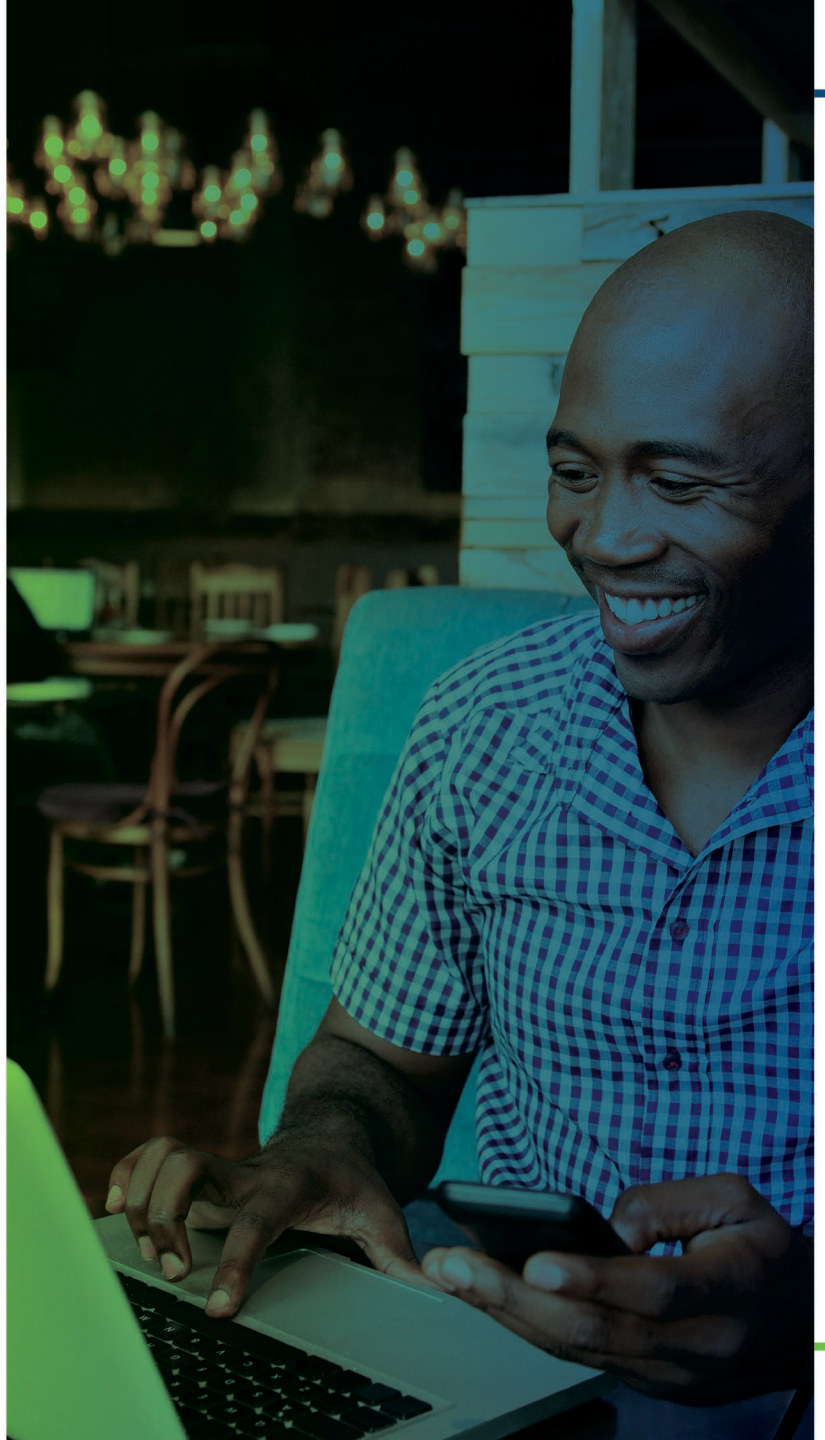


Don't DROP the Ball: California's Looming Deadline and DSR Operations at Scale

Tuesday, 14 July
08:00–09:00 PDT
11:00–12:00 EDT
17:00–18:00 CEST

Welcome & Introduction

Alex Proctor
AIGP, CIPP/E, CIPP/US, CIPM, CIPT, FIP
Chief Trust & Privacy Officer
Captain Compliance

www.captaincompliance.com

Today's Agenda

1. **Understanding DROP.** Platform Requirements, Compliance Timeline, & Risk Management
2. **DSR Operations at Scale.** Common Challenges, Friction Points, & Industry Standards.
3. **Automation & Integration.** Orchestrating DSR Workflows with Captain Compliance.
4. **Questions & Answers.** *Feel free to drop questions in the chat box throughout the session!*

Understanding DROP

Platform Requirements, Compliance Timeline, & Risk Management

Poll: Is DROP on Your Desk?

A **Yes**. We're a registered data broker (…or perhaps we *should* be?)

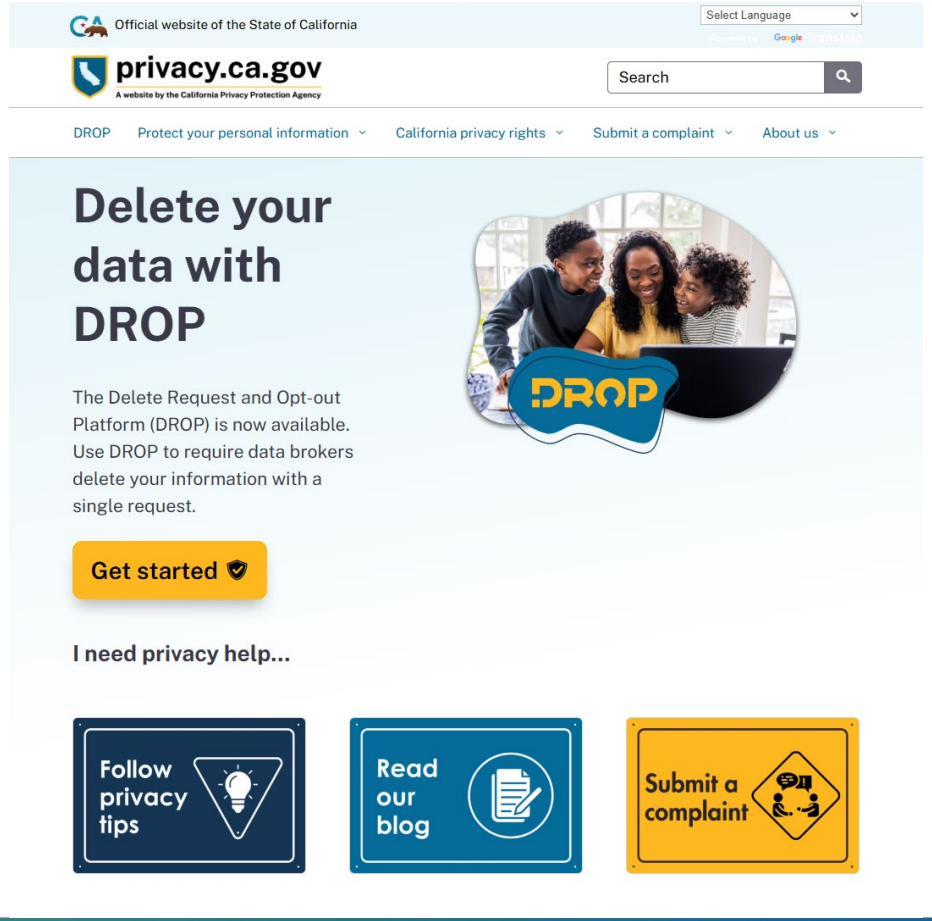
B **Indirectly**. We're not a data broker ourselves, but we have relationships with them.

C **No**. DROP does not apply to us. I'm here for the broader DSR discussion.

D **Not Applicable.** I'm an advisor, a student, or something like that.

What is California's DROP (Platform)?

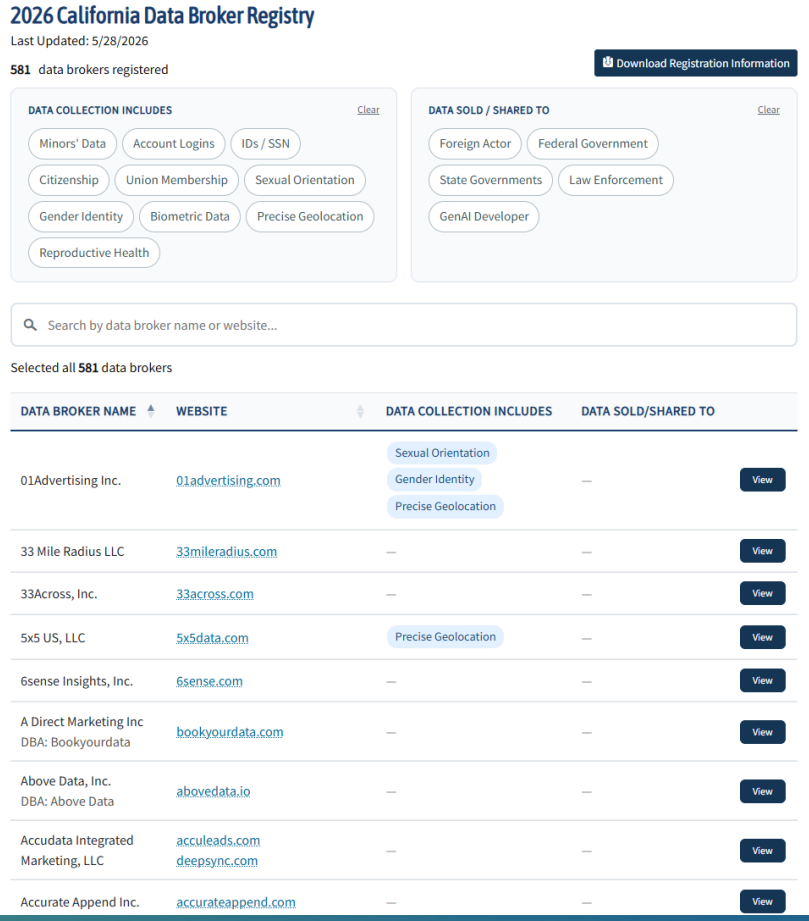
- California's **Delete Request and Opt-out Platform ("DROP")** is the state's new system for facilitating consumer deletion and opt-out requests.
- DROP serves as a unified channel intended to orchestrate deletion and opt-out requests that would otherwise need to be delivered to hundreds of **data brokers** individually.
- Data brokers must successfully match consumer identity and accurately locate relevant records before they can process deletions and honor opt-out requests.
- The platform is already live, and data brokers can access it today. Beginning **August 1, 2026**, registered data brokers must check DROP every 45 days and honor requests.
- Compliance with DROP is mandatory for data brokers, and non-compliance carries regulatory and legal risk.



