THE COMPLIANCE PACKS · SECOND EDITION · SEPTEMBER 2026

What data and political firms must obey, country by country.

An expert-level map of the privacy, political-advertising, communications, foreign-influence and synthetic-media rules that bind firms like ours — the United States, Canada, Europe and the rest of the world — with the thresholds, the definitions that decide a case, the enforcement that has actually happened, and what each regime means in practice. Published free by Brushworks. Not legal advice.

Brushworks
brwrks.com/compliance
Corrections: research@brwrks.com
Cite as: Brushworks (2026), The compliance packs, second edition, September 2026

Reading the packs

What this is. Four regional packs and a set of cross-cutting analyses, written for the people who have to decide whether a program can run: compliance leads, counsel, campaign managers, ministry project officers and the data vendors that serve them. Each entry names the instrument, the trigger that brings a firm within it, the obligations that bite in political and data work, the enforcement record, and the practical consequence. Where the law is unsettled or litigated, the entry says so. Currency: the firm's review of September 2026, reviewed with each site release. Statutes, thresholds and guidance move monthly; treat every row as the question to ask, not the answer to rely on.

58

jurisdictions across four regions

6

kinds of rule: privacy, political advertising, communications, foreign influence, synthetic media, data brokers

14

enforcement actions that changed how this work is done

Three definitions recur and decide most cases. **Sensitive or special-category data** – in most of the world, political opinions are on the list, so the act of scoring someone's likely vote is itself a regulated act; in the United States it is not, and the regulated acts are the sale, the call, the disclaimer and the foreign principal. **Sale or sharing** – the transfer of personal data to a third party for value or for cross-context advertising, which most U.S. state laws let residents opt out of and which several treat a browser signal as exercising. **Political advertising** – now defined in statute in the European Union, the United Kingdom, Canada and Australia, each with a labeling and record-keeping regime that platforms enforce before regulators do.

Ten insights an expert should take from the packs

1. **The United States regulates the channel; the rest of the world regulates the data.** American law is a patchwork of communications, campaign-finance and consumer-protection rules with no general privacy statute and no treatment of political opinion as sensitive. Almost everywhere else, a political-opinion score is special-category data whose mere processing needs a legal basis. A firm that models behavior rather than ideology is compliant by design in both worlds; a firm that models ideology needs consent it cannot get at scale outside the United States.

2. **Platforms are now the first regulator.** Meta and Google withdrew paid political and issue advertising from the European Union in October 2025 rather than meet Regulation 2024/900's targeting and transparency duties; their ad libraries, verification and disclaimer rules are enforced in hours, not months. A program's compliance review must read platform policy as law, because the practical sanction — account loss mid-flight — is faster than any fine.

3. **"Register before you persuade" is now global.** FARA and the LDA in the United States, FIRS in the United Kingdom (commenced July 2025), FITS in Australia, third-party regimes in Canada, the United Kingdom and New Zealand, transparency registers in the European Union: the filing date must precede the first activity, and the filings are public. A registered program has nothing to find; an unregistered one is a criminal exposure for the firm and a scandal for the client.

4. **Consent for calls and texts is nearly universal, and political speech is not the exemption people think it is.** The TCPA exempts nothing political; the Do Not Call registry does. Canada's CASL exempts donation solicitations but not much else; PECR treats party messages as direct marketing. The FCC's 2024 ruling that AI voices are "artificial" and the $6 million forfeiture for the New Hampshire primary robocall settled the question for synthetic voice.

5. **Synthetic media is regulated by three different theories at once.** Labeling (the EU AI Act, roughly half of U.S. states, Brazil, China), prohibition near elections (Korea's ninety-day ban, several U.S. states, Singapore, Brazil), and existing fraud and impersonation law (the FCC, the FEC's fraudulent-misrepresentation provision). Several U.S. state laws have been enjoined on First Amendment grounds; the theory that survives everywhere is disclosure.

6. **The data-broker registries are the new perimeter.** California's Delete Act builds a one-stop deletion mechanism that brokers must honor from August 2026; Texas, Oregon and Vermont maintain registries; the FTC has banned the sale of sensitive location data by order. A licensor that is not registered where it must be is a provenance failure for every downstream program.

7. **Party exemptions protect parties, not vendors.** Australia exempts registered parties from the Privacy Act; PIPEDA does not reach federal parties; most U.S. state laws exempt nonprofits and committees. None of these reach a vendor, which is covered in its own right, and British Columbia's regulator has held that its private-sector law reaches federal parties operating in the province.

8. **Cross-border transfers are solved on paper and fragile in practice.** The EU–U.S. Data Privacy Framework survived its first challenge in 2025; standard contractual clauses and the UK addendum carry the rest; Brazil, India, Saudi Arabia, China and Vietnam add localization or adequacy conditions of their own. Institutional mandates increasingly require in-country holding, which is a design decision, not a paperwork one.

9. **Enforcement follows the scandal, and the scandal is always the same one.** Cambridge Analytica produced the ICO's fine, the FTC's order, Canada's joint finding, Australia's settlement and the EDPB's statement; the

New Hampshire robocall produced the FCC's rule. Regulators act on political data when a case is vivid, and the cases are vivid when consent was missing and the messenger was hidden.

10. **The cheapest compliance is a method that does not need the exemption.** Behavior instead of identity, disclosed messengers, one account of record, a sealed control and a written declination policy satisfy most of these regimes without a special legal basis. The compliance review then checks paperwork rather than redesigning the program.

United States

No comprehensive privacy statute; a federal layer for campaign finance, foreign agents, communications and consumer protection; twenty state consumer-privacy laws with different thresholds and exemptions; four state registries for data brokers; and a wave of state law on artificial intelligence in political advertising, some of it enjoined.

Federal instruments

INSTRUMENT	TRIGGER	OBLIGATIONS THAT BITE	ENFORCEMENT AND RECORD	IN PRACTICE
Federal Election Campaign Act and FEC regulations (52 U.S.C. §30101 et seq.; 11 C.F.R.)	Any public communication for or against a federal candidate; any expenditure coordinated with a campaign; any contribution	Disclaimers with sponsor and "paid for by" language on public communications (§30120; 11 C.F.R. §110.11), including internet communications placed for a fee; coordination test with payment, content and conduct prongs (§109.21) and a firewall safe harbor for vendors serving both sides (§109.21(h)); prohibition on foreign-national contributions, expenditures and decision-making (§30121); fraudulent misrepresentation of campaign authority (§30124), which the FEC has said reaches deceptive AI content under existing law	FEC civil penalties and conciliation; DOJ criminal prosecution for knowing and willful violations; the FEC declined in 2024 to write AI-specific rules, relying on §30124	The compliance review confirms disclaimer wording per channel, documents the firewall between practices, and screens every funder for foreign-national status; vendor payments appear in the committee's reports
Foreign Agents Registration Act (22 U.S.C. §611–621)	Acting within the United States as an agent of a foreign principal in political activities, public relations, publicity or political consulting; "foreign principal" includes governments, parties, and foreign persons and entities	Registration within ten days of agreeing to act and before acting; conspicuous statement on informational materials disseminated to two or more persons; supplemental statements every six months; retention of records; the LDA exemption (§613(h)) is unavailable where the principal is a foreign government or party	DOJ National Security Division FARA Unit; criminal penalties for willful failure; advisory opinions published since 2018; enforcement rose sharply after 2016 and continues	The firm registers before any activity that touches the United States, labels every informational material, and reports semiannually; the acceptance screen refuses any mandate aimed at a U.S. election
Lobbying Disclosure Act (2 U.S.C. §1601 et seq.)	Lobbying contacts with covered federal officials above the statutory time and income thresholds	Registration within 45 days of the first contact; quarterly activity reports (LD-2); semiannual contribution reports (LD-203); FARA applies instead where the client is a foreign government or party	Clerk of the House and Secretary of the Senate; civil and criminal penalties; DOJ enforcement	Institutional mandates that involve official contacts are registered under whichever regime applies before the first meeting

