Privacy Foundations

Certified Information Privacy Professional/United States

KNOWLEDGE CHEATSHEET

PRIVACY PROGRAM LIFECYCLE

Map — Data and purposes → **Assess** — Risks and law → **Control** — Uses and access → **Review** — Evidence and change

01 Privacy foundations and program governance

The U.S. legal framework

- **Sectoral privacy law** combines federal statutes, state laws, regulations, common law and enforceable promises. Identify the actor, data, activity and jurisdiction before choosing a rule.
- **Subject matter jurisdiction** concerns a court's authority over the type of dispute; **personal jurisdiction** concerns its authority over the parties. Venue identifies the appropriate location.
- **Federal preemption** can displace state rules, preserve stronger protections or govern only a specific issue. HIPAA generally preserves more protective state privacy law; CAN-SPAM broadly preempts email-specific state regulation, with exceptions.
- **Statutes** come from legislatures; agencies issue authorized regulations; courts interpret law. **Stare decisis** concerns precedent. A private right of action authorizes an individual lawsuit; agency enforcement is a separate route.

FTC authority and remedies

- **FTC Act Section 5** prohibits unfair or deceptive acts or practices. FTC jurisdiction has statutory limits, including important banking, nonprofit and common-carrier exclusions; another regulator may govern an excluded activity.
- **Deception** involves a material representation, omission or practice likely to mislead a reasonable consumer. Inaccurate privacy promises, hidden disclosures and materially inconsistent uses can create exposure.
- **Unfairness** requires substantial consumer injury that is not reasonably avoidable and is not outweighed by countervailing benefits. Unreasonable security can be unfair even without a misleading privacy notice.
- **Consent orders** settle enforcement disputes and impose binding obligations; a court-approved settlement is a **consent decree**. Remedies can include injunctions, monitoring and assessments. Penalty authority depends on the legal basis.
- **Agency roles:** FTC covers broad consumer protection; HHS OCR enforces HIPAA civil requirements; FCC regulates relevant communications practices; CFPB and financial regulators oversee financial activities. Commerce supports privacy policy and transfer programs; NIST develops standards.

Privacy Foundations

Certified Information Privacy Professional/United States

KNOWLEDGE CHEATSHEET

PRIVACY PROGRAM LIFECYCLE

Map — Data and purposes → **Assess** — Risks and law → **Control** — Uses and access → **Review** — Evidence and change

Fair information practices and choice

- **FIPPs** emphasize transparency, purpose specification, collection and use limits, data quality, security, individual participation and accountability. **Privacy by Design** embeds these protections throughout development and operation.
- **Notice** explains practices; **consent** authorizes a defined activity. Opt-in requires affirmative action; opt-out permits an activity until declined. Implied consent is contextual and cannot replace legally required express consent.
- **Context matters:** fulfillment and legally required disclosures may not require a separate choice, while sensitive or unexpected uses may require affirmative permission. A notice alone does not legalize every use.
- **Layered and just-in-time notices** pair accessible detail with information at the collection point. Material retroactive changes to existing privacy commitments may require affirmative consent, rather than merely posting a revised notice.

Inventory, classification and retention

- **Data inventories and flow maps** identify collection sources, data categories, purposes, systems, recipients, storage locations and retention. Interview business owners and inspect workflows when documentation is incomplete.
- **Data classification** matches safeguards to sensitivity and risk. Apply least privilege, separate sensitive datasets and avoid giving every employee access to all records.
- **Retention schedules** connect each category to a justified business or legal need. Delete securely when that need ends; preserve records covered by a legal hold. Apply the schedule to vendors, replicas and backups.
- **Program governance** assigns accountable owners, involves all departments, trains staff and checks actual practices. Public promises must be achievable; internal procedures should explain how each team meets the same policy.

