



ANCHOR CYBER SECURITY LLC

GDPR/CCPA Consent & Data Protection Field Reference

Two laws, two consent models. What counts as your data under each, who actually has to comply, and the practical checklist for protecting it either way.

ACCURATE AS OF OCTOBER 2026 – NOT LEGAL ADVICE

Thresholds, definitions, and citations reflect the law as of this card's publication date. This is general information, not legal advice — applicability tests especially have fact-specific exceptions this card can't capture. Confirm current requirements with counsel before relying on this for a specific situation.

Does This Apply To You

	GDPR	CCPA / CPRA
Trigger	Processing personal data of someone in the EU/EEA, when offering them goods or services or monitoring their behavior (Art. 3)	Doing business in California and meeting one of three thresholds below (Civ. Code §1798.140(d))
Size/revenue floor	None — no revenue or headcount exemption. A 3-person company selling to EU customers online is in scope.	Any one of: \$25M+ annual gross revenue, or buys/sells/shares personal info of 100,000+ consumers or households/year, or derives 50%+ of revenue from selling/sharing personal info
Who's covered	Any organization worldwide meeting the territorial test — location of the business is irrelevant	For-profit businesses only; most nonprofits are exempt regardless of size

\$ `diff --data-types`

What Counts As Your Data

	GDPR	CCPA / CPRA
Core term	"Personal data" (Art. 4(1)) — any info relating to an identified or identifiable natural person	"Personal information" (§1798.140(v)(1)) — identifies, relates to, or could reasonably be linked to a consumer or household
Common examples	Name, ID number, location data, online identifiers (IP address, cookie ID), and	Identifiers (name, email, SSN, IP), purchase history, biometric info, browsing/search history,

	physical/genetic/economic/social identity factors	geolocation, employment & education info, and inferences drawn into a profile
Elevated category	Special categories (Art. 9) — race/ethnicity, political opinions, religious belief, union membership, genetic data, biometric ID data, health data, sex life/orientation. Processing is banned by default unless an Art. 9(2) exception applies.	Sensitive personal information (§1798.140(ae)) — government ID numbers, login credentials, precise geolocation (~1,850 ft radius), race/ethnicity, religion, union membership, mail/email/text contents, genetic data, biometric ID data, health data, sex life/orientation. Consumers can limit its use (§1798.121).
Notably excluded	—	Lawfully obtained publicly available information (narrowed by CPRA — can't reuse it for an incompatible purpose) and properly de-identified or aggregate data

THE OVERLAP MATTERS MORE THAN THE DIFFERENCES

Health data, genetic data, biometric identifiers, religious belief, ethnicity, and union membership appear on *both* elevated lists. If you're already treating something as sensitive under one law, assume the other has an opinion about it too.

\$ diff --consent-model

Consent: The Part That Gets Confused

GDPR — OPT-IN

Consent is one of six legal bases for processing (Art. 6) — not the only one. When it's the basis actually used, it has to be freely given, specific, informed, unambiguous, and an affirmative act (Art. 4(11), Art. 7).

Pre-checked boxes don't count. Withdrawing consent has to be as easy as giving it.

CCPA/CPRA — OPT-OUT

Not a consent law in the GDPR sense.

Businesses collect and use personal information by default; consumers have to affirmatively opt out of sale or sharing (§1798.120) or limit use of sensitive personal information (§1798.121).

Opt-in consent is the exception here — mainly for consumers under 16 (§1798.120(c)-(d)) and for sensitive-data use after an opt-out.

MOST COMMON MISTAKE

Treating CCPA like it needs a GDPR-style cookie-consent banner with opt-in checkboxes. The statute's actual mechanism runs the other direction — opt-out, not opt-in.

\$ diff --rights

Rights At A Glance

Rights	Access (15), rectification (16), erasure (17), restrict processing (18), portability (20), object (21), rights re: automated decision-making (22)	Know/access (100, 110), delete (105), correct (106), opt out of sale/sharing (120), limit sensitive PI use (121), non-discrimination for exercising any right (125)
---------------	---	---

EXACT DEADLINES

For response-window day counts and breach notification timing, see [Privacy Law Quick-Diff](#) rather than duplicating those numbers here.

```
$ --protect ./personal-data
```

Protecting The Data Either Way

► Know what you actually have.

A data inventory — what you collect, where it's stored, which vendors touch it — is the precondition for everything else. You can't honor a deletion request for data you don't know you're holding.

► Minimize and set retention limits.

Don't collect what you don't need, and don't keep it longer than you need it.

► Get the vendor contracts right.

GDPR requires a data processing agreement with every processor (Art. 28). CCPA/CPRA has its own "service provider" contract terms (§1798.140(ag), (j)) — a vendor without the right language can turn routine data sharing into a "sale" you didn't intend to make.

► Honor opt-out signals automatically.

The Global Privacy Control is a legally recognized opt-out signal under CCPA regulations (11 CCR §7025) — a browser-level "don't sell my data" flag your site has to respect without a separate form.

► Disclose before you collect, not after.

CCPA requires a notice at collection (§1798.100(b)); GDPR requires transparency notices up front (Art. 13-14). Both want this before data changes hands, not buried in a privacy policy nobody opens.

► Have a breach plan before you need one.

Know your actual notification trigger and timeline ahead of time — see Privacy Law Quick-Diff for the specific deadlines per law.

► Train the people who touch the data.

Most consent and data-protection failures are a process gap, not a technology gap.

src: GDPR Art. 3, 4(1), 4(11), 6, 7, 9, 13, 14, 15-18, 20-22, 28 · Cal. Civ. Code §1798.100, 105, 106, 110, 120, 121, 125, 130, 140(d)/(ae)/(ag)/(j)/(v) · 11 CCR §7025

```
exit 0
```