INSTRUMENT	TRIGGER	OBLIGATIONS THAT BITE	ENFORCEMENT AND RECORD	IN PRACTICE
Telephone Consumer Protection Act and FCC rules (47 U.S.C. §227; 47 C.F.R. §64.1200)	Any call or text to a mobile number made with an automatic telephone dialing system or an artificial or prerecorded voice; any prerecorded call to a residential line	Prior express consent for autodialed or prerecorded calls and texts to mobiles (political messages included); the Supreme Court's narrow reading of "autodialer" (Facebook v. Duguid, 2021) exempts human-initiated peer-to-peer texting but not prerecorded or AI voice; the FCC's February 2024 declaratory ruling treats AI-generated voices as "artificial"; revocation of consent by any reasonable means must be honored within ten business days (rules effective April 2025); accurate caller identification; time-of-day limits	FCC forfeitures and private actions at $500–$1,500 per call or text with class treatment; the FCC fined the consultant behind the January 2024 New Hampshire primary deepfake robocall $6 million and the carrier $1 million; the FCC's 2024 "one-to-one consent" rule was vacated by the Eleventh Circuit in January 2025	Autodialed texting needs documented consent; P2P texting runs on human-initiated platforms with a suppression list; no synthetic voice, ever; every opt-out honored across channels
Telemarketing Sales Rule and the National Do Not Call Registry (16 C.F.R. Part 310)	Telemarketing of goods, services or charitable solicitations	Political calls are outside the TSR and the national registry, but remain subject to the TCPA's consent rules and to state political-call statutes; caller-ID accuracy and abandonment rules apply to any seller	FTC; state attorneys general under the Telemarketing Act	A political program cannot rely on the DNC exemption to send autodialed texts
CAN-SPAM Act (15 U.S.C. §7701 et seq.)	Commercial electronic mail	Political email is largely outside the statute, but fundraising email with a commercial element, deceptive headers or subject lines, and failure to honor opt-outs can fall within it; mailbox providers enforce their own reputation rules regardless	FTC; state attorneys general; private ISP actions	Accurate headers, a working unsubscribe honored within ten days, and physical address on every message as a matter of practice
FTC Act §5 and data-broker enforcement (15 U.S.C. §45)	Unfair or deceptive acts affecting commerce	Privacy statements must be true; the FTC's 2019 order against Cambridge Analytica treated deceptive harvesting of profile data as unfair; 2024 orders against X-Mode/Outlogic and InMarket banned the sale of sensitive location data and required deletion; the Kochava litigation established that selling precise location revealing visits to sensitive sites can be an unfair practice	Consent orders with twenty-year terms, deletion and data-minimization requirements, civil penalties for order violations	Provenance records for every licensed source; no precise location; no data revealing visits to sensitive places; privacy policy statements audited against practice
Children's Online Privacy Protection Act (15 U.S.C. §6501)	Online services directed to children under thirteen, or actual knowledge of a child	Verifiable parental consent before collection; the 2025 rule amendments tighten third-party disclosure consent and retention	FTC civil penalties; state attorneys general	The firm holds no data on minors; age-gated sources are excluded at provenance review

INSTRUMENT	TRIGGER	OBLIGATIONS THAT BITE	ENFORCEMENT AND RECORD	IN PRACTICE
Platform political-advertising policies	Any paid political or issue placement on Meta, Google, Microsoft, X, TikTok (which bans political ads) and the connected-television and programmatic platforms	Advertiser verification in the sponsor's name; "paid for by" disclaimers; public ad libraries retaining ads for years; AI-generated content disclosure (Meta, Google since 2023–2024); targeting restrictions on political ads in some platforms; issue-ad definitions broader than statute	Ad rejection, account suspension, library annotation — applied algorithmically and appealed slowly	Seats are verified in the sponsor's name before day twelve; disclaimer language is set per platform; a rejected creative is a program delay, so masters are checked against platform policy at the studio stage

State consumer-privacy laws

Twenty states have comprehensive privacy statutes in force. They share a structure – rights of access, deletion, correction and portability; opt-outs from targeted advertising, sale and consequential profiling; opt-in consent for sensitive data; data-protection assessments for high-risk processing; controller–processor contracts – and differ on four points that matter for political work: whether nonprofits and political committees are covered; whether a browser opt-out signal must be honored; what counts as sensitive data; and whether the attorney general must offer a cure period. No state lists political opinion as sensitive data. Most exempt nonprofits; a vendor to a nonprofit is covered in its own right.

STATE	STATUTE; IN FORCE	APPLICABILITY THRESHOLD	NOTABLE FOR POLITICAL AND DATA WORK
California	CCPA as amended by the CPRA (2023); Delete Act (SB 362)	For-profit businesses with roughly $26 million revenue, or 100,000 consumers or households, or half of revenue from selling or sharing	"Share" for cross-context behavioral advertising is an opt-out right; Global Privacy Control must be honored; sensitive personal information includes racial or ethnic origin, religion and union membership with a right to limit use; risk assessments and cybersecurity audits under 2025 regulations; the California Privacy Protection Agency is a dedicated regulator with early enforcement against Honda and a retailer for defective opt-out flows; data brokers register with the CPPA and must process consumer deletion requests through the DROP mechanism from August 2026; political committees and nonprofits are outside "business"
Virginia	VCDPA (2023)	100,000 consumers, or 25,000 with half of revenue from sale	Opt-in for sensitive data; nonprofits exempt; no private right of action; cure period; AG enforcement
Colorado	CPA (2023); AG rules	100,000 consumers, or 25,000 with revenue from sale	Universal opt-out mechanisms binding since 2024; nonprofits are covered; detailed rules on profiling, dark patterns and consent refresh; amendments on minors and biometric data
Connecticut	CTDPA (2023, amended 2025)	Thresholds lowered by the 2025 amendments; sensitive-data processing alone can trigger coverage	Opt-out signals binding; expanded sensitive-data list; minors' protections; profiling rights
Utah	UCPA (2023)	$25 million revenue and consumer thresholds	Narrow rights, notice-and-opt-out for sensitive data, no assessments; the lightest of the twenty
Texas	TDPSA (2024); Data Broker Law (2023)	Any business that processes personal data and is not a small business under SBA definitions	No numeric threshold, so most vendors are covered; opt-out signals binding since 2025; data brokers register with the Secretary of State and post notices; the attorney general has been the most active state enforcer, with actions against automakers and brokers over driving and location data