Vendor oversight and security controls

- **Vendor due diligence** examines security, workforce training, subprocessors, financial viability and incident history. Oversight continues after contracting; a certification or audit report is evidence, not a compliance guarantee.
- **Contracts** should define permitted purposes, access, confidentiality, safeguards, incident reporting, subcontractors, audit rights, rights-request assistance and return or deletion. Confirm performance and deletion when the relationship ends.
- **Risk-based security** combines administrative, technical and physical safeguards. Use MFA, role-based access, patching, logging, phishing training and tested response plans; separate encryption keys from protected data.
- **De-identification** reduces identifiability only when its legal and technical conditions are met. Hashing, tokenization or removing names alone may leave linkable personal data. Insurance and indemnities allocate loss without replacing controls.

Privacy Foundations

Certified Information Privacy Professional/United States

KNOWLEDGE CHEATSHEET

PRIVACY PROGRAM LIFECYCLE

Map — Data and purposes → **Assess** — Risks and law → **Control** — Uses and access → **Review** — Evidence and change

International privacy and transfers

- **GDPR controller** determines purposes and means; a **processor** acts on documented instructions. U.S. service-provider and HIPAA business-associate roles have their own definitions; classify the actual activity.
- **GDPR scope** can reach U.S. organizations through an EU establishment, offering goods or services to people in the EU, or monitoring their behavior there. A company's European presence does not automatically extend every right worldwide.
- **Transfer mechanisms** include applicable adequacy arrangements, standard contractual clauses and binding corporate rules. SCC-based transfers require assessment of destination risks and effective supplementary measures where needed.
- **Schrems II** invalidated Privacy Shield, an older transfer arrangement. The **Data Privacy Framework** imposes principles on participating organizations, including access, independent complaint recourse and accountability for onward transfers.
- **UK transfers** require a UK-valid route, such as an applicable adequacy arrangement, IDTA or UK Addendum to EU SCCs. EU transfer documents alone do not automatically satisfy UK requirements.
- **APEC Privacy Framework** principles include preventing harm, notice, collection limits, use limits, choice, integrity, security, access/correction and accountability. **CBPR** certification supports accountable cross-border practices; it does not displace local law. **GPEN** supports cooperation among privacy authorities.

AI, profiling and data ethics

- **AI governance** starts with a defined purpose, lawful inputs, data minimization and risk assessment. Publicly accessible or scraped data can still trigger privacy, contract, consumer-reporting and discrimination duties.
- **Automated decisions** need accurate data, explainable outcomes, bias testing and suitable human review. A proprietary model does not excuse adverse-action explanations or unlawful disparate impact.
- **Sensitive inferences** can reveal health, religion or other protected traits without collecting them directly. Assess outputs and downstream uses, rather than only the input fields.
- **Data protection assessments** document benefits, foreseeable harms, safeguards and residual risk for covered high-risk processing. Ethical review, audit and accountability supplement legal compliance; automation itself is not a privacy safeguard.

Private-sector Privacy

Certified Information Privacy Professional/United States

KNOWLEDGE CHEATSHEET

MATCH THE LAW TO THE ACTIVITY

- **Finance** — GLBA and FCRA
- **Health** — HIPAA and apps
- **Children** — COPPA and FERPA
- **Marketing** — Email and calls

02 Private-sector privacy laws

GLBA: financial privacy and safeguards

- The **Gramm-Leach-Bliley Act (GLBA)** applies based on covered financial activities, not simply whether an organization calls itself a bank or charges a fee. **Nonpublic personal information (NPI)** includes covered information obtained through consumer financial relationships.
- **Consumer** is broader than **customer**, who has a continuing relationship. Required notices explain categories collected and disclosed, recipient categories, choices and security practices. Annual customer notices have a conditional statutory exception.
- **Privacy Rule:** certain nonaffiliate disclosures require notice and an opportunity to opt out. Exceptions include specified servicing and processing activities. Affiliate sharing and marketing also require analysis under FCRA and FACTA.
- **Safeguards Rule** requires an information security program for covered institutions. **Pretexting** restrictions target obtaining financial information by false pretenses. Limits on sharing account numbers for marketing are distinct from ordinary processing exceptions.