Reference: https://privacy.ca.gov/

What is a Data Broker?

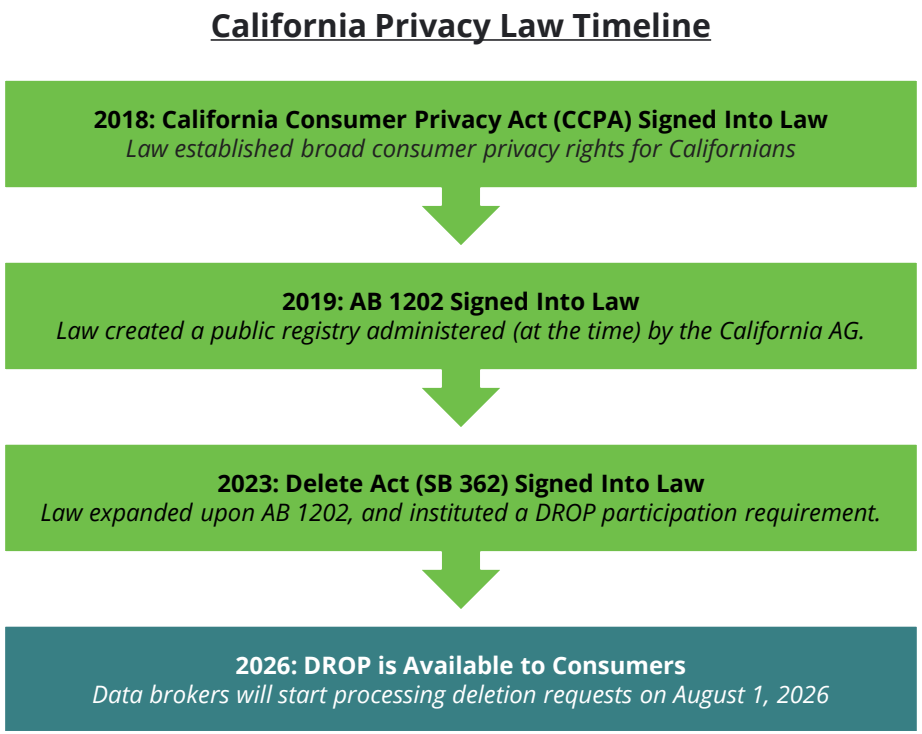
- **Data brokers** collect and sell personal information about consumers with whom they have no direct relationship.
- State registries exist to bring transparency to the data broker industry, enable oversight, and give consumers visibility into who holds their data and how to exercise their privacy rights.
- Any business that meets CA's definition of "data broker" must register annually with CalPrivacy between January 1-31. (The 2026 annual registration fee is $6,000 plus an associated third-party fee for processing electronic payments).
- Registered data brokers increased from 459 entities in June 2025 to more than 575 in February 2026, representing the largest state data broker registry in U.S. history.
- Data brokers that fail to register by January 31st of each year may be liable for administrative fines and costs in an administrative action or investigation brought by CalPrivacy.



Reference: https://cppa.ca.gov/data_broker_registry/

How Did DROP Come to Be?

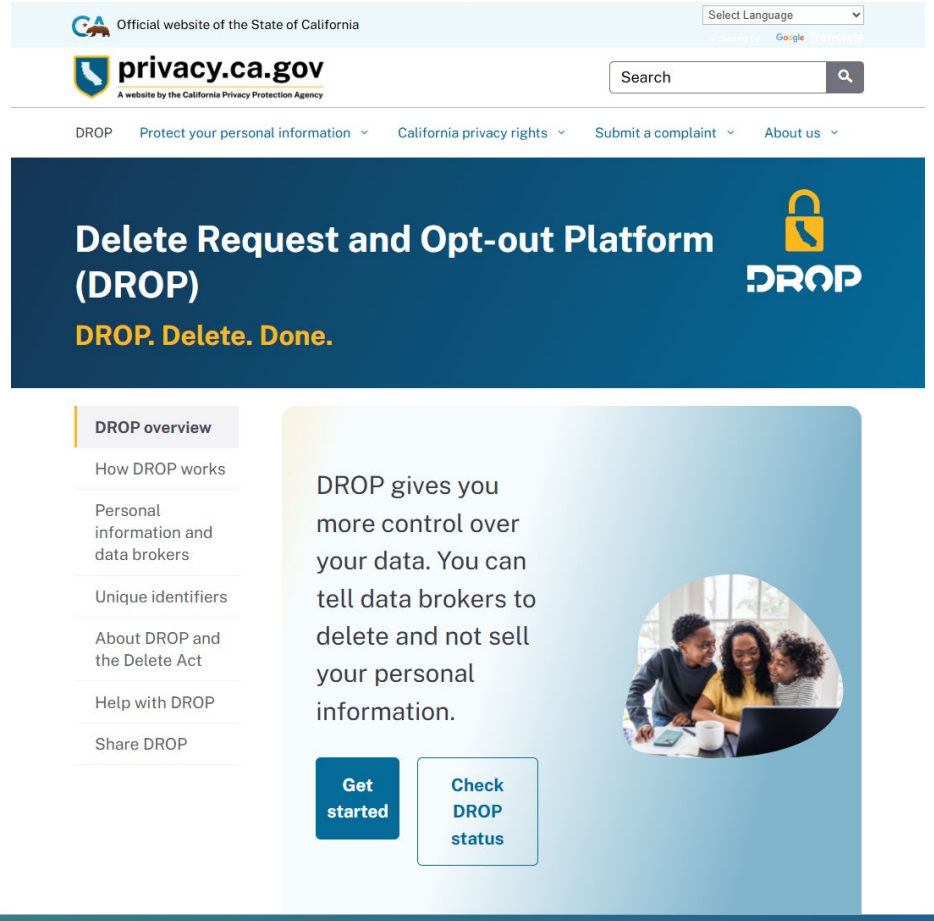
- The California Consumer Privacy Act (CCPA) of 2018 established **foundational consumer privacy rights**, which the California Privacy Rights Act (CPRA) expanded in 2020 while creating the California Privacy Protection Agency ("**CalPrivacy**") to enforce.
- California's original data broker registration law (**AB 1202**, 2019) requires data brokers to register annually (now with) CalPrivacy.
- The **Delete Act** (Senate Bill 362, 2023) expanded upon AB 1202, including by requiring registered data brokers to process deletion requests through DROP beginning August 1, 2026.
- Senate Bill 361 (2025) amended the Delete Act to require additional disclosures in the data broker registration process.
- As of 2026, the **DROP platform** has been created to satisfy the requirements of the Delete Act. Non-compliance carries administrative fines and penalties enforced by CalPrivacy.



Reference: https://privacy.ca.gov/

What is the Scope of DROP?