STATE	STATUTE; IN FORCE	APPLICABILITY THRESHOLD	NOTABLE FOR POLITICAL AND DATA WORK
Oregon	OCPA (2024); data-broker registry (2024)	100,000 consumers, or 25,000 with revenue from sale; nonprofits covered from July 2025	Consumers may obtain the list of specific third parties that received their data; opt-out signals binding; brokers register with the Department of Consumer and Business Services
Montana	MCDPA (2024, amended 2025)	50,000 consumers, lowered by amendment	Opt-out signals binding; amendments removed the cure period and added minors' protections
Florida	Digital Bill of Rights (2024)	Controllers with more than $1 billion in revenue and specified business models; some provisions apply more broadly	Sensitive-data and children's provisions reach smaller entities; treat as a large-platform law
Delaware	DPDPA (2025)	35,000 consumers, or 10,000 with revenue from sale	Nonprofits covered except narrow categories; opt-out signals binding from 2026
Iowa	ICDPA (2025)	100,000 consumers	Narrower rights; opt-out rather than opt-in for sensitive data; long cure period
Nebraska	NDPA (2025)	Texas-style: any non-small business	Broad reach; opt-out signals binding
New Hampshire	NHPA (2025)	35,000 consumers, or 10,000 with revenue from sale	Opt-out signals binding; AG rulemaking
New Jersey	NJDPA (2025)	100,000 consumers, or 25,000 with revenue from sale	Covers financial data; opt-out signals binding; regulations from the Division of Consumer Affairs; nonprofits not exempt
Tennessee	TIPA (2025)	$25 million revenue plus consumer thresholds	Affirmative defense for programs conforming to the NIST Privacy Framework
Minnesota	MCDPA (2025)	100,000 consumers, or 25,000 with revenue from sale	Right to question the result of profiling and learn what data was used; documented privacy program and inventory required; opt-out signals binding
Maryland	MODPA (2025)	35,000 consumers, or 10,000 with revenue from sale	The strictest minimization standard in the country — collection limited to what is reasonably necessary; sale of sensitive data prohibited outright; sensitive data includes national origin, citizenship and immigration status; targeted advertising to minors prohibited
Indiana	ICDPA (2026)	100,000 consumers	Virginia-style rights; long cure period
Kentucky	KCDPA (2026)	100,000 consumers	Virginia-style; cure period
Rhode Island	RIDTPPA (2026)	35,000 consumers, or 10,000 with revenue from sale	Requires listing third parties to which data is sold; no cure period

Political-specific state rules

AREA	THE RULE	WHERE IT IS STRICTEST	WHAT TO DO
Voter registration files	Every state licenses its file on its own terms; most restrict use to election, political, scholarly or journalistic purposes and prohibit commercial use, resale or public posting; some require an applicant's sworn statement	California (certified purpose, no commercial use), Pennsylvania and Virginia (restricted purposes); a few states sell to anyone	Obtain the file under the state's terms, record the permitted purpose in the provenance record, never commingle with commercial licensing, and destroy at close where the license requires
Artificial intelligence in political advertising	By 2026 roughly half of the states require disclosure of AI-generated or materially altered content in political ads, or prohibit deceptive deepfakes of candidates within a window before an election, with candidate injunctive remedies	Texas (criminal, 2019), California (three 2024 statutes, one enjoined as viewpoint-based), Minnesota, Michigan, Washington, New York, Florida, Arizona, Utah, Wisconsin, Indiana, New Mexico, Oregon, Colorado and others	Label AI-assisted content where required in the statute's words; never produce synthetic depictions of real people; confirm each state's window, remedy and pending litigation in the compliance review
State disclaimers and reporting	State campaign-finance law adds "paid for by", top-funder and committee-name requirements, and independent-expenditure reports within 24 to 72 hours near elections	California (top three funders on committee ads), Washington, New York, Colorado, Alaska	The compliance review confirms exact wording per jurisdiction and channel before air
Political calls and texts	State statutes regulate political robocalls and texts beyond the TCPA — identification at the start, hours, opt-out, state registries, and outright bans in a few states	Florida (consent for automated political texts), Oklahoma (mini-TCPA), Washington, Indiana, Wyoming, Arkansas and Louisiana (bans or registries)	Consent for autodialed texts; state-specific identification; a suppression list that honors every opt-out everywhere
Data brokers	Registration and disclosure regimes in California, Vermont, Texas and Oregon; California's DROP deletion mechanism from 2026	California (CPPA registry, DROP, audits), Texas (registration and security), Oregon (registry with consumer lookup)	Every licensor is checked for registration; no license from a broker that is not registered where it must be

Canada

A federal private-sector privacy law that does not reach political parties, provincial laws that sometimes do, the strictest anti-spam statute in the world, and an election law that reaches third parties, foreign spenders and calling services.

INSTRUMENT	TRIGGER	OBLIGATIONS THAT BITE	ENFORCEMENT AND RECORD	IN PRACTICE
Personal Information Protection and Electronic Documents Act (PIPEDA)	Collection, use or disclosure of personal information in the course of commercial activity, federally and in provinces without substantially similar law	Meaningful consent appropriate to sensitivity; purpose limitation; openness; access and correction; safeguards; mandatory breach reporting and record-keeping; accountability for transfers to processors; federal political parties are not "commercial activity" and are outside the Act, but their vendors are within it	Privacy Commissioner of Canada investigates and issues findings; damages through the Federal Court; the 2019 joint finding with British Columbia that Facebook contravened PIPEDA in the Cambridge Analytica–AggregateIQ matter; Bill C-27, which would have replaced PIPEDA and regulated AI, died in January 2025	Consent documented per purpose; profiling disclosed in plain language; processors bound by contract; breach clock started on discovery
Quebec: Act respecting the protection of personal information in the private sector, as amended by Law 25	Any enterprise collecting Quebec residents' data, wherever established	Person in charge of protection (a privacy officer) by default the CEO; privacy impact assessments before projects involving personal information and before transfers outside Quebec; consent by purpose in clear language; disclosure of automated decisions and profiling with the means to deactivate; portability since 2024; transparency about technology that identifies, locates or profiles; administrative penalties to CAD 10 million or 2 percent of worldwide turnover and penal fines to CAD 25 million or 4 percent	Commission d'accès à l'information; the strictest regime in North America and the closest to the GDPR	Programs touching Quebec run a PIA before the terrain brief, document the transfer assessment, and present profiling controls in French
Alberta and British Columbia Personal Information Protection Acts	Private-sector organizations in the province; BC's Act reaches non-commercial organizations	Consent and access regimes substantially similar to PIPEDA; BC's Information and Privacy Commissioner held in 2022–2024 that PIPA applies to federal political parties collecting personal information in the province, a position upheld by the BC Supreme Court	Provincial commissioners; orders and, in Alberta, offences	A party program in British Columbia is treated as covered regardless of the federal gap

