AI Compliance Checklist for Marketing and Lead Generation

Privacy, Legal, Marketing, and Operations Considerations

AI tools can speed up marketing and sales, but they also raise privacy, consumer protection, and telemarketing risks. Use this checklist to pressure-test AI tools and campaigns before launch. Check each box when your team has confirmed the item and can document it.

Privacy Considerations

- [ ] **Classify every AI provider correctly.**
  Make a list of every AI tool your business uses that receives personal information. For each one, check whether the provider can use that information for its own purposes, such as training its general AI model. If it can't, the provider is generally a service provider. If it can, keep personal information out of that tool, or be prepared to treat the disclosure as a "sale" or "share," which brings added privacy notice and opt-out obligations.

- [ ] **Match each AI use to the purpose disclosed in your privacy policy and at collection.**
  Use only data collected for a compatible purpose and disclosed in your privacy policy or at collection. Don't use AI to combine data sources in ways consumers wouldn't reasonably expect.

- [ ] **Assess profiling and automated decisions.**
  Flag every use that scores, routes, prices, or screens consumers for consequential decisions, including education, employment, housing, financial/lending services, insurance, health-care services, and essential services. Document data protection assessments and build notice, opt-out, access, and appeal workflows.

- [ ] **Protect chatbots and AI voice tools from wiretap and biometric claims.**
  Disclose AI processing before a chat or call begins and confirm no biometric identifiers are created (or obtain written consent and publish a retention schedule).

Legal Considerations

- [ ] **Negotiate data protection terms in every AI provider contract.**
  Require a data protection addendum with processor terms, a ban on training or commingling your data, and zero or short fixed retention.

- [ ] **Negotiate output ownership and IP indemnification.**
  Confirm you own inputs and outputs, the provider indemnifies against third-party IP claims outside the liability cap (read the conditions), and training data was lawfully licensed.

- [ ] **Allocate regulatory risk in the contract.**
  Obtain a compliance warranty (including AI disclosure laws), liability carve-outs for breaches and privacy violations, notice of material model changes with a termination right, and certified deletion on exit.

- [ ] **Keep a traceable approval record for every AI marketing asset.**
  Adopt an AI acceptable use policy and a content record for each AI asset (prompt, tool and model version, sources, reviewer, substantiation, risk assessment, approval date). Require legal review of high-risk claims.

Marketing Considerations

- [ ] **Substantiate every claim, including claims about your own AI.**
  Keep a substantiation file for each objective claim before content goes live, and review "AI-powered" style descriptions with the rigor of a performance claim.

- [ ] **Never use synthetic reviews or testimonials.**
  Ban AI-generated testimonials, get written releases covering AI replication for synthetic spokespeople and voice clones, and screen output for third-party trademarks and celebrity lookalikes.

- [ ] **Reduce IP exposure in AI content.**
  Avoid prompts that copy competitors' trademarks, creative, or real voices and likenesses. Adopt a labeling standard for realistic synthetic content.

- [ ] **Set limits for AI targeting and personalization.**
  AI can infer far more about people than they knowingly shared, and that creates legal, reputational, and fairness risks for your business. Regularly check whether audiences, offers, and pricing produce different outcomes by protected class, including through proxies such as zip code.

Operations Considerations

- [ ] **Confirm consent at the time of dialing.**
  Before each AI call or text, verify written consent covers the seller and AI or prerecorded messages and keep a consent record per lead. Check state rules too.

- [ ] **Build required disclosures into the call and chat flow.**
  Play required disclosures as fixed scripted segments rather than model-generated text, identify the system as AI at the start and throughout, and review telemarketing, AI, and privacy disclosure rules.

- [ ] **Monitor, test, and escalate.**
  Continuously monitor and test AI outputs, train the AI to recognize plain-language opt-outs, push opt-outs to the internal Do Not Call list across channels and affiliates, and set thresholds for human handoff.

- [ ] **Make production controls show what the AI did and why.**
  Being able to show what the AI did and why matters because, without that record, you can't defend its outputs to regulators, courts, or consumers, and you can't find and fix problems when something goes wrong.

Additional Privacy Resources

Scan to visit the Privacy Resources page on our website for additional regulatory guidance.

This checklist is for general educational purposes only. It is not legal advice and does not form an attorney-client relationship with Mac Murray & Shuster LLP. You should consult legal counsel before acting on any information in this checklist.

© 2026 Mac Murray & Shuster LLP | mslawgroup.com | 614.939.9955