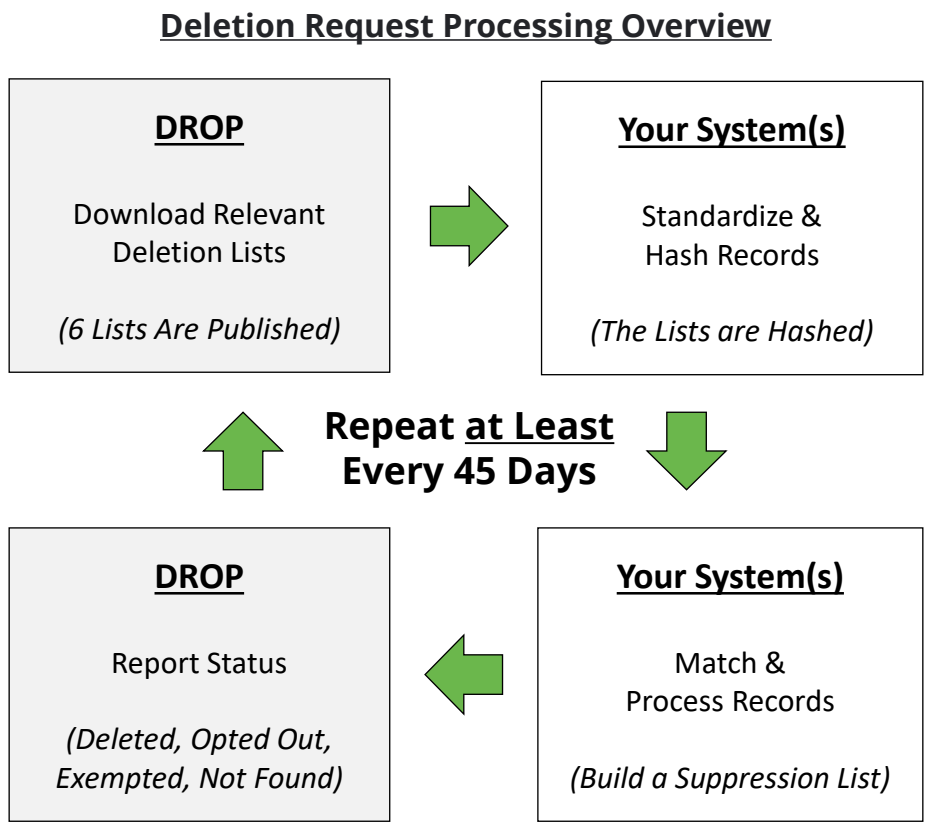
- DROP only applies to **data brokers** gathering and selling consumer information that they didn't obtain from the consumer directly (it does not apply to all businesses).
- The platform covers deletion and opt-out requests exclusively and does not address other CA consumer privacy rights like access, correction, or portability.
- Certain data is exempt from DROP's deletion requirements, including public records, data related to criminal or civil investigations, and data covered by other privacy laws.
- Deletion requirements may not extend to data which brokers have already shared with third parties, depending on how the law is interpreted.
- The exact boundaries of what "must be deleted" versus what "can be retained" remain ambiguous and may be subject to regulatory guidance or litigation.



Reference: https://privacy.ca.gov/drop/

What Does DROP Compliance Require?

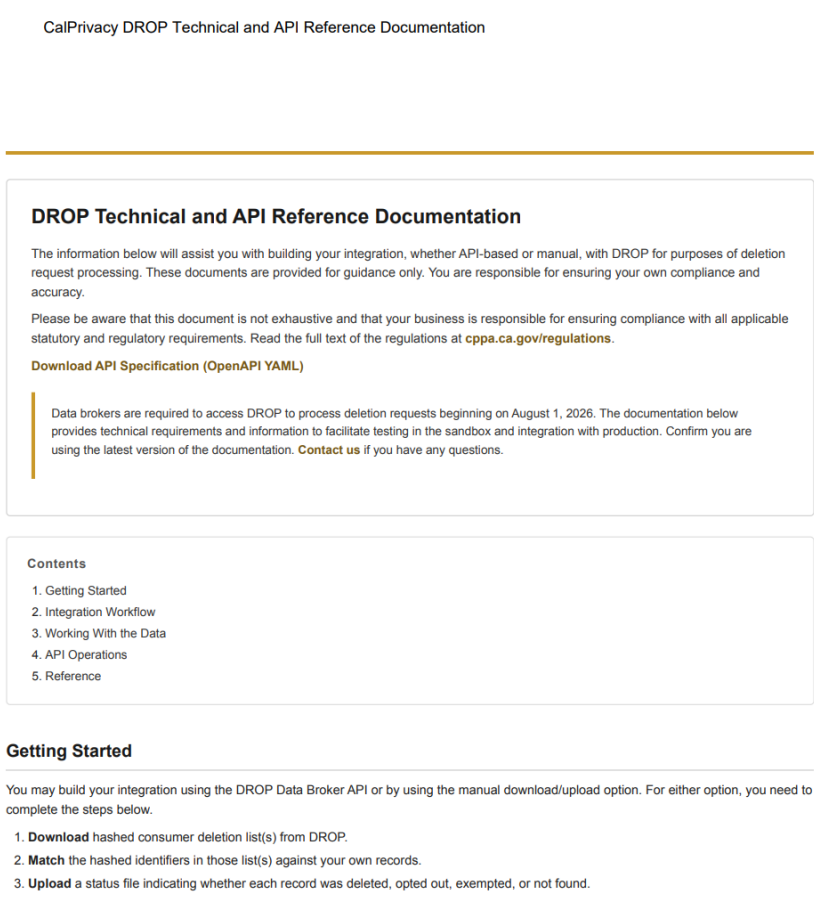
- Data brokers must create a DROP account, select from the six consumer deletion lists that may match their records, and keep those selections current as collection practices change.
- Beginning August 1, 2026, data brokers must access DROP at least once every 45 days and download new deletion requests
- Consumer identifiers on DROP lists are all hashed, so your own data must also be standardized and hashed in a specific way.
- For each matched consumer record hash, data brokers must **delete non-exempt personal information**, including inferences, and direct any service providers to do the same.
- Multi-consumer matches must be processed as **opt-outs of sale and sharing**, unmatched requests report as not found, and new data on deleted consumers must be deleted on the same cycle.
- After request processing, data brokers must report the status of each request (manually or via API) within 45 days of download.



Reference: https://privacy.ca.gov/drop-for-data-brokers/process-drop-requests/

Can DROP Interaction Be Automated?

- DROP provides a fully documented API that supports automated download, processing, and upload of deletion requests without manual intervention.
- Data brokers can choose between API-based integration or manual portal upload/download, depending on technical capacity and existing infrastructure.
- The API follows a cycle: download consumer deletion data via GET /data/download, match hashed identifiers against your records, then upload status responses via POST /data/upload.
- Automation requires the orchestration of identity matching and hashing standardization (SHA-256 Base64) to compare incoming requests against your records accurately.
- Scheduled automation must account for DROP's daily maintenance window (1–3 AM PT) when the platform closes push and pull requests and should include retry logic.



CalPrivacy DROP Technical and API Reference Documentation

DROP Technical and API Reference Documentation

The information below will assist you with building your integration, whether API-based or manual, with DROP for purposes of deletion request processing. These documents are provided for guidance only. You are responsible for ensuring your own compliance and accuracy.

Please be aware that this document is not exhaustive and that your business is responsible for ensuring compliance with all applicable statutory and regulatory requirements. Read the full text of the regulations at **cppa.ca.gov/regulations**.

Download API Specification (OpenAPI YAML)

> Data brokers are required to access DROP to process deletion requests beginning on August 1, 2026. The documentation below provides technical requirements and information to facilitate testing in the sandbox and integration with production. Confirm you are using the latest version of the documentation. **Contact us** if you have any questions.

Contents

1. Getting Started
2. Integration Workflow
3. Working With the Data
4. API Operations
5. Reference

Getting Started

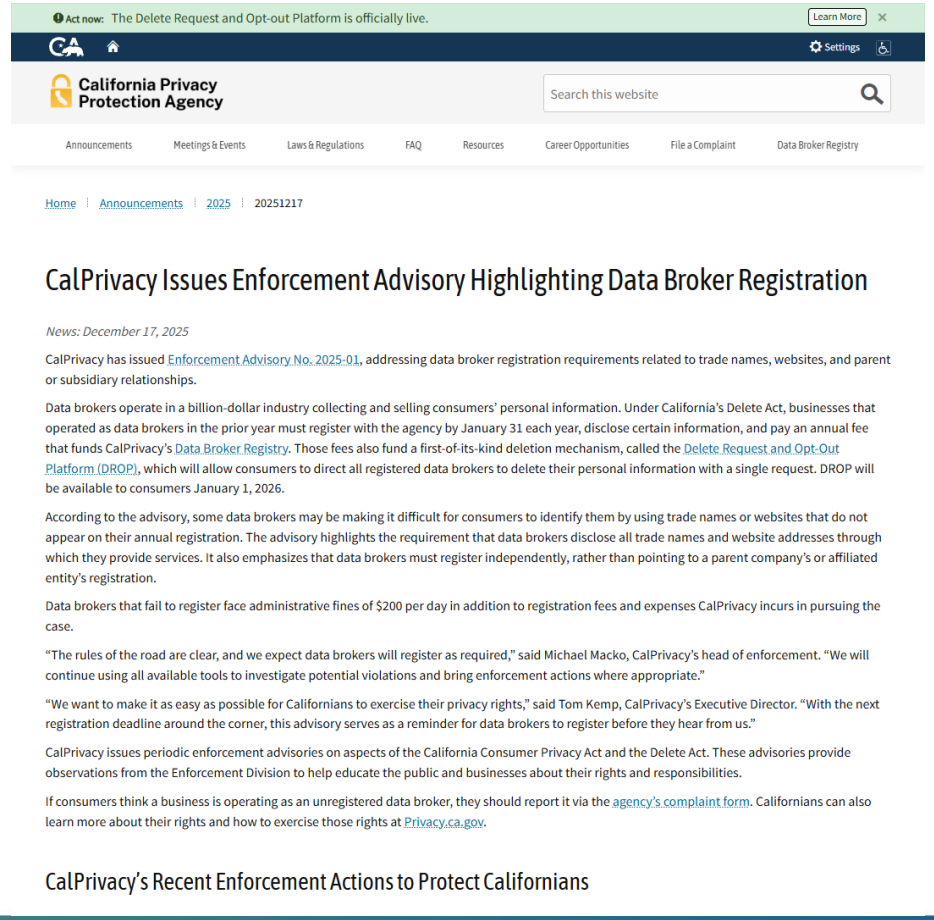
You may build your integration using the DROP Data Broker API or by using the manual download/upload option. For either option, you need to complete the steps below.

