COMPLIANCE MAP · PART 2 OF 9

// ART-DAT-009 · PUBLISHED 24 NOVEMBER 2026

Privacy Law for SaaS: One FTC Act and Twenty-Four States

Personal data in a SaaS product is governed by the Federal Trade Commission Act, a set of narrower federal statutes, and comprehensive privacy laws in twenty-four states. The federal laws attach to kinds of data and kinds of messages; the state laws attach to where the consumer lives.

Jason Newell · MAX Research Collective · Article ART-DAT-009 · Published 24 November 2026
Licensed under the Creative Commons Attribution 4.0 International License (CC BY 4.0), https://creativecommons.org/licenses/by/4.0/
Original: https://www.maxresearchcollective.com/articles/privacy-law-for-saas.html
Cite as: Newell, J. (2026). Privacy Law for SaaS: One FTC Act and Twenty-Four States. MAX Research Collective, ART-DAT-009. https://www.maxresearchcollective.com/articles/privacy-law-for-saas.html

Part 2 of 9 in the series The Compliance Map for Web SaaS.

General information, not legal advice. Legal information current as of 22 November 2026. Laws, rules and court orders change, so check each date and threshold against the cited source before relying on it, and have a qualified lawyer review anything built or published from this map.

How to read the marks. A bracketed number points to a primary source in the sources appendix that was opened for this edition. A dagger marks a statement that names its law but whose text wasn't opened on a primary source for this edition. A dagger with a number (†6) points to the secondary reference in the secondary appendix that the statement came from, which is a law-firm alert, a tracker or trade press and never a primary source. A dagger alone (†) marks a statement that is considered but not known: it's kept so the rule stays in view, it has no reference behind it, and it hasn't been confirmed. (2026) marks a rule that is new, or first due, in 2026.

Where this part starts

4. PII: federal law

There is no federal comprehensive privacy statute. The federal layer is the FTC's general authority plus topic laws.

Table 1. Federal laws that reach personal data.

LAW	COVERS	WHAT IT REQUIRES OF A SAAS PRODUCT	ENFORCEMENT
FTC Act § 5	Unfair or deceptive practices, any company in commerce	Do what the privacy policy says; reasonable security; no dark patterns; no quiet policy change to allow new uses of old data	FTC orders, often 20 years, with required programs, audits and deletion of data and models [1]
COPPA and the amended COPPA Rule	Online collection from children under 13	Verifiable parental consent; separate consent before disclosing a child's data to third parties for advertising; a written retention policy, no indefinite retention; a written security program. Full compliance was due 2026-04-22 (2026)	FTC and state attorneys general; civil penalties per violation [2]
CAN-SPAM	Commercial email	Honest headers and subject, a postal address, a working opt-out honored within 10 business days	FTC [3]
TCPA	Calls and texts	Prior express written consent for marketing texts and autodialed calls; honoring revocation	FCC, and private suits with $500 to $1,500 per message [4]
FCRA	Consumer reports used for credit, employment, insurance, tenancy	Permissible purpose; adverse action notices; accuracy and dispute handling; disposal rule	FTC, CFPB, private suits [5]
GLBA	Financial institutions' customer data	Privacy notice and opt-out (Privacy Rule); written security program (Safeguards Rule, § 7 below)	FTC, banking regulators, CFPB [6][31]

LAW	COVERS	WHAT IT REQUIRES OF A SAAS PRODUCT	ENFORCEMENT
FERPA	Education records at schools that take federal funds	SaaS acts as a ”school official” under the school’s direct control; no use beyond the school’s purpose	Department of Education, through the school [7]
VPPA	Video viewing records	Consent before disclosing what a person watched; a source of class actions over tracking pixels on video pages	Private suits, $2,500 per violation [8]
ECPA / Wiretap Act and state wiretap laws	Interception of communications	Consent before recording or letting a third party read chats, calls and sessions. Several states need all parties’ consent, California, Florida, Illinois, Maryland, Massachusetts, Pennsylvania and Washington among them. Session-replay, chat widgets and AI note-takers are the current litigation targets	Private suits; California’s CIPA carries $5,000 per violation [9] [64]; other states †
DOJ Data Security Program (28 CFR Part 202)	Bulk sensitive personal data and government-related data	No data brokerage with, and restrictions on vendor, employment and investment agreements giving access to, six countries of concern (China, Russia, Iran, North Korea, Cuba, Venezuela) above set volumes (for example, health or financial data of more than 10,000 US persons). In force since 2025-04-08; due diligence and audit duties since 2025-10-06	DOJ, civil and criminal [10]
PADFA	Data brokers	No sale of sensitive data of US individuals to foreign adversary	FTC [11]

LAW	COVERS	WHAT IT REQUIRES OF A SAAS PRODUCT	ENFORCEMENT
		countries or companies they control	
TAKE IT DOWN Act	Platforms hosting user content	A notice-and-removal process for non-consensual intimate images, real or AI-generated, within 48 hours; in place by 2026-05-19 (2026)	FTC [12]

5. PII: state law

5.1 Comprehensive privacy laws: 24 states (2026)

Four states enacted laws in 2026 (Alabama, Louisiana, Oklahoma, Vermont), which brings the count to 24 if Florida's narrower law is counted.