INSTRUMENT	TRIGGER	OBLIGATIONS THAT BITE	ENFORCEMENT AND RECORD	IN PRACTICE
Canada's Anti-Spam Legislation (CASL)	Any commercial electronic message sent to or from a Canadian address; installation of software; alteration of transmission data	Express or implied consent, sender identification and a working unsubscribe on every commercial message; messages by or on behalf of registered parties, candidates and nominees soliciting contributions are exempt, but other campaign messaging with a commercial element is not; administrative penalties to CAD 10 million per violation for organizations	CRTC investigates and levies penalties; the Competition Bureau and the Privacy Commissioner share enforcement; a private right of action remains suspended	Donation solicitations rely on the exemption; anything else is sent on documented consent with identification and unsubscribe
Canada Elections Act (as amended by Bill C-76, 2018)	Parties, candidates, third parties and calling-service providers in federal elections	Third parties spending above CAD 500 on regulated activities during the pre-election and election periods must register with Elections Canada, report and observe spending limits; foreign entities are prohibited from spending to influence electors; partisan and election advertising must carry a tagline identifying the sponsor; registered parties must publish a privacy policy (a weak requirement Bill C-65 proposed to expand before it died); calling-service providers and their clients register with the CRTC's Voter Contact Registry and retain scripts and recordings	Commissioner of Canada Elections; administrative monetary penalties and prosecution; CRTC for the Voter Contact Registry	Third-party status is determined at acceptance; taglines on every master; calling services registered before the first call
CRTC Unsolicited Telecommunications Rules	Telemarketing and automatic dialing-announcing devices	Political calls are exempt from the National Do Not Call List but must identify the caller and honor calling hours; ADAD calls must begin with identification and provide a contact number; internal do-not-call lists must be kept	CRTC administrative monetary penalties	Identification scripts and hours by time zone across seven offices
Provincial election acts	Provincial and municipal campaigns and third parties	Separate third-party registration, spending limits and advertising blackouts; Quebec's Election Act restricts third-party spending most tightly; Ontario's regime was litigated to the Supreme Court in 2025 over pre-election third-party limits	Provincial chief electoral officers	Provincial programs are reviewed against the province's own regime, not the federal one

Europe

The most developed regime in the world, in four layers: a general data-protection law in which political opinions are special-category data; an EU regulation on political advertising that the largest platforms answered by withdrawing the product; platform duties under the Digital Services Act and labeling duties under the AI Act; and national election and marketing law on top. The United Kingdom mirrors the structure with its own instruments.

European Union

INSTRUMENT	TRIGGER	OBLIGATIONS THAT BITE	ENFORCEMENT AND RECORD	IN PRACTICE
General Data Protection Regulation (Regulation (EU) 2016/679)	Processing by a controller or processor established in the EU, or of data subjects in the EU when offering them goods or services or monitoring their behavior (Art. 3)	A lawful basis for every purpose (Art. 6); political opinions, religious beliefs, ethnic origin and health are special-category data whose processing is prohibited unless explicit consent or a narrow condition applies (Art. 9) — scoring likely vote is processing political opinions; transparency to the person (Arts. 13-14) including the logic of profiling; rights of access, erasure, restriction, objection to direct marketing (absolute) and to profiling, and not to be subject to solely automated decisions with significant effects (Arts. 15-22); data-protection impact assessments before large-scale profiling (Art. 35); a DPO where core activities involve large-scale special-category processing (Art. 37); a representative for non-EU controllers (Art. 27); records of processing (Art. 30); breach notice to the authority within 72 hours (Art. 33); transfers only with adequacy, standard clauses or another Chapter V mechanism	National authorities coordinated by the European Data Protection Board; fines to €20 million or 4 percent of worldwide turnover; EDPB Statement 2/2019 on personal data in political campaigns; national fines on political profiling (Italy's Rousseau platform, 2019); the EU-U.S. Data Privacy Framework (2023) survived the Latombe challenge in the General Court in September 2025	The firm does not process political opinions as data: behavior only, no ideology scores, which removes the Art. 9 problem for the program's data; DPIAs before every EU program; the objection right honored as a permanent suppression; transfers under the DPF or standard clauses with a transfer assessment
ePrivacy Directive (2002/58/EC) as implemented nationally	Electronic communications, cookies and direct marketing by electronic means	Consent for cookies and trackers beyond the strictly necessary; consent for automated calls, SMS and email marketing to individuals (with a narrow existing-customer exception); national variations in the treatment of political messaging, generally as direct marketing	National data-protection and telecom authorities; cookie fines have been the most frequent enforcement in several states	No tracking on the firm's site; SMS and email programs run on consent held by the client or partner of record, verified before use

INSTRUMENT	TRIGGER	OBLIGATIONS THAT BITE	ENFORCEMENT AND RECORD	IN PRACTICE
Regulation (EU) 2024/900 on the transparency and targeting of political advertising	Political advertising — preparation, placement, promotion, publication or dissemination of a message by, for or on behalf of a political actor, or liable to influence an election, referendum, legislative process or voting behavior — in the EU; applies from 10 October 2025	Every political ad labeled as such with the sponsor, the entity ultimately controlling it, the amounts, the election or referendum, and a link to a transparency notice; a European repository of political advertisements; targeting and ad delivery only with explicit consent collected separately for that purpose, never on special-category data (Art. 9 GDPR) and never to minors; sponsors from outside the EU barred from paid political advertising in the three months before an election or referendum; due diligence and record-keeping for publishers and intermediaries	National authorities, with data-protection authorities enforcing the targeting rules under GDPR penalties; Meta and Google announced that they would cease political, electoral and social-issue advertising in the EU from October 2025 rather than comply	Paid political advertising in the EU is now largely a matter of publisher inventory, television and out-of-home under national law; EU programs run through organic advocacy, earned media and disclosed placements with the transparency notice, and never on behavioral targeting of political opinion
Digital Services Act (Regulation (EU) 2022/2065)	Intermediaries and platforms serving EU users; heightened duties for very large online platforms and search engines	No advertising based on profiling with special-category data (Art. 26); no profiling-based ads to minors (Art. 28); ad repositories with sponsor, payer, targeting parameters and reach for very large platforms (Art. 39); systemic-risk assessment and mitigation including electoral processes (Arts. 34-35); the Commission's 2024 election guidelines on integrity measures	European Commission for very large platforms, with fines to 6 percent of turnover; national Digital Services Coordinators	Platform ad repositories are the public record of a program; the compliance review checks that placements appear correctly there
Artificial Intelligence Act (Regulation (EU) 2024/1689)	Providers and deployers of AI systems in the EU market; general-purpose model providers	Transparency duties (Art. 50) — deployers of systems generating deepfakes must disclose that content is artificially generated or manipulated, with a narrower duty for text published to inform the public; AI systems intended to influence the outcome of elections or voting behavior are listed as high-risk (Annex III, point 8(b)), triggering risk management, data governance, human oversight and registration duties on providers; general-purpose model obligations since August 2025; most Art. 50 and high-risk obligations apply from August 2026	National market-surveillance authorities and the AI Office; fines to €35 million or 7 percent for prohibited practices, €15 million or 3 percent for most other breaches	AI-assisted content is labeled where the Act requires; no synthetic depictions of real people; the firm's models predict responsiveness to a message, not voting behavior, and the compliance review documents why the Annex III listing does not attach