FCRA: consumer reports and employment

- The **Fair Credit Reporting Act (FCRA)** regulates consumer reporting agencies, furnishers and users of consumer reports. Reports can concern credit, character or other attributes and support credit, insurance, employment and other specified eligibility decisions.
- **Permissible purpose** is required to obtain or use a consumer report. Verify the intended purpose; publicly sourced information can still form a regulated report when assembled and used for covered decisions.
- **Employment screening** generally requires a clear, conspicuous standalone disclosure and written authorization before procuring a report. State laws may further restrict credit checks and investigative consumer reports.
- **Pre-adverse action:** before an employment decision based on a report, provide the report and a summary of FCRA rights, allowing a reasonable opportunity to respond. **Final adverse-action notice** identifies the CRA and explains dispute and report rights.
- **Accuracy and disputes:** CRAs must follow reasonable procedures and investigate disputes, generally within 30 days, subject to extensions. Obsolete-information limits vary by record and exception. Negligent and willful violations have different remedies.

Private-sector Privacy

Certified Information Privacy Professional/United States

KNOWLEDGE CHEATSHEET

MATCH THE LAW TO THE ACTIVITY

- **Finance** — GLBA and FCRA
- **Health** — HIPAA and apps
- **Children** — COPPA and FERPA
- **Marketing** — Email and calls

FACTA, identity theft and financial decisions

- The **Fair and Accurate Credit Transactions Act (FACTA)** amended FCRA with identity-theft protections, free annual file disclosures, fraud alerts and receipt truncation. Electronic card receipts generally omit expiration dates and show no more than the last five account digits.
- **Disposal Rule** requires reasonable measures when disposing of consumer-report information. Shred or destroy paper and securely erase electronic records; mere tearing or ordinary file deletion may be inadequate.
- **Red Flags Rule** requires covered financial institutions and creditors with covered accounts to detect, prevent and mitigate identity theft through a written program. Evaluate coverage before assuming every business is a creditor.
- **Misconduct investigations** can fall outside ordinary FCRA consumer-report procedures when statutory conditions are met; adverse actions can still trigger a later summary disclosure. This is a limited exception, not a general exemption for background checks.
- **Dodd-Frank** addresses unfair, deceptive or abusive financial practices and established the CFPB. **ECOA** prohibits covered credit discrimination and requires adverse-action reasons. **FDCPA** constrains covered debt collectors, including improper third-party disclosures.

HIPAA: actors, information and rights

- The **Health Insurance Portability and Accountability Act (HIPAA)** covers health plans, clearinghouses and providers conducting covered electronic transactions. A pharmaceutical company, employer or fitness app is not automatically a **covered entity** merely because it handles health information.
- **PHI** is identifiable health information held or transmitted in a covered HIPAA role; the Privacy Rule covers oral, paper and electronic forms. The Security Rule applies to **ePHI**. Employment records held as employer records are excluded from PHI.
- **Business associates** perform covered functions or services involving PHI for covered entities. Billing and cloud-storage vendors may qualify. A **BAA** governs uses and safeguards; relevant subcontractors need corresponding written assurances.
- **Individual rights** include access, amendment requests and an accounting of certain disclosures. A direct-treatment provider generally supplies its notice at first service, makes it available and seeks acknowledgment; a new copy at every visit is unnecessary.

Private-sector Privacy

Certified Information Privacy Professional/United States

KNOWLEDGE CHEATSHEET

MATCH THE LAW TO THE ACTIVITY

- **Finance** — GLBA and FCRA
- **Health** — HIPAA and apps
- **Children** — COPPA and FERPA
- **Marketing** — Email and calls

HIPAA: permitted uses and authorization

- **Treatment, payment and healthcare operations (TPO)** generally permit PHI use and disclosure without a separate patient authorization. Permission under HIPAA does not eliminate applicable conditions or other legal restrictions.
- **Minimum necessary** limits covered uses, requests and disclosures to the needed information. Important exceptions include treatment disclosures to healthcare providers, disclosures to the individual and uses under a valid authorization.
- **Public health, abuse reporting and law enforcement** have specific permission pathways. Check the precise condition and legal process; a police request alone does not authorize unrestricted release of a patient record.
- **Litigation disclosures** may follow an appropriate court order or, for specified other process, satisfactory assurances of notice or a qualified protective order. Limit the response to the authorized information.
- **Authorization** is generally needed for uses outside permitted pathways, including many marketing uses and sales of PHI. Research may use authorization, an approved waiver or another applicable route. Identifying a patient in a personal paper needs its own lawful basis.

