the legal time limit
Spam complaint	Feedback loop or mailbox provider report	Suppress and review the source of that contact
Hard bounce	Sending tool bounce data	Suppress the address; check for a better one only through a legitimate source
Do not contact	Reply by email or phone, or a LinkedIn message	Log as a manual suppression with the date and what was said
Active customer or open deal	CRM lifecycle stage or deal status	Pause outbound; route to the account owner
Excluded region or role	Contact record fields	Block at enrolment

04

Message structure and cadence that earn replies without pressure

A short cold message does four things: says who you are and why this person, offers one specific reason to talk, makes the ask small, and gives an easy way out. The reason to talk has to be true and checkable. A line like "I saw you hired three SDRs this quarter" is fine if it came from a public job board; it is a problem if a model invented it. Do not use a fake "Re:" or "Fwd:" subject line, a made-up prior conversation or a countdown that does not exist; apart from being deceptive under CAN-SPAM rules on subject lines, these tricks are what draw complaints.

On cadence, we do not have a primary source that says how many touches or how many days apart is best, and the figures in many sales blogs are single-vendor claims. Our recommendation is a judgement: a short sequence, with several days between touches, mixed across email and LinkedIn only where you have a real reason for both, and a hard stop. Four to six touches over three to four weeks is a reasonable starting point to test, not a proven optimum. Whatever you choose, write it down, apply it consistently and measure your own reply, unsubscribe and complaint rates by sequence. If the unsubscribe or complaint rate rises, shorten or stop the sequence before changing the copy.

LinkedIn adds its own constraints. Connection requests and messages are governed by LinkedIn's user agreement and its limits, which can restrict accounts that use automation to send at scale. Read the terms before using any tool that automates actions on the platform, and treat the account of each rep as a business asset you can lose. Manual or lightly assisted outreach at low volume is the safer way to use the channel. The legal consent and opt-out rules for email do not disappear on LinkedIn: someone who tells you to stop must go on the suppression list there too.

- One clear reason for contacting this person, drawn from a source you can name
- One small ask, such as a reply or a short call, never a demand
- A plain unsubscribe line and a physical address in every email
- A fixed maximum number of touches, then a stop
- No fake reply threads, false urgency or invented familiarity

On cadence, we do not have a primary source that says how many touches or how many days apart is best, and the figures in many sales blogs are single-vendor claims.

05

Reply handling and CRM logging

A reply is a state change, and the sequence has to react. A positive reply stops the sequence and creates a task for the owner with a stated response time. A negative reply stops the sequence. A request to stop contact goes on the suppression list. An out-of-office message pauses the sequence until the return date, and an auto-reply naming a different contact should prompt a person to decide what happens next rather than letting a tool forward the pitch. Check that your sequencing tool stops on reply, and confirm that it works for replies sent from a different address than the one you mailed, which is common in B2B.

Every step should write to the CRM. At a minimum, log the sequence name and version, the step sent, the date and channel, the outcome (reply, bounce, unsubscribe, none), the owner, the data source and basis recorded at enrolment, and any suppression reason. That record answers compliance questions, such as when you last contacted someone and what they said, and it feeds reporting, such as which sequence produced meetings. It also keeps two reps from contacting the same person in the same week, which is a quiet cause of complaints.

Treat opt-out handling as an operations task with an owner, not as something the tool handles in the background. Someone should review the shared inbox for stop requests that did not come through the unsubscribe link, such as "please remove me" in a reply, and act on them the same day. Test the full path on a throwaway address every month: enrol, unsubscribe, confirm it is suppressed everywhere and that the CRM shows it.

06

AI-assisted drafting with a human gate

Language models are useful for first drafts and for variants of a template you have already approved. They are poor at knowing which facts are true of a particular company, and they will sometimes state invented details with confidence. The workable arrangement is that a person approves the template and every claim it contains, and that any personalisation field draws from a recorded data source such as a CRM property or a cited public page, not from a model's guess. Where a rep wants to add a line of their own, they write it and own it.

Do not let a model both write and send. A sequence that generates a different message for each contact and sends it without review removes the point at which someone would notice a false claim, a wrong name or a tone that would draw a complaint. Sampling a batch before launch, and again each week, is a minimum. Keep the prompt, the template version and the approver in the record, so you can show later what was sent and who agreed to it.

Be careful what you paste into an AI tool. Prospect data is personal data, and regimes such as GDPR apply to processing it, including by a vendor. Check that your AI provider's terms fit your obligations, and ask counsel before sending personal data about contacts in regulated regions to a third-party model.

07

Build checklist

Each step has a gate you can verify. Do not launch a sequence until every gate has been passed and the owner has signed it off.

Step	Owner	Gate to pass before moving on
Write the regional contact policy	Legal counsel with sales leadership	Written list of permitted regions, the basis for each, and what must be recorded on the contact
Set up the master suppression list and sync it to every sending tool	Revenue operations	A test address suppressed in one tool is blocked in all of them
Define the audience and record its source	Sales operations	Every enrolled contact has source, date and basis fields filled in
Write the sequence plan: touches, channels, days, stop rule	Sales manager	Plan names a maximum number of touches and the reason for each channel
Draft templates; AI may help, a person approves	Sales manager and a second reviewer	Each claim traced to a named source; footer includes address and opt-out; approver recorded

Step	Owner	Gate to pass before moving on
Configure reply, bounce and out-of-office rules	Revenue operations	Test replies from a different address stop the sequence; stop requests land on the suppression list
Configure CRM logging fields and reports	Revenue operations	A test enrolment writes sequence, step, outcome and source to the contact record
Send to a small pilot group and review	Sales manager	Complaint, unsubscribe and bounce rates reviewed before any scale-up decision
Weekly and monthly review	Revenue operations	Suppression test run monthly; stop requests in shared inbox cleared same day

Key Takeaways

- A sequence is a set of rules about who may be contacted, how, how often and when to stop. The copy is the smallest part of it.
- CAN-SPAM covers business email too: accurate headers, a physical address, a working opt-out honoured within ten business days, and responsibility for what your vendors send.
- Rules differ by country. Canada and the EU and UK lean on consent or legitimate-interest tests that are stricter than the US approach, so get counsel to sign off by region.
- One suppression list, checked at enrolment and before every step, matters more than any personalisation you can add.
- AI can draft first versions, but a person should approve the template and every claim in it before it is sent to anyone.

Sources

1. LinkedIn: User Agreement — <https://www.linkedin.com/legal/user-agreement>
2. FTC: CAN-SPAM Act, a compliance guide for business — <https://www.ftc.gov/business-guidance/resources/can-spam-act-compliance-guide-business>
3. Canada: Fighting Internet and Wireless Spam Act (S.C. 2010, c. 23) — <https://laws-lois.justice.gc.ca/eng/acts/E-1.6/>
4. GDPR Article 6: Lawfulness of processing — <https://gdpr-info.eu/art-6-gdpr/>
5. GDPR Article 7: Conditions for consent — <https://gdpr-info.eu/art-7-gdpr/>
6. UK ICO: Direct marketing and privacy and electronic communications — <https://ico.org.uk/for-organisations/direct-marketing-and-privacy-and-electronic-communications/>
7. Google: Email sender guidelines — <https://support.google.com/a/answer/81126>
8. RFC 8058: Signaling One-Click Functionality for List Email Headers — <https://datatracker.ietf.org/doc/html/rfc8058>