United Kingdom

INSTRUMENT	TRIGGER	OBLIGATIONS THAT BITE	ENFORCEMENT AND RECORD	IN PRACTICE
UK GDPR and the Data Protection Act 2018, as amended by the Data (Use and Access) Act 2025	Processing by UK-established organizations or of UK data subjects when offering services or monitoring behavior	Same structure as the EU regulation; political opinions are special-category data, with a specific condition in Schedule 1 permitting registered parties to process political opinions as part of their legitimate activities, subject to the right to object; DPIAs, DPOs and records as in the EU; the 2025 Act eases some research and legitimate-interest rules, restructures the ICO as the Information Commission, and lifts PECR penalties to UK GDPR levels	Information Commissioner's Office: the 2018 investigation into data analytics in political campaigns, the £500,000 fine against Facebook under the previous law, the audits of all major parties in 2020 with published recommendations, and fines against Leave.EU and an insurer for cross-use of data; fines to £17.5 million or 4 percent	Parties rely on the Schedule 1 condition; vendors do not — the firm's UK work processes behavior, not opinion, and honors objection as permanent suppression
Privacy and Electronic Communications Regulations 2003 (PECR)	Electronic direct marketing — calls, texts, emails, cookies	Consent for marketing calls to TPS-registered numbers, for automated calls, and for texts and emails to individuals; the ICO treats political parties' promotional messages as direct marketing; penalties raised by the 2025 Act	ICO monetary penalties; a substantial record of fines for texting and calling without consent	Texting and email on documented consent only; TPS screening; no automated calls
Elections Act 2022, Part 6: digital imprints	Paid digital political material anywhere; unpaid material from parties, candidates, campaigners and certain others	Since November 2023 an imprint with the promoter's name and address on all paid digital political material and on unpaid material from regulated actors; the Electoral Commission's guidance covers where the imprint sits when the platform cannot carry it	Electoral Commission investigation and civil sanctions; criminal offence for failure	The imprint is set on every master before it leaves the studio
Political Parties, Elections and Referendums Act 2000 (non-party campaigners)	Spending on regulated campaign activity above the registration threshold during the regulated period	Registration with the Electoral Commission, spending limits, donation controls and reporting; foreign-source funding restrictions	Electoral Commission	Third-party status confirmed at acceptance; spending tracked against the regulated period
National Security Act 2023, Part 4: Foreign Influence Registration Scheme (FIRS)	Arrangements to carry out political-influence activities in the UK at the direction of a foreign power; an enhanced tier for specified states	Registration within ten days of the arrangement and before activity, since the scheme commenced on 1 July 2025; the enhanced tier (initially covering Russia and Iran) registers a wider range of activity; public register for the political-influence tier	Home Office; criminal offences for failure to register	Any institutional mandate from a foreign government touching UK political influence is registered before the brief is written

National layers in the EU

MEMBER STATE	INSTRUMENTS	WHAT MATTERS FOR POLITICAL AND DATA WORK
Germany	Bundesdatenschutzgesetz; Gesetz gegen den unlauteren Wettbewerb §7; Bundesmeldegesetz §50; state election laws	Consent required for telephone and email advertising to consumers; parties may obtain registry extracts (name, address, doctorate) in the six months before an election, for that election only; state data-protection authorities have examined party microtargeting on social platforms; the Federal Constitutional Court's tradition on informational self-determination shapes strict readings
France	Loi Informatique et Libertés; CNIL guidance on political communication; Code électoral (L.52-1, L.49); Loi du 22 décembre 2018 on information manipulation	Paid political advertising on television and radio is prohibited; commercial advertising for electoral purposes is banned in the six months before an election, including online; campaigning is silent from the eve of the vote; CNIL's guidance governs prospecting, consent and the use of the electoral roll; platforms must publish sponsor and payment information for issue content during campaign periods under the 2018 law
Spain	LOPDGDD (2018); LOREG Art. 58 bis	The 2018 law permitted parties to compile political opinions from public web sources within the electoral framework; the Constitutional Court struck the provision down in 2019 (STC 76/2019) as an unjustified interference with fundamental rights — the clearest judicial statement in Europe that opinion profiling by parties needs a precise legal basis
Italy	Codice privacy; the Garante's decisions	The Garante fined the Five Star Movement's Rousseau platform operator in 2019 for security and profiling failures, and has issued guidance on political communication and the use of membership data
Netherlands	UAVG; the Authority for Personal Data's guidance; the DDMA code	The regulator has warned parties against political microtargeting without consent and audited campaign apps; Dutch practice is consent-heavy for email and SMS
Ireland	Data Protection Act 2018; Electoral Reform Act 2022	The Data Protection Commission supervises most platforms' EU operations, so platform ad-library and targeting behavior is shaped by Irish enforcement; the 2022 Act created an Electoral Commission and provides a framework for online political-advertising transparency
Poland, Czechia, Nordic and Baltic states	GDPR with national election codes	Consent-based marketing regimes; election silence periods; sponsor identification on political material; several authorities have issued campaign-period guidance on data use

The rest of the world

Most major markets have a comprehensive privacy law modeled loosely on the GDPR; the local variations that matter are whether political opinion is sensitive, whether parties are exempt, whether the law localizes data, and whether the election authority regulates online advertising and synthetic media directly.