HIPAA: security, breaches and special records

- **Security safeguards** are administrative, physical and technical. Conduct risk analysis, train staff, control access and evaluate vendors. An addressable specification requires a documented assessment; it is not simply optional.
- **Breach analysis** starts with an impermissible use or disclosure of unsecured PHI, subject to exceptions or a documented low probability of compromise. Consider the data, recipient, actual acquisition/viewing and mitigation; ransomware can trigger this analysis.
- **Individual breach notices** are due without unreasonable delay and within 60 days of discovery. Notify HHS within 60 days for breaches affecting at least 500 people; smaller breaches may be reported within 60 days after year-end.
- **Media notice** is required when more than 500 residents of a state or jurisdiction are affected. A business associate notifies the covered entity; contracts may require faster reporting. State obligations can also apply.
- **HITECH** strengthened health-information privacy, security and breach duties and supported electronic health records. **42 CFR Part 2** separately protects covered substance-use-disorder patient records. **GINA** addresses genetic discrimination in health insurance and employment, generally not life, disability or long-term-care insurance.

Private-sector Privacy

Certified Information Privacy Professional/United States

KNOWLEDGE CHEATSHEET

MATCH THE LAW TO THE ACTIVITY

- **Finance** — GLBA and FCRA
- **Health** — HIPAA and apps
- **Children** — COPPA and FERPA
- **Marketing** — Email and calls

COPPA and online services for children

- The **Children's Online Privacy Protection Act (COPPA)** covers operators of child-directed websites or online services, and operators with actual knowledge they collect personal information online from children under 13. FTC rules also address covered third-party collection.
- **Verifiable parental consent** generally precedes covered collection, use or disclosure unless an exception applies. A parent-directed text or passive permission to use the internet is not itself verified consent.
- **Operator duties** include clear notices, parental review and deletion controls, reasonable security, limited retention and collecting only what is reasonably necessary. Persistent identifiers can be personal information even without a child's name.
- **Safe harbor** means participation in an FTC-approved self-regulatory program, not merely publishing a notice. A school's limited educational consent does not authorize unrelated commercial exploitation of children's data.

FERPA and education records

- The **Family Educational Rights and Privacy Act (FERPA)** applies to covered educational institutions receiving relevant federal funding. Education records are directly related to a student and maintained by the institution or its agent; record format does not determine coverage.
- **Rights transfer** from parents to the eligible student at age 18 or attendance at a postsecondary institution, whichever comes first. Access must generally be provided within 45 days; amendment and hearing rights address inaccurate or misleading records.
- **Disclosure** generally requires consent unless an exception applies. Examples include legitimate educational interests, qualifying school transfers, specified emergencies and disclosure to parents of tax-dependent eligible students.
- **Directory information** may be disclosed after proper designation, notice and an opportunity to opt out. Sole-possession notes and qualifying law-enforcement-unit records are separate exclusions; a vendor's copies of education records do not automatically lose protection.
- **School-official vendors** must meet the applicable exception, including institutional control over use and maintenance and restricted use/redisclosure. Limit access to legitimate educational needs; independent public apps are not automatically governed by FERPA.