1. **Download** hashed consumer deletion list(s) from DROP.
2. **Match** the hashed identifiers in those list(s) against your own records.
3. **Upload** a status file indicating whether each record was deleted, opted out, exempted, or not found.

Reference: https://cppa.ca.gov/orph/drop_tech_api_ref.pdf

What Will Enforcement Look Like?

- Enforcement belongs to **CalPrivacy,** and it is administrative; there is no private right of action under the Delete Act.
- The fine structure penalizes companies **$200 per day for registration failures**, and **$200 per (unprocessed) deletion request per day** after August 1, plus investigation costs.
- A dedicated **Data Broker Enforcement Strike Force** launched in November 2025, and its first settlements landed in January. Datamasters paid $45,000 and must stop selling Californians' personal information entirely; S&P Global paid $62,600 over a registration lapse attributed to administrative error.
- In total, CalPrivacy has brought **more than ten actions against other unregistered brokers** and issued a December 2025 enforcement advisory warning the industry directly.
- In addition to fines, shutdowns, market exit, and mandated compliance programs are all on the table. After August 1, enforcement will turn to misprocessed DROP requests.



Act now: The Delete Request and Opt-out Platform is officially live. Learn More

Settings

California Privacy Protection Agency

Search this website

Announcements | Meetings & Events | Laws & Regulations | FAQ | Resources | Career Opportunities | File a Complaint | Data Broker Registry

Home | Announcements | 2025 | 20251217

CalPrivacy Issues Enforcement Advisory Highlighting Data Broker Registration

News: December 17, 2025

CalPrivacy has issued Enforcement Advisory No. 2025-01, addressing data broker registration requirements related to trade names, websites, and parent or subsidiary relationships.

Data brokers operate in a billion-dollar industry collecting and selling consumers' personal information. Under California's Delete Act, businesses that operated as data brokers in the prior year must register with the agency by January 31 each year, disclose certain information, and pay an annual fee that funds CalPrivacy's Data Broker Registry. Those fees also fund a first-of-its-kind deletion mechanism, called the Delete Request and Opt-Out Platform (DROP), which will allow consumers to direct all registered data brokers to delete their personal information with a single request. DROP will be available to consumers January 1, 2026.

According to the advisory, some data brokers may be making it difficult for consumers to identify them by using trade names or websites that do not appear on their annual registration. The advisory highlights the requirement that data brokers disclose all trade names and website addresses through which they provide services. It also emphasizes that data brokers must register independently, rather than pointing to a parent company's or affiliated entity's registration.

Data brokers that fail to register face administrative fines of $200 per day in addition to registration fees and expenses CalPrivacy incurs in pursuing the case.

"The rules of the road are clear, and we expect data brokers will register as required," said Michael Macko, CalPrivacy's head of enforcement. "We will continue using all available tools to investigate potential violations and bring enforcement actions where appropriate."

"We want to make it as easy as possible for Californians to exercise their privacy rights," said Tom Kemp, CalPrivacy's Executive Director. "With the next registration deadline around the corner, this advisory serves as a reminder for data brokers to register before they hear from us."

CalPrivacy issues periodic enforcement advisories on aspects of the California Consumer Privacy Act and the Delete Act. These advisories provide observations from the Enforcement Division to help educate the public and businesses about their rights and responsibilities.

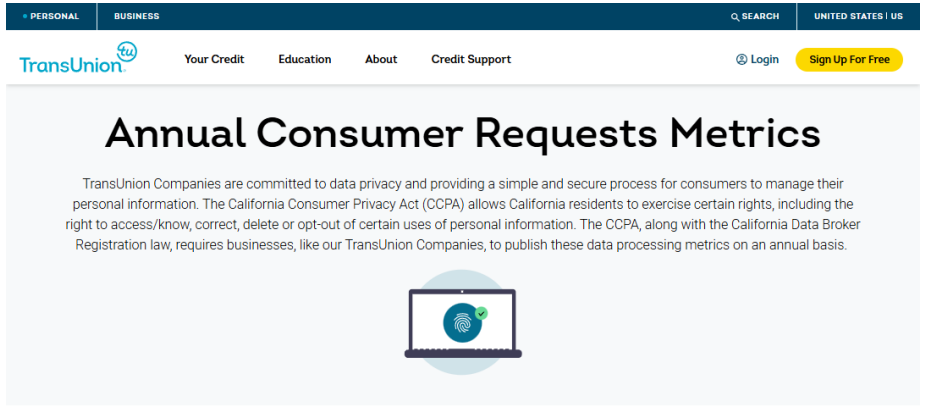
If consumers think a business is operating as an unregistered data broker, they should report it via the agency's complaint form. Californians can also learn more about their rights and how to exercise those rights at Privacy.ca.gov.

CalPrivacy's Recent Enforcement Actions to Protect Californians

Reference: https://cppa.ca.gov/announcements/2025/20251217.html
Reference: https://cppa.ca.gov/announcements/2026/20260108.html

Expect a Major Increase in DSR Volume

- For large companies, DSR volume is public record. As a point of reference, **TransUnion's** registered-broker entities reported 1,598 deletion requests in 2025, while 42,000+ opt-outs were processed within the same timeframe.
- Even prior to DROP, TransUnion's reporting highlights DSR volume increases year-over-year. 2024 data showed 1,057 deletion requests, implying a 51% increase from 2024 to 2025. 2024 reporting also contained 30,000+ opt-out requests, for a 41% increase year-over-year.
- Now, DROP is going to increase the processing scale for 2026. At least 242,000 requests were already queued as of late February 2026, and every request requires a hash, match check, and response (even the non-matches). TransUnion's precise match rate is externally unknowable, but the increase in processing volume is coming.
- Analyst estimates put manual DSR processing at around $1,500 per request, almost entirely labor (searching systems, verifying identities, compiling and documenting responses, etc.).



2025 Consumer Requests Report

In calendar year 2025, we received and responded to consumer requests as set forth in the table below. For more information regarding our privacy practices at TransUnion Companies, review our Privacy Notices, and to exercise your privacy rights and choices, visit our US State Privacy Rights page.

Request Type	Requests Received	Requests Complied (in whole or in part)	Requests Denied*	Mean Days to Resolution	Median Days to Resolution
Deletion	1598	1598	0	57	53
Correction	133	133	0	39	40
Opt out of sale/sharing	42663	42663	0	1	1
Limit Use of Sensitive Data	42281	42281	0	1	1
Access Request/Right to Know	3651	3651	0	14	4
Opt out of automated decision making	41932	41932	0	1	1
Opt out of marketing	42228	42228	0	1	1

** Denied requests include unverified requests where no account or related file was found.*

This data reflects requests received in 2025 from all individuals.

Reference: https://www.transunion.com/ccpa-metrics

August 1st: DROP Readiness Checklist

- **The first download may be a challenge**. CalPrivacy reports hundreds of thousands of deletion requests already waiting in DROP, so plan capacity for a potential backlog.
- Accounts need CalPrivacy approval before first access, which takes about two business days. The sandbox has been open since March, and as of July, the timeline to prepare is tight.
- Select every deletion list that matches identifiers in your records and revisit as collection practices change. A missed list represents unprocessed requests accruing penalties.
- Build an internal playbook for exemptions and unverifiable matches. Exemptions must be legally defensible, multi-consumer matches become opt-outs, and unmatched requests report as not found.
- Brokers are responsible for manual downloads when integrations break, and the 45-day cadence necessitates a clear process owner, calendar, and paper trail to support audits.

DROP Readiness Checklist

Readiness Item	Suggested Owner
DROP Account Created & Approved	Privacy Lead
Deletion Lists Selected & Current	Privacy Operations
Data Standardization & Hashing Sandbox-Tested	Engineering
Exemption & Opt-Out Playbook Ready	Legal
Status Reporting Workflow Ready	Privacy Operations
Manual Fallback & Failure Reporting	Privacy Operations
Service Providers Informed & Instructed	Vendor Management
“August 1 Backlog” Capacity Plan Ready	Privacy Operations
45-Day Cycle Assigned & Calendared	Privacy Operations

Reference: https://privacy.ca.gov/drop-for-data-brokers/
Reference: https://privacy.ca.gov/drop-for-data-brokers/account-creation-fees-and-annual-registration/

After August 1: The Road Through 2028

- After August 1, 2026, **DROP's 45-day cycles run indefinitely.**
- By January 31, 2027, data brokers must register (or re-register) with CA. SB 361's expanded disclosures (AI developer, foreign adversary, and government/law enforcement sharing) have applied since the 2026 cycle.
- Beginning January 1, 2028, each broker must undergo an independent third-party compliance audit every three years, arrange it, pay for it, and retain the report and supporting materials for six years. These reports must be provided to CalPrivacy within five business days of a request.
- Connecticut recently enacted its own registration and deletion-mechanism law, with broker registration opening January 1, 2027, and a DROP-style mechanism arriving by July 1, 2028.
- States continue to establish new privacy rights and programs must be capable of absorbing these changes indefinitely.