Americas

JURISDICTION	INSTRUMENTS	OBLIGATIONS THAT BITE	ENFORCEMENT AND RECORD
Brazil	Lei Geral de Proteção de Dados (2020); Superior Electoral Court (TSE) Resolution 23.610/2019 as amended in 2024	Political opinion and party membership are sensitive data requiring specific, highlighted consent; legal bases, DPIA-like reports on request, DPO appointment, international transfer rules (ANPD regulation 2024, with standard clauses); the TSE's 2024 electoral rules require labeling of AI-generated content, prohibit deepfakes, bar chatbots simulating candidates, restrict paid boosting to candidates and parties, and hold platforms liable for failing to remove disinformation promptly	ANPD administrative sanctions since 2021 (warnings, fines to 2 percent of Brazilian revenue capped at R$50 million per infraction); the TSE removed content and sanctioned campaigns in the 2024 municipal elections
Mexico	Ley Federal de Protección de Datos Personales en Posesión de los Particulares (new law, 2025); INE regulations on the electoral roll and propaganda	Consent and privacy notices; ARCO rights; the 2025 reform dissolved the independent regulator INAI and moved oversight to a government secretariat, a change international counsel flag for adequacy and independence; the electoral authority controls the padrón electoral and regulates campaign propaganda and the use of citizen data	Administrative fines; electoral sanctions by INE and the electoral tribunal
Argentina	Ley 25.326 (2000); reform bill pending	Database registration with the Agencia de Acceso a la Información Pública; political opinion is sensitive; EU adequacy since 2003; the pending reform would align with the GDPR	Administrative sanctions; habeas data actions
Chile	Ley 21.719 (published December 2024; in force December 2026)	GDPR-style rights and bases, sensitive data including political opinion, DPO-like roles, transfer rules, and a new Personal Data Protection Agency with fines to 4 percent of turnover	The new Agency from 2026
Colombia	Ley 1581 (2012); Decree 1377	Registration of databases with the National Database Registry; sensitive data includes political affiliation and requires explicit consent; the electoral authority regulates propaganda	Superintendencia de Industria y Comercio fines and orders
Peru, Uruguay, Costa Rica, Panama, Ecuador	Peru Law 29733; Uruguay Law 18.331 (EU-adequate); Costa Rica Law 8968; Panama Law 81; Ecuador LOPDP (2021)	Consent-based regimes; political opinion sensitive in each; registration duties in Peru and Costa Rica; Ecuador's law is GDPR-modeled with a superintendency	National authorities of varying activity

Middle East and Africa

JURISDICTION	INSTRUMENTS	OBLIGATIONS THAT BITE	ENFORCEMENT AND RECORD
United Arab Emirates	Federal Decree-Law 45/2021 (PDPL); DIFC Data Protection Law 2020; ADGM Data Protection Regulations 2021	Consent-based federal regime with sensitive-data rules and cross-border restrictions, executive regulations still developing; the free-zone laws are GDPR-close with DPO and DPIA duties and active commissioners; political campaigning is not a lawful activity — institutional and public-communication work only, with government counterparties, under the relevant emirate's media rules	Federal Data Office; DIFC and ADGM commissioners with published fines
Saudi Arabia	Personal Data Protection Law (Royal Decree M/19, 2021, amended 2023; enforced from September 2024) and implementing regulations	Consent or another basis; data-subject rights; records; DPO where required; transfer rules with adequacy and safeguards; registration of certain controllers with SDAIA; no political campaigning — institutional communication only	SDAIA; fines and, for sensitive-data disclosure, criminal penalties
Israel	Protection of Privacy Law, Amendment 13 (in force August 2025); Elections Law	Modernized regime with a strengthened Privacy Protection Authority, DPO duties for large processors, database registration narrowed, and administrative fines; political opinion is sensitive; after the 2020 leak of the voter registry through a party's campaign app, use of the registry is tightly conditioned	Privacy Protection Authority; fines under Amendment 13
Turkey	Law 6698 (KVKK), amended March 2024	Explicit consent or a listed condition for sensitive data including political opinion; controllers' registry (VERBIS); the 2024 amendments aligned cross-border transfer rules with the GDPR (adequacy, standard clauses, binding rules)	Personal Data Protection Authority fines
South Africa	Protection of Personal Information Act (in force 2021); Electoral Act	Political persuasion is special personal information (s.26) with a specific authorization for political parties (s.31) that does not extend to vendors; direct marketing by electronic means requires consent or an existing-customer relationship (s.69); prior authorization for certain processing; cross-border rules (s.72)	Information Regulator with enforcement notices and administrative fines to R10 million; the Regulator's first fines fell on public bodies in 2023
Nigeria	Nigeria Data Protection Act 2023	Registration of data controllers and processors of major importance; political opinion is sensitive; DPO duties; transfer rules; the Commission has issued directives and begun enforcement	Nigeria Data Protection Commission; fines to 2 percent of annual revenue
Kenya	Data Protection Act 2019	Registration of controllers and processors; political opinion is sensitive; the Office of the Data Protection Commissioner has penalized organizations, including a political party sanctioned for registering members without consent	ODPC penalties to KES 5 million or 1 percent of turnover
Ghana	Data Protection Act 843 of 2012	Registration with the Data Protection Commission; consent; sensitive data includes political opinion; the Electoral Commission's rules govern the voters' register	Data Protection Commission

JURISDICTION	INSTRUMENTS	OBLIGATIONS THAT BITE	ENFORCEMENT AND RECORD
Egypt, Morocco, Tunisia	Egypt Law 151/2020 (regulations pending); Morocco Law 09-08; Tunisia Organic Law 2004-63 with reform pending	Licensing and registration regimes; sensitive data including political opinion; enforcement developing	National authorities

Asia-Pacific

JURISDICTION	INSTRUMENTS	OBLIGATIONS THAT BITE	ENFORCEMENT AND RECORD
Japan	Act on the Protection of Personal Information (amended 2022); Public Offices Election Act	Purpose specification; opt-out third-party provision with notification to the PPC; "special care-required" data (including creed) needs consent; records of third-party transfers; the election law permits internet campaigning but restricts paid online advertising to parties and bans it for candidates, with strict timing rules	Personal Information Protection Commission orders and fines
South Korea	Personal Information Protection Act (amended 2023); Public Official Election Act (amended December 2023)	Consent-centric regime with separate consent for sensitive data including political opinion; large administrative fines (to 3 percent of related revenue); the election law bans deepfake campaign content in the ninety days before an election and requires labeling outside that window, with the National Election Commission prosecuting violations in the 2024 election	Personal Information Protection Commission; NEC
China	Personal Information Protection Law (2021); Data Security Law; Deep Synthesis Provisions (2023); AI labeling measures (2025)	Consent and separate consent for sensitive data; localization and security assessment for transfers by important operators; synthetic media must be labeled visibly and in metadata; no political campaigning exists; institutional communication under state media rules only	Cyberspace Administration of China; fines to 5 percent of turnover
India	Digital Personal Data Protection Act 2023 (rules notified 2025 with phased implementation); Election Commission advisories	Consent or legitimate use; notice; consent managers; significant data fiduciaries with DPO and audit duties; children's data with verifiable consent; the Election Commission's 2024 advisories require labeling of AI content and removal of deepfakes within hours during campaigns	Data Protection Board with penalties to INR 250 crore per breach
Singapore	Personal Data Protection Act 2012 (amended 2020); Parliamentary Elections Act; Elections (Integrity of Online Advertising) (Amendment) Act 2024; POFMA	Consent and Do Not Call registry; mandatory breach notification; online election advertising must identify the publisher and be paid for by or on behalf of registered actors; the 2024 Act bans realistic manipulated content depicting candidates during the election period; falsehood correction directions under POFMA	PDPC fines to S$1 million or 10 percent of turnover; Returning Officer directions
Indonesia	Personal Data Protection Law 27/2022 (fully effective October 2024)	GDPR-style bases and rights; political views are specific (sensitive) data; DPO duties; transfer rules; a supervisory agency still being stood up; election commission rules on campaign content	Administrative fines to 2 percent of revenue; criminal provisions
Malaysia	Personal Data Protection Act 2010, amended 2024 (phased in 2025)	Consent; breach notification and DPO appointment added in 2024; cross-border transfer whitelist replaced by adequacy assessment; Election Commission oversight of campaign material	Personal Data Protection Commissioner