Private-sector Privacy

Certified Information Privacy Professional/United States

KNOWLEDGE CHEATSHEET

MATCH THE LAW TO THE ACTIVITY

- **Finance** — GLBA and FCRA
- **Health** — HIPAA and apps
- **Children** — COPPA and FERPA
- **Marketing** — Email and calls

CAN-SPAM and online advertising

- **CAN-SPAM** generally uses an opt-out model for commercial email, including business-to-business messages. Use accurate routing information and subjects, identify advertising as required, include a valid physical address and offer a clear unsubscribe method.
- **Unsubscribe requests** must be honored within 10 business days; the mechanism must remain available for at least 30 days after sending. Do not charge a fee or demand unnecessary personal information. Hiring an email vendor does not remove responsibility.
- **Transactional or relationship messages** follow a different rule set; mixed messages depend on their primary purpose. CAN-SPAM does not generally require advance opt-in for every advertising email.
- **AdChoices** provides notice and access to behavioral-advertising choices under industry self-regulation. It does not mean the industry sponsored an ad or that statutory duties are satisfied. Mobile carrier-domain messages can invoke additional FCC rules.

Telephone marketing and preferences

- **TCPA and FCC rules** address covered calls, texts, artificial/prerecorded voices and consent. **TSR and FTC rules** govern covered telemarketing sales practices. Check both regimes, plus state requirements.
- **Do Not Call** compliance requires applicable registry screening and company-specific suppression. Under the TSR, calls generally occur only from 8 a.m. to 9 p.m. at the recipient's location; identify the seller and sales purpose as required.
- **Established business relationships** can support limited live-call exceptions, but do not override a company-specific do-not-call request. Applicable written permission identifies the number and includes the consumer's signature.
- **Preference management** must work across channels, agents and relevant divisions. State registration, calling restrictions and do-not-call lists may add duties. Nonprofits calling for themselves and for-profit charitable telefunders can have different TSR treatment.

Private-sector Privacy / Government Access

Certified Information Privacy Professional/United States

KNOWLEDGE CHEATSHEET

MATCH THE LAW TO THE ACTIVITY

- **Finance** — GLBA and FCRA
- **Health** — HIPAA and apps
- **Children** — COPPA and FERPA
- **Marketing** — Email and calls

Other protected records and health apps

- **VPPA** restricts disclosure of covered consumers' identifiable video-viewing information, subject to statutory exceptions. **Cable privacy law** addresses subscriber notice, consent exceptions, access and destruction when information is no longer needed.
- **DPPA** restricts obtaining, using and disclosing personal information from state motor-vehicle records. Permissible uses include specified governmental, insurance and litigation activities; bulk marketing requires the applicable express consent.
- **Consumer health apps** may fall outside HIPAA yet remain subject to FTC Act duties, state laws and the **FTC Health Breach Notification Rule**. Covered PHR vendors, related entities and service providers have distinct notification responsibilities.
- **FTC health-breach scope** can include apps with the technical capacity to draw identifiable health information from multiple sources. Unauthorized disclosures can qualify without a hacker. Evaluate role, data and incident facts rather than assuming every wellness app is covered.
- **Contact-tracing apps** face a patchwork of laws. Limit collection, uses, access and retention; assess confidentiality and meaningful user choice.
- **State insurance departments** supervise insurers. The National Association of Insurance Commissioners' **model AI bulletin** guides governance, with legal effect depending on state action and existing law.

03 Government access and legal process

Constitutional and government-record protections

- **Constitutional privacy protections** primarily constrain government action. Courts have derived privacy protections from specific guarantees and due process. The Fourth Amendment addresses unreasonable searches and seizures; statutes and state law can provide additional protection.
- **Reasonable expectation of privacy** and the nature of the search affect Fourth Amendment analysis. Government collection of device or location information requires its own legal analysis; a private employer's program is not automatically a constitutional search.
- **Privacy Act** governs covered federal agency systems of records retrieved by personal identifier. It establishes notice, access, amendment and disclosure controls, with defined exceptions and exemptions, including some law-enforcement records.
- **FOIA** provides access to federal agency records subject to exemptions, including personal privacy and law-enforcement protections. The **E-Government Act** requires privacy impact assessments for specified federal information activities.