Table 2. State comprehensive privacy laws by effective date.

IN EFFECT	STATE
2020 (amended 2023)	California (CCPA as amended by CPRA) †6
2023	Virginia, Colorado, Connecticut, Utah †6
2024	Texas, Oregon, Florida (very large companies only), Montana †6
2025	Iowa, Delaware, Nebraska, New Hampshire, New Jersey, Tennessee, Minnesota, Maryland †6
2026-01-01	Indiana, Kentucky, Rhode Island †6
2027-01-01	Louisiana, Oklahoma †6
2027-05-01	Alabama †6
2028-01-01	Vermont [47]

What nearly all of them share:

Table 3. Duties the state privacy laws share.

DUTY	WHAT IT MEANS IN THE PRODUCT
Privacy notice	Categories of data, purposes, who receives it, how to exercise rights. California also wants retention periods per category [64]; other states †6
Consumer rights	Access, delete, correct (not Iowa), portability, opt out of sale, targeted advertising and profiling; an appeal route; answers in 45 days [46]
Sensitive data	Opt-in consent before processing (opt-out in California, Iowa and Utah) †6
Data protection assessments	Written, before targeted advertising, sale, sensitive data processing and profiling with legal or similar effect †6
Processor contracts	Instructions, confidentiality, deletion or return, audit rights, subprocessor flow-down †6
Universal opt-out signals	Honor Global Privacy Control in a growing list of states, California, Colorado, Connecticut, Texas, Oregon, Montana, New Jersey, Delaware, Minnesota and Maryland among them †6
Data minimization	"Adequate, relevant and limited" in most; Maryland goes further: collection must be reasonably necessary for the product the consumer asked for, and sale of sensitive data is banned outright [25]
Enforcement	Attorney general only, except California (its privacy agency too, and a private right of action for breaches). Cure periods are expiring state by state †6

5.2 California's extra layer

Table 4. California's added rules and their dates.

RULE	REQUIREMENT	DATE
Risk assessments (CCPA regulations)	Before selling or sharing data, processing sensitive data, using automated decision-making for significant decisions, or training such systems on personal data	Duty began 2026-01-01; first attestations to the agency due 2028-04-01 [48]
Cybersecurity audits	Annual independent audit for businesses whose processing poses significant security risk	First certifications due 2028-04-01 (revenue over $100 million), 2029-04-01 ($50 million to $100 million), 2030-04-01 (under $50 million) [48]
Automated decision-making technology (ADMT)	Pre-use notice, opt-out and access rights when ADMT makes significant decisions (finance, housing, education, employment, health care)	2027-01-01 [48]
Delete Act	Registered data brokers must honor deletion requests made through the state's one-stop platform	Brokers process requests from 2026-08-01 (2026) [64]
Breach notice (SB 446)	Notify residents within 30 calendar days of discovery; the attorney general within 15 days of that notice when more than 500 residents	2026-01-01 (2026) [64]

5.3 Topic laws at state level

Table 5. State laws by topic.

TOPIC	LEADING LAWS	WHAT TO BUILD FOR
Biometrics	Illinois BIPA; Texas CUBI; Washington	Written consent before collecting face, voice or fingerprint identifiers; a public retention schedule (Illinois: destroy when the purpose ends or within 3 years of last interaction); no sale. BIPA has a private right of action [51][66]
Consumer health data (outside HIPAA)	Washington My Health My Data Act; Nevada SB 370; Connecticut's amendments; Virginia's reproductive health amendment	See § 6.4 [23][24][25]
Children and teens	California and Maryland age-appropriate design codes (partly enjoined); state laws limiting targeted ads and data sale for under-16 or under-18 users; app-store age verification acts in Utah, Texas and Louisiana (challenged in court)	Age signals, high-privacy defaults, no targeted ads to known minors †
Data brokers	Registration in California, Vermont, Texas and Oregon; new laws in Connecticut and New Jersey (2026)	Register and honor deletion if you sell data about people you have no direct relationship with †7
Pricing by personal data	New laws in Connecticut, Maryland and New Jersey (2026); New York's algorithmic pricing disclosure	Disclose, and in some cases stop, setting prices from personal data [67]; other states †7
Security	Massachusetts 201 CMR 17 (a written program and encryption of personal data on laptops and across public networks); New York SHIELD Act; Ohio, Utah and Connecticut safe harbors for following a recognized framework	A written information security program mapped to NIST CSF, ISO 27001 or CIS Controls [62][67]; Massachusetts †