JURISDICTION	INSTRUMENTS	OBLIGATIONS THAT BITE	ENFORCEMENT AND RECORD
Vietnam	Decree 13/2023 on personal data protection; Personal Data Protection Law (passed June 2025, in force January 2026)	Consent and impact assessments filed with the Ministry of Public Security; sensitive data includes political views; localization for certain operators; no political campaigning	Ministry of Public Security; fines under the 2025 law
Thailand	Personal Data Protection Act 2019 (in force 2022); Election Commission regulations	GDPR-modeled bases; political opinion sensitive; DPO for large-scale processing; the Election Commission regulates campaign spending and online material	PDPC administrative fines
Philippines	Data Privacy Act 2012; COMELEC rules on social media and AI (2025)	Consent; registration of data-processing systems; political affiliation is sensitive; COMELEC requires registration of official campaign accounts and platforms, and regulates AI-generated content in campaigns	National Privacy Commission; COMELEC
Australia	Privacy Act 1988 as amended by the Privacy and Other Legislation Amendment Act 2024; Foreign Influence Transparency Scheme Act 2018; Commonwealth Electoral Act 1918	Registered political parties are exempt from the Privacy Act (s.6C) and members of parliament for political acts (s.7C), but their vendors are not; political opinion is sensitive information; the 2024 reforms add a statutory tort for serious invasions of privacy, a children's online privacy code, automated-decision transparency and higher penalties; electoral matter must carry an authorisation statement; foreign-influence arrangements — including on behalf of foreign governments and parties — must be registered under FITS; foreign donations are restricted	Office of the Australian Information Commissioner (which settled with Meta for A$50 million in 2024 over Cambridge Analytica); Attorney-General's Department for FITS; Australian Electoral Commission
New Zealand	Privacy Act 2020; Electoral Act 1993	Principles-based regime with breach notification; election advertisements must carry a promoter statement; third-party promoters register above spending thresholds; foreign donations capped	Privacy Commissioner; Electoral Commission

Comparison matrix

Twelve jurisdictions, eight questions a compliance lead asks first.

JURISDICTION	POLITICAL OPINION SENSITIVE?	PARTIES EXEMPT?	VENDOR COVERED?	AD LABELS REQUIRED?	FOREIGN-INFLUENCE REGISTER?	SYNTHETIC-MEDIA RULE?	CONSENT FOR TEXTS?	BROWSER OPT-OUT SIGNAL?
United States (federal)	No	n/a	Sectoral	Yes (FEC)	Yes (FARA)	Fraud law; FCC on voice	Yes (TCPA)	No
California	No	Yes	Yes	Yes (state)	—	Yes (partly enjoined)	Yes	Yes
Canada (federal)	No	Yes (PIPEDA)	Yes	Yes (tagline)	Third-party regime	No	Yes (CASL, partial)	No
Quebec	Yes (sensitive)	Partly	Yes	Yes	Provincial	No	Yes	No
European Union	Yes (Art. 9)	No	Yes	Yes (2024/900)	Transparency register	Yes (AI Act)	Yes (ePrivacy)	No
United Kingdom	Yes	Sch. 1 condition	Yes	Yes (imprints)	Yes (FIRS)	No (fraud law)	Yes (PECR)	No
Germany	Yes	No	Yes	Yes	EU register	Yes (AI Act)	Yes	No
Brazil	Yes	No	Yes	Yes (TSE)	No	Yes (ban and label)	Consent-based	No
India	No list	No	Yes	ECI rules	No	ECI advisories	Consent-based	No
Japan	Creed	No	Yes	Election law	No	No	Opt-out	No
South Korea	Yes	No	Yes	Yes	No	Yes (90-day ban)	Yes	No
Australia	Yes	Yes (s.6C)	Yes	Yes (authorisation)	Yes (FITS)	No (SA/ACT truth laws)	Spam Act consent	No

Cross-cutting analyses

Consent standards, compared

REGIME	STANDARD FOR ORDINARY DATA	STANDARD FOR SENSITIVE DATA	STANDARD FOR TEXTS AND EMAIL
GDPR / UK GDPR	A lawful basis; consent must be freely given, specific, informed, unambiguous, withdrawable	Explicit consent or a narrow condition; profiling on political opinion needs the former	Consent (ePrivacy / PECR), narrow existing-customer exception
U.S. state laws	Notice; opt-out of sale, sharing, targeted advertising and profiling	Opt-in (most states); Utah and Iowa opt-out; Maryland bans sale	TCPA prior express consent for autodialed or prerecorded messages
Canada (PIPEDA / Law 25)	Meaningful consent proportionate to sensitivity; Law 25 consent by purpose	Express consent	CASL express or implied consent; donation solicitations exempt
Brazil LGPD	Ten legal bases including legitimate interest	Specific, highlighted consent	Consent or legitimate interest with opt-out; electoral rules on messaging
Australia / New Zealand	Notice and reasonable expectation; consent for secondary use	Consent	Spam Act / Unsolicited Electronic Messages Act consent; electoral messages partly exempt
Japan / Korea	Purpose notice (Japan); consent (Korea)	Consent (both)	Opt-out (Japan); consent (Korea)

Cross-border transfers

Programs run from seven offices move data across borders by design, and the mechanisms are settled but fragile. Transfers out of the EU and the UK rest on adequacy (the EU–U.S. Data Privacy Framework for certified U.S. importers, which survived the General Court's judgment in *Latombe* in September 2025; the UK extension; adequacy for Japan, Korea, Canada and others), on standard contractual clauses with a transfer impact assessment, or on binding corporate rules. Brazil's ANPD regulation (2024) adds standard clauses of its own; Saudi Arabia, Turkey and China require adequacy or safeguards and, in China's case, security assessment; India permits transfers except to blacklisted countries; Vietnam and Indonesia impose filing or localization duties on certain operators. The practical rule for institutional mandates is in-country holding with replication attestations, decided in the terrain brief rather than discovered at close.