Government Access

Certified Information Privacy Professional/United States

KNOWLEDGE CHEATSHEET

EVALUATE A DISCLOSURE DEMAND

Authority Validate process → **Scope** Identify records → **Protect** Review and limit → **Respond** Authorized data

ECPA: interception versus stored access

- **ECPA** includes the Wiretap Act, Stored Communications Act and pen-register provisions. Distinguish interception of communications in transit, access to stored communications, and collection of dialing/routing information.
- **Wiretap Act consent** can permit interception when a party consents under federal law, subject to limitations. Some states require all-party consent; the federal one-party baseline does not resolve every recording question.
- **Provider and ordinary-course exceptions** are limited by their statutory purposes. Business phone monitoring does not authorize unlimited interception of personal calls merely because the employer owns the equipment.
- **Stored Communications Act** regulates unauthorized stored access and provider disclosure. Legal process differs for content and noncontent records. Consent to use an employer device does not automatically authorize access to every personal cloud account.
- **Computer-trespasser interception** has a limited exception involving owner authorization and a qualifying lawful investigation. An existing contractual user is not automatically a trespasser; ordinary employee surveillance is not justified merely by invoking cybersecurity.

National security and overseas data

- **FISA** establishes foreign-intelligence surveillance procedures. The **Section 702** framework concerns targeting non-U.S. persons reasonably believed outside the United States, with certification, targeting and minimization controls; it is not blanket authority to target Americans.
- **USA PATRIOT Act** expanded specified investigative authorities. **USA FREEDOM Act** curtailed the former bulk telephone-records program. Distinguish these historical changes from whether a particular authority is presently available.
- **CLOUD Act** addresses provider obligations for data within possession, custody or control even when stored abroad, and supports qualifying international agreements. It does not make every subpoena sufficient to obtain email content or eliminate conflict-of-law challenges.
- **CALEA** requires interception capability for covered communications services. It does not impose a universal duty to decrypt customer encryption when the carrier did not provide it and lacks the decryption information.

Government Access / Workplace Privacy

Certified Information Privacy Professional/United States

KNOWLEDGE CHEATSHEET

EVALUATE A DISCLOSURE DEMAND

- **Authority** — Validate process
- → **Scope** — Identify records
- → **Protect** — Review and limit
- → **Respond** — Authorized data

Disclosure demands and preservation

- **Legal demands** require validation of authority, jurisdiction, scope, confidentiality restrictions and deadlines. A subpoena, warrant and court order are different tools; challenge overbroad demands and disclose only authorized information.
- **E-discovery** covers identification, preservation, collection, review and production of relevant electronically stored information. Suspend ordinary deletion under a legal hold; spoliation can lead to sanctions.
- **Protective orders, redaction and privilege review** reduce unnecessary disclosure. Cross-border discovery may also trigger GDPR restrictions; a foreign demand is not automatically a valid international-transfer basis.
- **RFPA** limits federal government access to covered customer financial records with procedures and exceptions. **Bank Secrecy Act** reporting duties are separate. The **Privacy Protection Act** restricts specified government searches for journalistic work product and documentary materials.

04 Workplace privacy

Employee monitoring and common-law claims

- **Private-sector monitoring** is governed by statutes, state law, contracts and torts. Federal constitutional restrictions generally do not apply directly to an ordinary private employer; public employment requires separate analysis.
- **Notice and proportionate scope** help define employee expectations but do not waive every legal protection. Assess the business purpose, location, data captured, off-duty activity, access and retention before monitoring.
- **Intrusion upon seclusion** generally concerns intentional, highly offensive intrusion into private affairs. Changing-room cameras or remote webcams capturing home life pose stronger concerns than limited monitoring of public business activity.
- **Privacy torts** also include public disclosure of private facts, false light and appropriation of name or likeness, subject to state recognition. Negligence requires duty, breach, causation and harm; breach litigation may also allege contract or fiduciary duties.