TOPIC	LEADING LAWS	WHAT TO BUILD FOR
Wiretap and recording	California CIPA, and all-party consent laws in Florida, Illinois, Maryland, Massachusetts, Pennsylvania, Washington and others	Consent banners that cover session replay, chat transcripts and call recording; vendor contracts that bar the vendor's own use [64]; other states †
Auto-renewal	California's automatic renewal law and similar laws in many other states, over the federal floor in the Restore Online Shoppers' Confidence Act	Clear terms before charging, affirmative consent, and cancellation as easy as sign-up [63][64]; other states †

Why it matters

State attorneys general enforce almost all of this, and cure periods are ending state by state. A product that honors the shared duties once, including the opt-out signal and the sensitive-data consent, meets most of the list. The state that a company never marketed to still counts once its residents sign up.

Appendix A: the series

Section numbers run through the whole series, so a reference to a section outside this part points to the part that holds it.

- Part 1, SaaS Compliance Basics: sections 1, 2, 3.
- Part 2, Privacy Law for SaaS: sections 4, 5.
- Part 3, HIPAA for SaaS: sections 6.
- Part 4, Payment and Financial Data in SaaS: sections 7.
- Part 5, Security Controls for Regulated SaaS: sections 8, 9, 10.
- Part 6, Data Retention and Consent in SaaS: sections 11, 12, 13.
- Part 7, Breach Notification and Vendor Contracts for SaaS: sections 14, 15, 16, 17.
- Part 8, AI in Regulated SaaS: sections 18, 19, 20.

- Part 9, One Compliance Program for SaaS: sections 21, 22, 23.

Glossary

TERM	DEFINITION
ADMT	Automated decision-making technology: software that makes, or largely makes, a decision about a person. State rules attach notices and opt-outs to it.
Addressable	A HIPAA Security Rule safeguard that must be put in place, or replaced with a documented equivalent, when it is reasonable and appropriate.
BAA	Business associate agreement: the contract HIPAA requires between a covered entity and a vendor that handles PHI for it.
Business associate	A vendor that creates, receives, maintains or transmits PHI for a covered entity. Most health SaaS companies are one.
CDE	Cardholder data environment: the systems that store, process or transmit card data, and so fall inside PCI DSS scope.
Controller	Under GDPR and most state privacy laws, the company that decides why and how personal data is processed.
Covered entity	Under HIPAA, a health plan, a clearinghouse, or a provider that bills electronically.
De-identification	Removing or changing data so it can no longer reasonably be linked to a person, to the standard the governing law sets.
Deployer	Under AI laws, the company that uses an AI system to make or help make decisions.
Developer	Under AI laws, the company that builds or substantially modifies an AI system. The EU AI Act calls it the provider.
DPIA	Data protection impact assessment: the written risk review GDPR and many state laws require before risky processing.
ePHI	Electronic protected health information, the subject of the HIPAA Security Rule.

Newell, J. (2026). MAX Research Collective, ART-DAT-009. CC BY 4.0

TERM	DEFINITION
MFA	Multi-factor authentication: sign-in that needs two or more kinds of proof.
NPI	Nonpublic personal information: the customer data GLBA protects at a financial institution.
PCI DSS	Payment Card Industry Data Security Standard: the card brands' contract standard for anyone handling card data.
PHI	Protected health information: identifiable health information held by a covered entity or its business associate.
PII	Personally identifiable information: data that identifies or can reasonably be linked to a person. Statutes call it personal information or personal data.
Processor	A vendor that handles personal data only on a controller's instructions. California calls it a service provider or contractor.
RAG	Retrieval-augmented generation: a model answering from documents fetched at the time of the question, usually through an embedding index.
SAQ	Self-assessment questionnaire: the form a smaller merchant or service provider uses to validate PCI DSS compliance.
Sensitive authentication data	The card security code, full track data and PIN. PCI DSS bars storing it after authorization.
SOC 2	An independent auditor's report on a service company's security and related controls.
Subprocessor	A vendor's own vendor that also handles the customer's data.
Tokenization	Replacing a card or account number with a stand-in value that is useless outside the system that issued it.

Appendix C: primary sources cited in this part

Each entry was opened on the issuing body's own site between 20 and 22 November 2026. The numbers are the same in every part of the series.