Upcoming Milestones for Data Brokers and Businesses

Date	Milestone
Aug 1, 2026	CA DROP processing begins; 45-day cycles start
Jan 1, 2027	OK privacy law go-live (OCDPA, grants new privacy rights)
Jan 1, 2027	LA privacy law go-live (LDPA, grants new privacy rights)
Jan 1, 2027	CT data broker registration opens (Details TBD)
Jan 31, 2027	CA data broker annual registration (2027)
May 1, 2027	AL privacy law go-live (APDPA, grants new privacy rights)
Jan 1, 2028	VT privacy law go-live (VDPOSA, grants new privacy rights)
Jan 1, 2028	CA independent third-party audit begin *(Details TBD)*
Jul 1, 2028	CT DROP-style deletion mechanism goes live

Reference: https://www.dglaw.com/connecticuts-newly-enacted-data-broker-law-how-it-stacks-up-against-californias-delete-act/

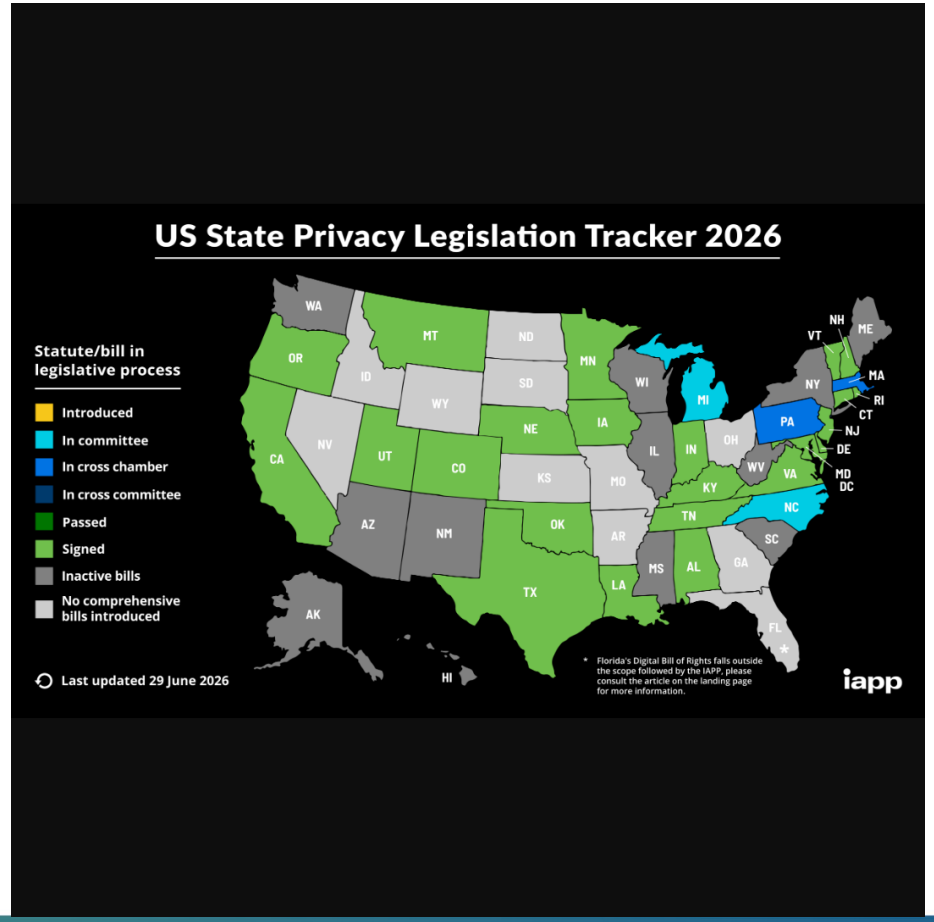
iapp

DSR Operations at Scale

Common Challenges, Friction Points, & Industry Standards

The Broader U.S. DSR Landscape

- Comprehensive privacy laws are now in effect in roughly twenty U.S. states, with new legislation advancing constantly.
- Every state privacy law shares a common theme around **enforceable individual rights**, and a **deadline-bound duty to respond** when consumers choose to exercise them.
- The theme is consistent, but the requirements are not. **Timelines, verification rules, appeal duties, and exemptions** all vary by statute, and beneath that sits the bigger divide: states with consumer-rights-granting laws and states without.
- Just because a state lacks a comprehensive privacy law does not mean it is obligation-free: **sector laws like Washington's MHMDA add their own privacy rights, including deletion**.
- Consumer privacy rights tend to move in only one direction. Every session hands DSR programs another law to absorb, and the more regional the program's design, the more expensive each new law becomes.



Reference: https://iapp.org/resources/article/us-state-privacy-legislation-tracker

DSR Obligations By U.S. State

State Regulation	Effective Date	General Consumer Rights				Opt-Out Rights			Private Right of Action	Fulfillment Obligation	Max Extension	Exceptions to Fulfillment Obligation
		Access	Correct	Delete	Portability	Targeted Advertising	Sale	Certain Profiling				
California Consumer Privacy Act	01-01-2020	✓	✓	✓	✓	✓	✓	✗	✓	45 Days	+ 45 Days	Opt-Out Rights: 15 Business Days
Colorado Privacy Act	07-01-2023	✓	✓	✓	✓	✓	✓	✓	✗	45 Days	+ 45 Days	N/A
Connecticut Data Privacy Act	07-01-2023	✓	✓	✓	✓	✓	✓	✓	✗	45 Days	+ 45 Days	N/A
Delaware Personal Data Privacy Act	01-01-2025	✓	✓	✓	✓	✓	✓	✓	✗	45 Days	+ 45 Days	N/A
Indiana Consumer Data Protection Act	01-01-2026	✓	✓	✓	✓	✓	✓	✓	✗	45 Days	+ 45 Days	N/A
Iowa Consumer Data Protection Act	01-01-2025	✓	✗	✓	✓	✗	✓	✗	✗	90 Days	+ 45 Days	N/A
Kentucky Consumer Data Protection Act	01-01-2026	✓	✓	✓	✓	✓	✓	✓	✗	45 Days	+ 45 Days	N/A
Maryland Online Data Privacy Act	10-01-2025	✓	✓	✓	✓	✓	✓	✓	✗	45 Days	+ 45 Days	N/A
Minnesota Consumer Data Privacy Act	07-31-2025	✓	✓	✓	✓	✓	✓	✓	✗	45 Days	+ 45 Days	N/A
Montana Consumer Data Privacy Act	10-01-2024	✓	✓	✓	✓	✓	✓	✓	✗	45 Days	+ 45 Days	N/A
Nebraska Data Privacy Act	01-01-2025	✓	✓	✓	✓	✓	✓	✓	✗	45 Days	+ 45 Days	N/A
New Hampshire Privacy Act	01-01-2025	✓	✓	✓	✓	✓	✓	✓	✗	45 Days	+ 45 Days	N/A
New Jersey Data Privacy Act	01-15-2025	✓	✓	✓	✓	✓	✓	✓	✗	45 Days	+ 45 Days	N/A
Oregon Consumer Privacy Act	07-01-2024	✓	✓	✓	✓	✓	✓	✓	✗	45 Days	+ 45 Days	N/A
Rhode Island (...) Privacy Protection Act	01-01-2026	✓	✓	✓	✓	✓	✓	✓	✗	45 Days	+ 45 Days	N/A
Tennessee Information Protection Act	07-01-2025	✓	✓	✓	✓	✓	✓	✓	✗	45 Days	+ 45 Days	N/A
Texas Data Privacy and Security Act	07-01-2024	✓	✓	✓	✓	✓	✓	✓	✗	45 Days	+ 45 Days	N/A
Utah Consumer Privacy Act	12-31-2023	✓	✓	✓	✓	✓	✓	✗	✗	45 Days	+ 45 Days	N/A
Virginia Consumer Data Protection Act	01-01-2023	✓	✓	✓	✓	✓	✓	✓	✗	45 Days	+ 45 Days	N/A

Reference: https://iapp.org/resources/article/us-state-privacy-legislation-tracker/

DROP vs. U.S. DSR Programs

- DROP and broader DSR programs necessitate similar underlying cycles. In general, requests come in, identities are matched, requests are fulfilled, and outcomes are documented.
- With respect to DROP, California controls intake, performs identity verification, and standardizes responses. With broader DSR programs, these are organizational accountabilities.
- Verification is an inversion: brokers may not contact consumers to verify requests, while general programs are required to communicate acknowledgments, responses, and appeal routes.
- DROP's deletion obligation is stricter than most statutes require, as it reaches **all non-exempt PI tied to the consumer, including inferences**, though data collected directly from the consumer as a first party is carved out.
- DROP doesn't invalidate broader DSR obligations for data brokers, rather it adds to CCPA/CPRA and multistate duties. Again, non-brokers are not required to engage with DROP.

DROP vs. U.S. DSR Programs

Obligation	DROP	U.S. DSR Program
U.S. Jurisdiction	CA	~20 States (incl. CA)
Request Intake	Bulk-Based Download	Individual Requests
Delete & Opt-Out Requests	DROP-Originated Lists	Your DSR Channels
Access, Correct, & Portability Requests	Not Relevant	Your DSR Channels
Identity Verification	Handled by CalPrivacy	Handled by You
Deletion Scope	All PI + Inferences	Statute Dependent
Direct Communication	Prohibited	Required
Timeline	45-Day Download Cycle	Statute Dependent
Timeline Extensions	Not Available	Generally Available

Reference: https://privacy.ca.gov/drop-for-data-brokers/

Poll: What's Your DSR Pain Point?