Synthetic media, three theories

THEORY	WHERE	WHAT IT REQUIRES	LITIGATION AND LIMITS
Disclosure	EU AI Act Art. 50; roughly half of U.S. states; Brazil TSE; China; Korea outside the ban window; platform policies	A label that content is AI-generated or materially altered, in the statute's wording, at the point of display	The most durable theory; a U.S. court enjoined a California statute whose disclosure format was found to burden speech, so format matters

THEORY	WHERE	WHAT IT REQUIRES	LITIGATION AND LIMITS
Prohibition near elections	Korea (ninety days), Singapore (election period), Brazil (campaign period), several U.S. states (candidate deepfakes within 60–120 days)	No realistic manipulated depiction of a candidate in the window, with takedown and injunctive remedies	U.S. bans face First Amendment challenges; outside the U.S. they are enforced
Fraud and impersonation	FCC (artificial voice), FEC §30124, state consumer-fraud statutes, tort law	No deceptive impersonation of a candidate or official; consent rules for synthetic voice calls	The New Hampshire robocall forfeiture and the parallel criminal case show the theory works without new statute

Data brokers and provenance

Four U.S. states register brokers (Vermont since 2019, California since 2020 with the CPPA's Delete Act regime, Texas since 2023, Oregon since 2024); California's DROP mechanism requires registered brokers to process consumer deletion requests from August 2026 and to be audited from 2028; the FTC's 2024 orders bar the sale of sensitive location data by specific brokers and signal the theory for others; the EU and UK reach the same activity through records of processing, legitimate-interest assessments and the objection right. A provenance record — source, license, permitted purpose, registration status, refresh cadence, retention — is the document every regime asks for first, and the one most programs cannot produce.

Enforcement that changed the work

YEAR	ACTION	WHAT IT ESTABLISHED
2018	ICO fines Facebook £500,000 (Cambridge Analytica); ICO report "Democracy disrupted?"	Harvested profile data used for political profiling is a data-protection breach; regulators will audit parties and vendors
2019	FTC order against Cambridge Analytica; Canadian and BC commissioners' joint finding against Facebook; Spain's Constitutional Court strikes LOREG Art. 58 bis; Italy's Garante fines the Rousseau platform	Deceptive harvesting is an unfair practice; platforms are accountable for third-party apps; parties cannot compile opinions without a precise legal basis; party platforms must secure and limit profiling
2020	ICO audits of UK political parties; Israel's voter-registry leak through a campaign app	Published recommendations on lawful basis, transparency and vendor contracts; registry access conditioned after a breach
2021	Supreme Court, Facebook v. Duguid	The TCPA autodialer definition is narrow; peer-to-peer texting is outside it, prerecorded and artificial voice are not
2023–2024	FTC orders against X-Mode/Outlogic and InMarket; FTC v. Kochava proceeds	Sale of sensitive location data can be an unfair practice; deletion and minimization by order
2024	FCC declaratory ruling on AI voices; $6 million forfeiture over the New Hampshire primary robocall; Australia's OAIC settles with Meta for A$50 million; Brazil's TSE applies its AI rules in municipal elections; Korea prosecutes deepfake campaign content	Synthetic voice needs consent like any artificial voice; the Cambridge Analytica exposure is priced; election authorities will remove and sanction synthetic content
2025	Eleventh Circuit vacates the FCC's one-to-one consent rule; FIRS commences in the UK; the General Court upholds the EU-U.S. Data Privacy Framework; the CPPA's first enforcement actions on opt-out mechanics; Texas actions on driving-data brokers; Meta and Google withdraw political ads from the EU ahead of Regulation 2024/900	Consent rules will be litigated at the margin; foreign-influence registration is live in the UK; transfers rest on the DPF; opt-out flows are audited; platform withdrawal is a compliance outcome to plan around
2026	California DROP deletion processing from August; EU AI Act Art. 50 and high-risk duties from August; Chile's law in force in December	Broker deletion at scale; labeling of synthetic content as a legal duty in the EU; another GDPR-modeled regime in Latin America

The day-ten compliance review

What the firm's compliance lead and counsel of record sign before any program goes on air, and what any client can ask its vendor to produce.

ITEM	QUESTION ANSWERED	EVIDENCE
Acceptance screen	Who is the client, where do the funds come from, what is the purpose, which jurisdictions does the work touch, is any party sanctioned	Screening record; declination letter if any
Registration	Does FARA, the LDA, FIRS, FITS, a third-party regime or a transparency register apply, and was the filing made before activity	Filing receipts with dates preceding the first activity
Practice wall	Is this candidate or independent-expenditure work, and is the firewall documented for the cycle	Wall certification; team and system assignments
Provenance	For every data source: license, permitted purpose, broker registration, refresh, retention; no sensitive categories; no minors; voter-file terms honored	Provenance record per source
Legal basis and consent	For each jurisdiction: the basis for processing; consent held for texts, email and calls; objection and opt-out honored as suppression	Consent logs; suppression list; DPIA where required
Models	No model reconstructs an excluded attribute; model cards on file; the program predicts responsiveness, not vote	Proxy-reconstruction test results; model cards
Disclaimers and imprints	Exact language per jurisdiction and channel on every master; sponsor verification on every seat	Master approval records; platform verification screenshots
Synthetic media	No synthetic depictions of real people; AI-assisted content labeled where required	Studio attestation; labeling log
Calls and texts	Consent basis by channel; identification scripts; hours by time zone; no artificial voice	Platform configuration; scripts
Transfers and residency	Mechanism for each cross-border flow; in-country holding where required	Transfer assessment; residency attestation
Retention and destruction	Program data destroyed within ninety days of close with certification; holdout assignment retained per the client's instruction	Destruction certificate at close
Sign-off	Compliance lead and counsel of record sign; delivered to the client	Signed review

Questions to bring to counsel

- Which of the jurisdictions the program touches treat a persuadability score as political-opinion data, and what is our basis there?
- Which registrations must be filed before the first activity, and who is the local partner of record in each market?
- Are any of our data licensors required to be registered as brokers where they operate, and are they?
- What consent do we hold for texts and email in each jurisdiction, who holds it, and how is revocation propagated across channels within ten business days?

- Which state or national synthetic-media rules apply to our creative, what wording do they require, and which are currently enjoined?
- What is the transfer mechanism for each cross-border flow, and does any mandate require in-country holding?
- Which platform policies, as of this week, would reject or restrict the placements in the media plan?
- What does the client's own counsel need from us to certify the wall, the disclaimers and the media trail?

Download and citation

The packs are published as a single PDF, updated with the site: the brwrks.com/compliance page. Cite as: Brushworks (2026), *The compliance packs: what data and political firms must obey, country by country*, second edition, September 2026. Corrections and updates to research@brwrks.com; we publish them with a dated note.

Second edition, reviewed September 2026. These summaries are general information, not legal advice, and do not create a professional relationship; thresholds, dates and case outcomes should be verified against primary sources before any decision, and counsel consulted in each jurisdiction.