- [1] 15 U.S.C. § 45 (FTC Act § 5)
  - govinfo.gov · uscode
- [2] COPPA: 15 U.S.C. §§ 6501-6502; COPPA Rule, 16 CFR 312.2, 312.5, 312.8, 312.10; final rule amendments, FR Doc. 2025-05904 (effective 2025-06-23, compliance by 2026-04-22)
  - federalregister.gov
- [3] CAN-SPAM Act, 15 U.S.C. § 7704(a)(4)
  - govinfo.gov · uscode
- [4] TCPA, 47 U.S.C. § 227(b)(3); 47 CFR 64.1200
  - govinfo.gov · uscode
- [5] FCRA, 15 U.S.C. §§ 1681b, 1681m, 1681s-3, 1681w; Disposal Rule, 16 CFR 682.3
  - govinfo.gov · uscode
- [6] GLBA, 15 U.S.C. §§ 6801-6802; Regulation P, 12 CFR 1016.5, 1016.10
  - ecfr.gov · part 1016
- [7] FERPA, 20 U.S.C. § 1232g; 34 CFR 99.31(a)(1)(i)(B)
  - ecfr.gov · part 99
- [8] VPPA, 18 U.S.C. § 2710(c)(2)
  - govinfo.gov · uscode
- [9] Wiretap Act, 18 U.S.C. § 2511(2)(d)
  - govinfo.gov · uscode
- [10] DOJ Data Security Program, 28 CFR 202.205, 202.211, 202.1001, 202.1002; final rule, FR Doc. 2024-31486 (effective 2025-04-08; certain duties from 2025-10-06)
  - ecfr.gov · part 202
- [11] PADFA, 15 U.S.C. § 9901
  - govinfo.gov · uscode

- [12] TAKE IT DOWN Act, Pub. L. 119-12 (2025-05-19), § 3
  - govinfo.gov · PLAW 119publ12
- [23] Washington My Health My Data Act, RCW ch. 19.373
  - app.leg.wa.gov · RCW
- [24] Nevada consumer health data law, NRS 603A.400 to 603A.550
  - leg.state.nv.us · NRS 603A
- [25] Conn. Gen. Stat. ch. 743jj (§ 42-526); Va. Code § 59.1-200; Md. Code, Com. Law § 14-4707
  - cga.ct.gov · chap 743jj
- [31] FTC Safeguards Rule, 16 CFR 314.2, 314.4, 314.5
  - ecfr.gov · part 314
- [46] Iowa Code § 715D.3; ORS 646A.574; Minn. Stat. § 325M.14
  - revisor.mn.gov · cite
- [47] Vermont S.71 (2026), signed 2026-06-16, effective 2028-01-01
  - legislature.vermont.gov · status
- [48] California Privacy Protection Agency, announcement of final CCPA regulations (2025-09-23)
  - cppa.ca.gov · announcements
- [51] Biometrics: Tex. Bus. & Com. Code § 503.001; RCW ch. 19.375
  - app.leg.wa.gov · RCW
- [62] Ohio Rev. Code § 1354.02
  - codes.ohio.gov · section 1354.02
- [63] Restore Online Shoppers' Confidence Act, 15 U.S.C. § 8403
  - govinfo.gov · uscode
- [64] California: Civ. Code §§ 56.06, 1798.82, 1798.99.86, 1798.100, 1798.140, 1798.150; Penal Code § 637.2; Bus. & Prof. Code § 17602
  - leginfo.legislature.ca.gov · codes.xhtml

- [66] Illinois: 740 ILCS 14/15 and 14/20 (BIPA); Public Act 103-0804 (HB 3773); Public Act 104-0054 (HB 1806)
  - ilga.gov · Articles
- [67] New York: Gen. Bus. Law §§ 349-a, 899-aa, 899-bb; S6953B of 2025 (RAISE Act, signed); S929 of 2025 (vetoed)
  - nysenate.gov · GBS

Appendix D: secondary references, not primary sources

A dagger with a number points here. Apart from the few agency pages among them, none is a primary source.

- †6 State comprehensive privacy laws: MultiState, 2026-10-28; Venable; Morgan Lewis; IAPP; FPF key dates
  - multistate.us · twenty four states now have comprehensive consumer privacy laws
  - venable.com · 2026 mid year state privacy law update
  - morganlewis.com · new us state consumer privacy laws what businesses should know
  - iapp.org · new year new rules us state privacy requirements coming online as…
  - fpf.org · key dates for state privacy laws
- †7 Pricing and data broker laws: BakerHostetler Q2 2026
  - bakerlaw.com · state privacy in brief q2 2026

DATA ART-DAT-009

// ABOUT THE AUTHOR

Jason Newell leads organizations and people in technology, and is a researcher, deep technologist and builder — from a CRAY to agentic AI. He founded MAX Research Collective to build AI for regulated industries that runs where its owner has control, with healthcare as its strongest focus. About Jason → Connect on LinkedIn → ORCID →