A **Intake.** Multi-channel support, request quality, and/or identity verification.

B **Fulfillment.** Data inventory, workflow execution, and/or communication.

C **Efficiency**. Systems/datastore integrations, automation, and/or scaling.

D **Compliance.** Legal issues, record-keeping, and/or regional requirements.

Intake: Channel Harmonization

- Every request starts at the intake stage, and requests may be received through any of several channels, some mandatory depending on state law, your web presence, and whether you operate as a data broker.
- In most states, your privacy notice defines the official channels. These channels must be staffed, monitored, and tracked.
- Browser signals are a unique exception: UOOM/GPC opt-outs may not integrate with your standard DSR queue, although there are special criteria to consider here (logged-in users, etc.)
- Despite official channels, requests may be received elsewhere (web chat, support tickets, social, mail, etc.) Redirecting requests is allowed but ignoring them is not.
- Harmonize all DSR requests into **one queue**, with one record per request and consistent deadline tracking starting from the date of request receipt. Avoid deadline-impacting triage delays.

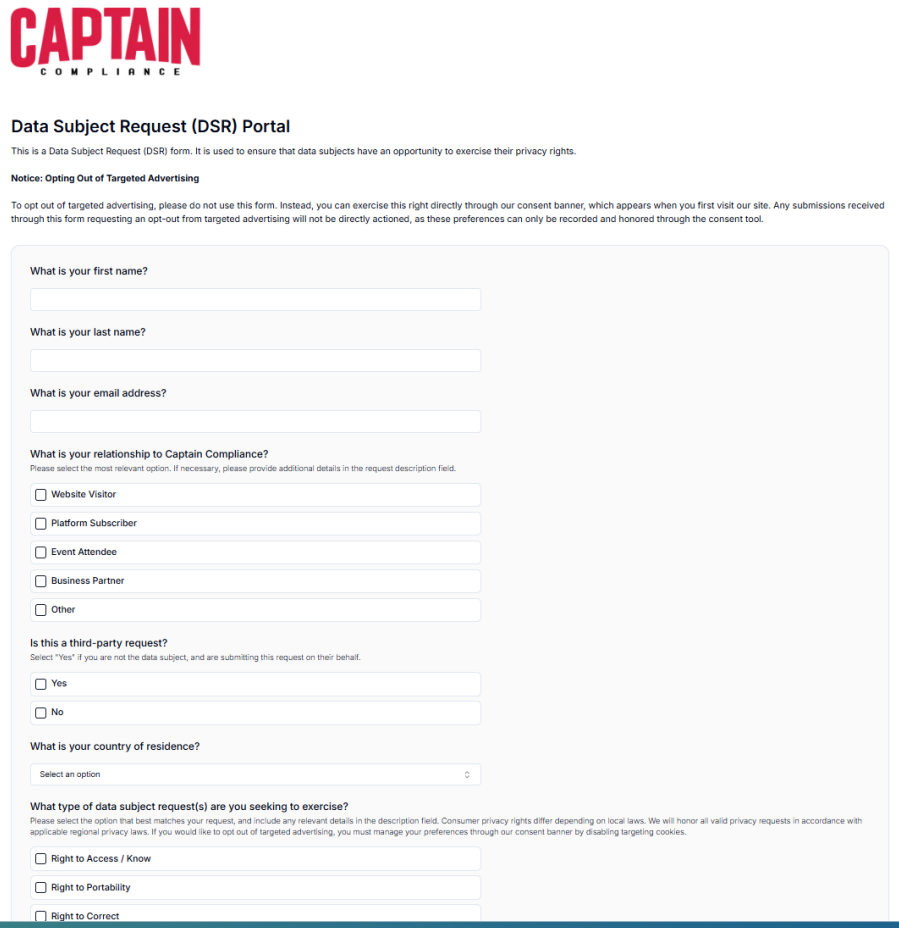
Potential DSR Intake Channels

Channel	Comment
DROP	Must Support (CA) *Data Brokers Only*
Web-Based Method *(DSR Portal, Privacy Webform, etc.)*	Must Support (CA/CO) *Reference in Privacy Notice*
Privacy-Specific Email Address	Recommend Support *(If No Web-Based Method)* *Reference in Privacy Notice*
Toll-Free Phone Number	Must Support (CA) (Some Exclusions) *Reference in Privacy Notice*
Browser-Based Opt-Out *(Global Privacy Control, etc.)*	Must Support (12+ States) *Handled by Consent Layer*
Other Channels *(Generic Email Address, Generic Contact Form, Chatbot, etc.)*	Avoid Suggesting! *These Requests Must Still Be Honored or Redirected!*

Reference: https://cppa.ca.gov/regulations/

Intake: Privacy Request Portals

- A dedicated DSR portal can drastically improve the DSR intake workflow. Identity, request scope, and jurisdiction can be collected consistently (with deadline tracking and an audit trail).
- Additionally, dedicated DSR portals tend to result in **fewer malformed or incomplete requests,** requiring less time and resource-intensive communication with the data subject.
- Design DSR portal questions with restraint, because asking for more information than a request requires is itself a violation. In a recent California enforcement action, Honda paid a penalty of $632,500, in part for over-collecting request-related data.
- Collect the minimum information needed to route and verify requests. Match fields to the request type, never require an account, and never conduct identity verification for opt-outs.
- Build an authorized-agent workflow, because CA (and other states) require businesses to accept agent-submitted requests. Validate the agent's authority at intake.



Reference: https://cppa.ca.gov/announcements/2025/20250312.html

Intake: Identity Verification

- Most request types require **identity verification** before fulfillment. The requester must be matched to the data before anything is disclosed, corrected, or deleted.
- Usually, verification involves matching the requester to information you already hold. A confirmed email or logged-in account often suffices, and regulations often frame the higher tiers as matching two or three data points already on file.
- Verify too loosely and you may disclose personal information to an unauthorized actor. In contrast, if you verify too strictly, making it difficult for data subjects to submit legitimate requests, that friction is itself a privacy law violation.
- Calibrate by request type and sensitivity. Opt-outs should not involve verification, deletion should require proportionate checks, and access to data may require the most rigor.
- **DROP shifts verification away from brokers.** CalPrivacy verifies requests directly (including CA residency), and brokers may not contact consumers to verify.

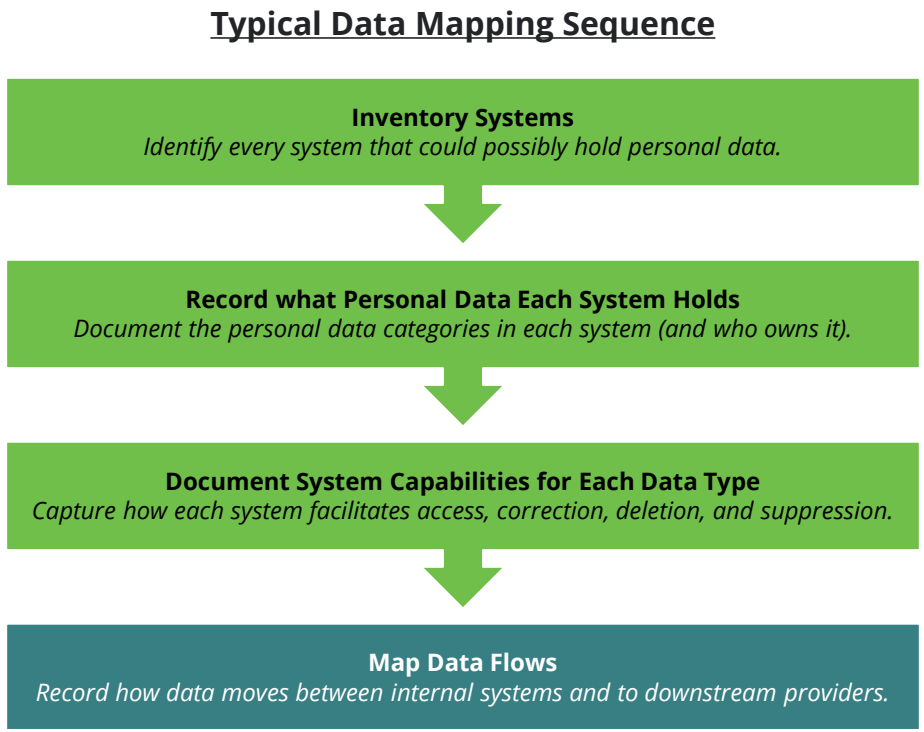
Identity Verification Calibration

Factor	Too Relaxed	Balanced	Too Strict
Example Approach	Verification Minimized for Everything	Verification Based on Request Type	Verification Maximized for Everything
Access & Portability Requests	Unauthorized Disclosure	Fulfilled After Matching	Blocked By Friction
Deletion & Correction Requests	Wrongful Deletion or Alteration	Fulfilled After Matching	Blocked By Friction
Opt-Out Requests	No Verification	No Verification	Any Verification (Prohibited)
Potential Consequence	Data Breach	None	Privacy Law Violation

Reference: https://cppa.ca.gov/announcements/2025/20250506.html
Reference: https://cppa.ca.gov/announcements/2025/20250312.html