Workplace Privacy / State Privacy

Certified Information Privacy Professional/United States

KNOWLEDGE CHEATSHEET

PROPORTIONATE WORKPLACE CONTROLS

- **Purpose** — Business need
- → **Notice** — Set expectations
- → **Limit** — Access and scope
- → **Review** — Rights and effects

Hiring, screening and protected characteristics

- **Anti-discrimination laws** restrict decisions based on protected characteristics and shape lawful inquiries. Title VII, ADA, ADEA, Equal Pay Act and pregnancy protections address different categories; state laws may add protections.
- **ADA** restricts pre-offer disability inquiries and medical examinations. Distinguish current illegal drug use from protected recovery or disability issues. Do not treat consent as a complete defense to an unlawful inquiry.
- **EPPA** generally restricts private employers' use of lie-detector tests, with limited statutory exceptions and procedural safeguards. Personality or honesty questionnaires are not automatically polygraph tests.
- **Background checks** combine FCRA procedures with state restrictions, including California investigative-report rules. Social-media screening and AI video analysis can reveal protected traits; examine job relevance, model features and disparate effects.

Medical records, BYOD and employee rights

- **Employee medical and genetic records** need restricted access and separate handling under applicable ADA, GINA and leave rules. FMLA certifications and OSHA records have specific purposes; ordinary employer health records are not automatically HIPAA PHI.
- **BYOD and remote work** require clear boundaries for work data, location tracking, device access, backups and remote wipe. Prefer separating work information from personal content and limiting off-hours collection.
- **NLRA** can protect concerted employee activity, including some workplace discussions on social media. Monitoring policies and discipline must account for these rights, not only privacy notices.
- **Former employees** retain relevant record and privacy protections. Revoke operational access promptly while securely retaining required records. Neither immediate deletion of every file nor indefinite retention of everything is a sound default.

05 State privacy, biometrics and breach response

State-law applicability and enforcement

- **Applicability** depends on the law's business nexus, thresholds, data, actor and activity. Physical presence is not always required. A business-contact or employee record may be covered under one law and excluded under another.
- **Entity exemptions** exclude qualifying organizations; **data exemptions** exclude specified processing or information. California's GLBA-related exemption is generally data-based; Virginia exempts covered financial institutions and specified HIPAA entities as well as certain data.

State Privacy

Certified Information Privacy Professional/United States

KNOWLEDGE CHEATSHEET

STATE-LAW ANALYSIS

Scope Actor and data → **Rights** Requests and choice → **Security** Controls and risk → **Breach** Triggers and notice

- **State UDAP laws** prohibit unfair or deceptive practices and may support attorney-general or consumer actions, depending on the statute. Comprehensive privacy statutes have their own enforcement and remedy provisions.
- **Cure periods** provide a specified chance to remedy an alleged violation before enforcement when available. They differ by statute and may expire; do not assume every violation carries a permanent right to cure.

California: CCPA as amended by CPRA

- **CCPA/CPRA** rights include knowing/accessing information, deletion, correction, sale/sharing opt-out, limiting specified sensitive-information uses and nondiscrimination. Rights have defined conditions and exceptions; CPRA amended CCPA rather than replacing it.
- **Personal information** includes linked identifiers, household/device data and qualifying inferences. Masked or tokenized data may remain covered. Employment and business-contact data are not generally excluded from California coverage.
- **Rights requests** require appropriate authentication for access, correction and deletion. An existing account can support verification, with further checks where needed. Avoid disclosing secrets or collecting excessive identity evidence.
- **Deletion and portability** require locating relevant data and coordinating with recipients as applicable. Deletion has exceptions, including qualifying security and legal needs; a portable response must protect other people's information.
- **Enforcement:** CPPA has regulatory and administrative enforcement authority; the Attorney General also has authority. The private right of action is limited to qualifying security breaches tied to unreasonable security, not every violation of a consumer right.

California: sale, sharing and service providers

- **Sale** includes covered transfers for money or other valuable consideration. **Sharing** separately covers cross-context behavioral advertising, even without payment. Cookies and tracking pixels require analysis of actual recipients and uses.
- **Service-provider and contractor exceptions** depend on qualifying roles, contractual restrictions and actual conduct. A vendor label, privacy-notice statement or absence of cash payment alone does not establish the exception.