Fulfillment: Data Mapping

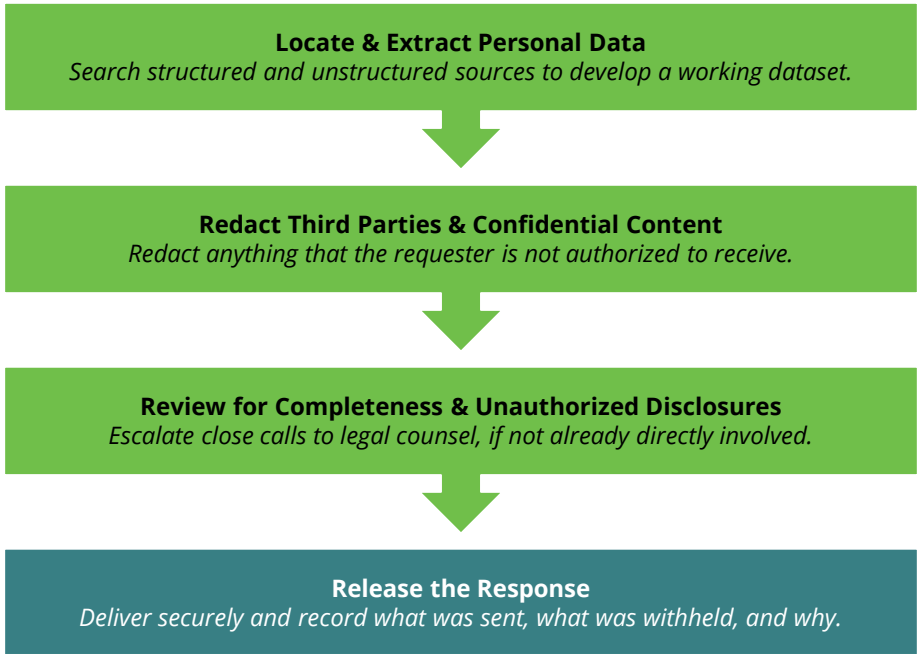
- You cannot fulfill requests relating to personal data that you are not aware of. The solution is to perform data-mapping, which means identifying which systems hold personal data (and of which category), who owns each system, and where data flows.
- Automate data mapping (especially systems and data discovery) where possible, as manual efforts tend to go stale very quickly.
- In the absence of robust system inventory data, consider using a combination of active scanning, SSO platform integration review, procurement record review, expense reports, etc.
- For each system and data type, capture how privacy requests can be executed. Whether a system can delete, or only de-identify or suppress, should be a **documented attribute**.
- Data mapping is not complete until it captures data flows, documenting how data is transferred between internal systems and out to service providers.



Fulfillment: Redaction

- Access requests are the heaviest lift when it comes to redaction. Everything else deletes or suppresses records, but access requires assembling a package and vouching for what's in it.
- Personal data can be found far beyond structured databases. Emails, meeting notes, support tickets, and project files that mention the requester may all be in scope.
- Over-disclosure (e.g., inadvertently sharing another person's personal data or another form of sensitive data) is a major risk and can easily lead to privacy incidents.
- Redaction is judgment-based work, and in many cases, it is not totally programmable. Redaction can require removing entire sections of content to balance the requester's rights against third parties' privacy and confidential business information.
- Counsel belongs deep in the workflow. Privilege, litigation holds, dual-subject records, etc. require legal decisions.

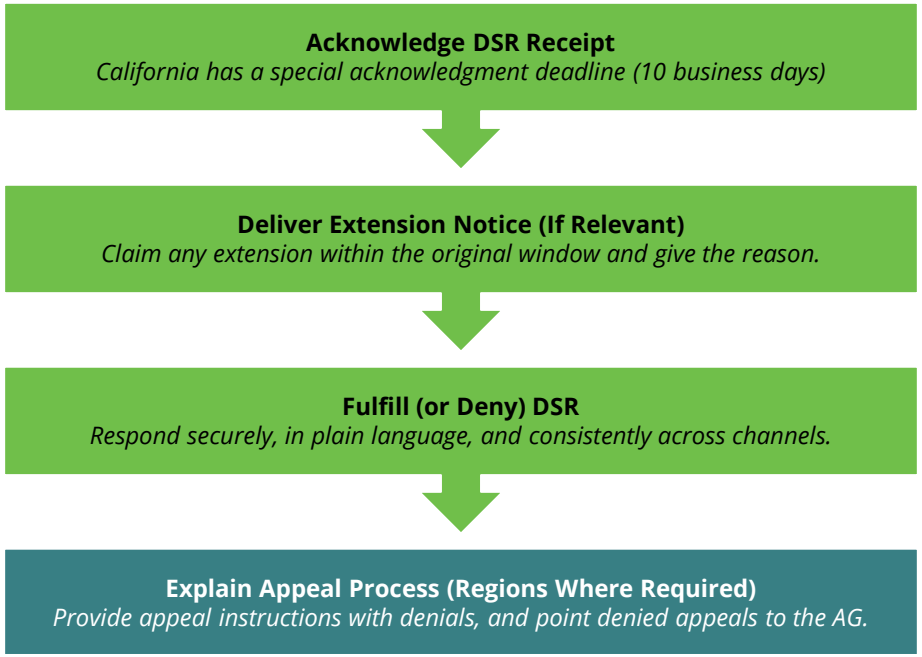
Typical DSR Redaction Sequence



Fulfillment: Subject Communication

- Every DSR comes with communication obligations, sometimes including request acknowledgment. California explicitly requires acknowledgment within 10 business days of request receipt.
- Request fulfillment notices must be provided. Most states require a response within 45 days, and any extension must be claimed within the original window, with reasons given.
- Request denials involve special communication requirements. Most states require an explanation, plus appeal instructions. A denied appeal must point the consumer to the relevant AG.
- Request-related communications must be delivered securely, in plain language, and consistently across channels (e.g., an access response sent insecurely could constitute a security incident).
- Every communication belongs in the record. Acknowledgments, extension notices, denials, and appeals must be auditable.
- **DROP simplifies "communication" from brokers**. DROP status codes convey responses rather than direct messaging.

Typical DSR Communication Sequence (N/A for DROP)



Reference: https://cppa.ca.gov/regulations/

Compliance: Regional Processing

- Organizations facing multi-state and multi-national DSR obligations must decide between using regional playbooks tailored to each law, or more universal processes. (In practice, the implementation of this decision may lie on a spectrum).
- More regional DSR processing aligns effort to each jurisdiction's minimum requirements, reducing the work of fulfilling requests. The downside stems from design complexity, as the regional approach requires more processes and risks drift.
- More universal DSR processing buys design consistency, and benefits consumer goodwill from honoring rights where the law does not require. The downside relates to fulfillment effort and over-serving more lenient regions.
- Mature programs may establish a few deliberate processing tiers, featuring a strict baseline with carve-outs only where statutes diverge significantly (e.g., opt-out timelines in CA). There is no right or wrong decision here but be deliberate.

Regional vs. Universal DSR Processing

Consideration	More Regional	More Universal
Design	More Playbooks (Per Jurisdiction)	Fewer Playbooks (Strictest Standards)
Fulfillment Effort	Lower (Aligns to Minimums)	Higher (Exceeds Minimums)
Consistency	Low (Drift Risk)	High (Fewer Standards)
Messaging	More Complex (Many Templates)	Less Complex (Fewer Templates)
Consumer Trust	Varies by Region	Similar Everywhere
New Laws	New Playbook	Configuration Update
Failure Mode	Unmanaged Complexity	Over-Extension

Compliance: Recordkeeping

- DSR processing must be thoroughly documented for auditability purposes. Practically, a fulfilled request without a record is indistinguishable from an ignored one.
- Audit trails should capture the full life of each request, including the request itself, verification actions, systems interacted with, vendors notified, redactions, and all subject communications.
- In some states (California, Colorado, etc.) privacy laws require businesses to maintain records of consumer requests and responses for at least 24 months.
- California's Delete Act goes further for data brokers, requiring independent audits every three years (beginning January 1, 2028), audit reports produced to CalPrivacy within five business days of a request, and audit records retained for six years.
- Automation is critical for high-quality recordkeeping. An orchestrated workflow "writes its own audit trail", while manual processes make documentation more challenging to maintain.

Mock Audit Trail: California Deletion Request

Date	Request #2026-0602 (CA Deletion Request)
June 2, 2026	Deletion request received via portal; 45-day clock starts
June 3, 2026	Acknowledgment sent (CA 10-business-day requirement)
June 4, 2026	Identity verified; two-point match documented
June 5, 2026	14 mapped systems queried; records found in 6
June 9, 2026	Deletion executed in 5 systems; 1 suppressed (system limitation documented)
June 12, 2026	Deletion directed to 4 service providers
June 20, 2026	Vendor confirmations complete (1 required follow-up)
June 24, 2026	Response delivered via secure channel; request closed
June 24, 2026	Record retained 24 months; purge scheduled June 2028

Reference: https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?sectionNum=1798.99.86.&lawCode=CIV

Compliance: Quantifiable Metrics

- **A healthy DSR program can be measured**, and leadership should expect to see quantifiable metrics. Recurring metrics should relate to intake volume (isolated by request type and/or intake channel), cycle time, on-time completion rate, exception and escalation rates, and cost per request.
- Trends are more meaningful than snapshots in time. For example, rising cycle times can predict future missed deadlines.
- Metrics have multiple purposes and can also support audit responses, demonstrating program effectiveness.
- An inability to produce DSR program metrics usually indicates that DSRs are processed ad-hoc (e.g., e-mail inboxes, spreadsheets) rather than via more robust systems of record.
- Public disclosures make some external benchmarking possible. Businesses over the 10-million-Californian threshold publish their DSR metrics, so you can see how your numbers compare.