State Privacy

Certified Information Privacy Professional/United States

KNOWLEDGE CHEATSHEET

STATE-LAW ANALYSIS

Scope — Actor and data → **Rights** — Requests and choice → **Security** — Controls and risk → **Breach** — Triggers and notice

- **Opt-out implementation** must cover sale and sharing and honor applicable opt-out preference signals, including **Global Privacy Control**. Known consumers under 16 receive special opt-in protections; parental authorization applies below 13.
- **Tracking changes** do not remove privacy duties. First-party identifiers, server-side tracking and analytics can still process personal information. Browser cookie deprecation is a technical development, not a general statutory command to delete all datasets.

Virginia and Colorado: consumer rights

- **VCDPA and Colorado Privacy Act** grant covered consumers access, correction, deletion and portability rights, plus opt-outs for specified targeted advertising, sales and significant-effect profiling. Both include an appeal process for denied requests.
- **Consumer scope** generally excludes people acting in employment or commercial contexts under these two laws. Do not infer job-applicant coverage merely because a profiling scenario resembles consumer automated decision-making.
- **Sensitive data** generally requires consent under both regimes, subject to their provisions. This differs from California's right to limit specified sensitive-information uses. Ordinary analytics is not automatically targeted advertising.
- **Assessments and contracts** address covered high-risk processing and processor duties. Virginia specifically includes targeted advertising, sales, sensitive data and risky profiling. Scope the law first; an assessment is not required simply because any corporation uses data.
- **Enforcement differs:** neither law creates a general private right of action. Colorado recognizes qualifying universal opt-out mechanisms; do not assume an identical obligation across every state. Privacy notices and consent must match each law's definitions.

Biometrics, brokers and consumer health data

- **Illinois BIPA** addresses covered biometric identifiers and information, with written notice/release, retention and destruction policies, disclosure restrictions and security duties. It restricts profiting from biometrics and permits private lawsuits.
- **Photographs versus biometric templates:** an ordinary photograph is excluded from BIPA's identifier definition, while extracting a covered face-geometry scan can trigger duties. Fingerprint or iris-based attendance and login systems require separate analysis.
- **Data brokers** aggregate information outside a direct consumer relationship. Vermont has broker registration requirements; Nevada regulates specified sales and broker activities. California's **Delete Act** adds broker duties and a centralized deletion mechanism.

State Privacy

Certified Information Privacy Professional/United States

KNOWLEDGE CHEATSHEET

STATE-LAW ANALYSIS

Scope Actor and data → **Rights** Requests and choice → **Security** Controls and risk → **Breach** Triggers and notice

- **Consumer health laws** can reach wellness data outside HIPAA. Washington's **My Health My Data Act** imposes collection/sharing consent and sale-authorization rules, with exceptions, and prohibits specified geofencing around in-person healthcare facilities; consent does not override that prohibition.
- **State security duties** include risk-based programs, secure disposal and sometimes specific encryption obligations. Massachusetts protects defined resident information regardless of the business's location. New York's **SHIELD Act** addresses safeguards and breach duties; it is not a general deletion-right law.

Breach triage and notification

- **Contain and investigate** while preserving evidence. Identify affected people, residence, data elements, access/acquisition, encryption and key exposure, discovery timing and applicable sector rules. A malware event is not automatically a notifiable personal-data breach.
- **State breach laws** exist in all 50 states but define protected information, compromise and risk exceptions differently. Name-plus-sensitive-element rules coexist with standalone credentials and other categories; check every relevant jurisdiction.
- **Encryption exceptions** depend on the statutory standard and whether keys were compromised. Access without proven export can still trigger notification. Merely complying with an internal policy or another law does not automatically excuse notice.
- **Notice obligations** can reach individuals, state authorities, consumer reporting agencies and sector regulators under different triggers. Deadlines and content vary; lawful investigative delays must meet the applicable conditions. Credit monitoring is not universally required.
- **Notification is one duty:** it does not erase liability for poor security or misuse. Card incidents may also invoke PCI and acquiring-bank obligations. Remediate causes, assess vendor failures and revise controls after the immediate response.