DSR Program Health Signals

DSR Metric	Healthy Trend Indicator	Warning Trend Indicator
Intake Volume *(By Type/Channel)*	Stable Mix	Untracked Channels
Cycle Time	Decreasing (or Flat)	Increasing
On-Time Fulfillment	At (or Near) 100%	Any Downward Trend
Extension Rate	Low & Documented	Frequent
Escalation Rate	Low & Documented	Frequent
Vendor Confirmation	Tracked	Untracked
Cost Per Request	Decreasing (via Automation)	Increasing

Summary: DSR Program Maturity

Example	Common Example #1 Low Maturity	Common Example #2 Medium-Low Maturity	Common Example #3 Medium Maturity	Common Example #4 Medium-High Maturity	Common Example #5 High Maturity
DSR Intake	No Contact Methods	Generic Contact Methods	Privacy E-Mail, Toll-Free Phone Number	Privacy/DSR Web Portal, UOOM/GPC	Privacy/DSR Web Portal, UOOM/GPC, DROP
Identity Verification	None	Ad-Hoc	One-Size-Fits-All	Calibrated	Calibrated, Agent-Handling
Data Mapping	None	Tribal Knowledge	Static & Stale	Static & Current	Automated & Current
Fulfillment Coverage	Unknown	Minimal (Manual)	Partial (Manual)	Complete (Manual)	Complete (Automated)
Redaction Controls	None	Ad-Hoc	Manual Review	Workflow-Based	Workflow-Based, Counsel Engagement
Subject Communication	None	Ad-Hoc	Fulfillment Only	Acknowledgment, Fulfillment	Acknowledgment, Fulfillment, DROP Codes
Vendor Propagation	None	Ad-Hoc	Manual, Unconfirmed	Automated, Unconfirmed	Automated, Confirmed
Regional Processing	Not Considered	One-Size-Fits-All	Manual, Per Request	Rules-Based	Rules-Based, New-Law Ready
Recordkeeping	None	Spreadsheet	Ticketing System	Application	Application (Verified)
Metrics	None	Ad-Hoc	Basic Metrics, Snapshot	Full Dashboard, Snapshot	Full Dashboard, Trends

Poll: How Mature is Your DSR Program?

A **Absent.** Requests are rarely received and/or DSR processing is unfamiliar.

B **Reactive.** Requests are handled ad-hoc, requiring lots of energy and effort.

C **Functional.** Processes are defined and manual DSR processing is competent.

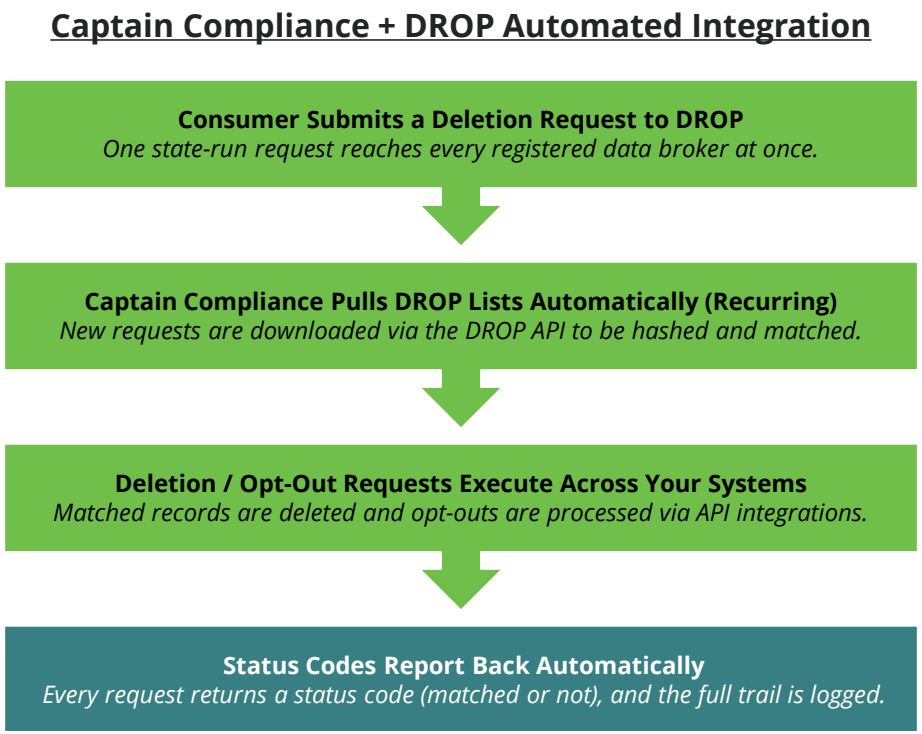
D **High-Performing.** Requests are orchestrated efficiently via thoughtful automation.

Automation & Integration

Orchestrating DSR Workflows with Captain Compliance

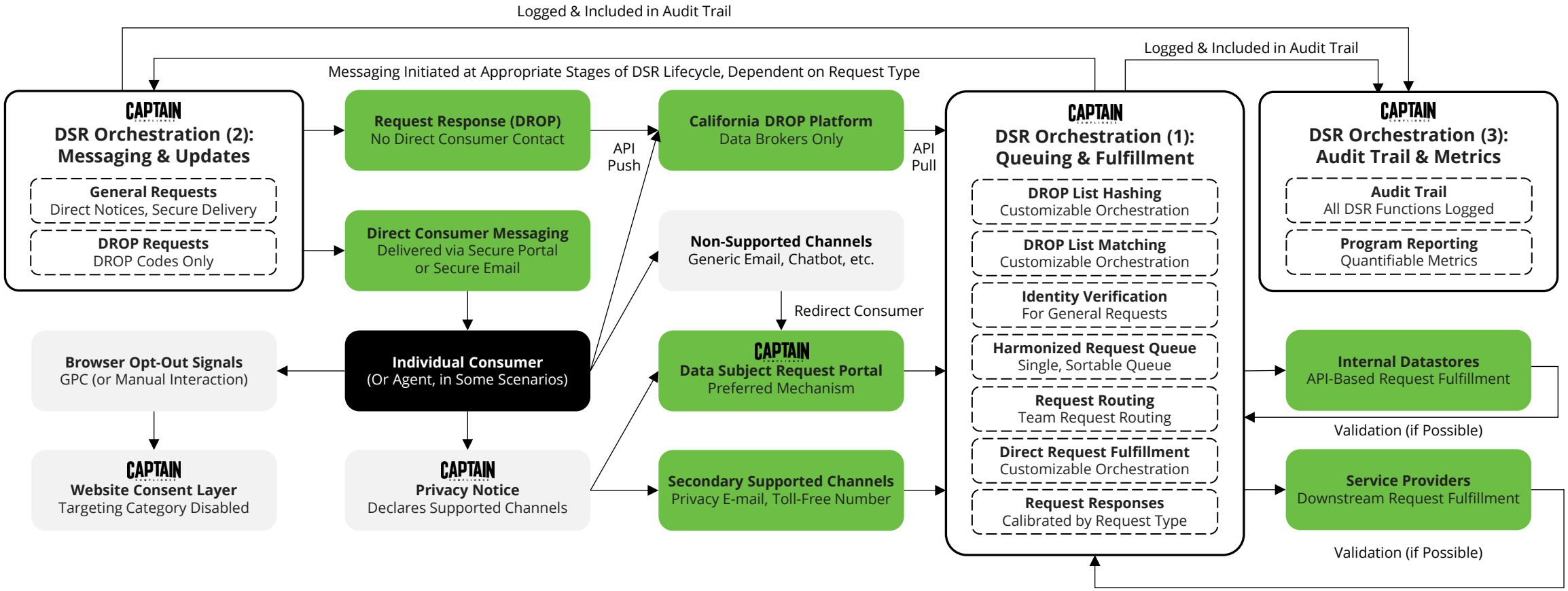
Captain Compliance + DROP Automation

- The Captain Compliance DSR Module's native DROP integration is launching now (in final testing). List download, hashing and matching orchestration, deletion and opt-out fulfillment, and reporting are automated on a configurable and recurring cadence (1 - 45 days).
- No two DSR programs run on the same architecture, so the platform is designed to adapt to yours rather than replace it.
- The Captain Compliance platform orchestrates and supports the full DROP cycle. DROP-originated requests are tagged and queued alongside your other DSR tickets, with unique processing elements to accommodate DROP requirements.
- Connectors are not a fixed catalog. Prebuilt integrations cover common systems, and new connectors are built as required.
- Workflows, teams, and routing are fully configurable. Request types, jurisdictions, and escalation paths follow your process.



Reference: https://captaincompliance.com/

DSR and DROP Automation Overview



Questions to Ask Your Operations Team

- Can we see every request (from every channel) in one place, with one record per request?
- How do we verify identity, for which request types, and when did we last test this?
- Do we have any fulfillment gaps (systems known to hold personal data but outside our current process)?
- How do we direct vendors to delete or process requests, and how do we confirm they acted?
- Which consumer rights do we honor in which states, and was this a deliberate decision?
- Could we hand a regulator a complete audit trail for any request from last quarter?
- Could we quickly produce this quarter's DSR volumes, cycle times, and on-time rate?
- If we are a data broker, who has accountability over DROP and the 45-day update cadence?

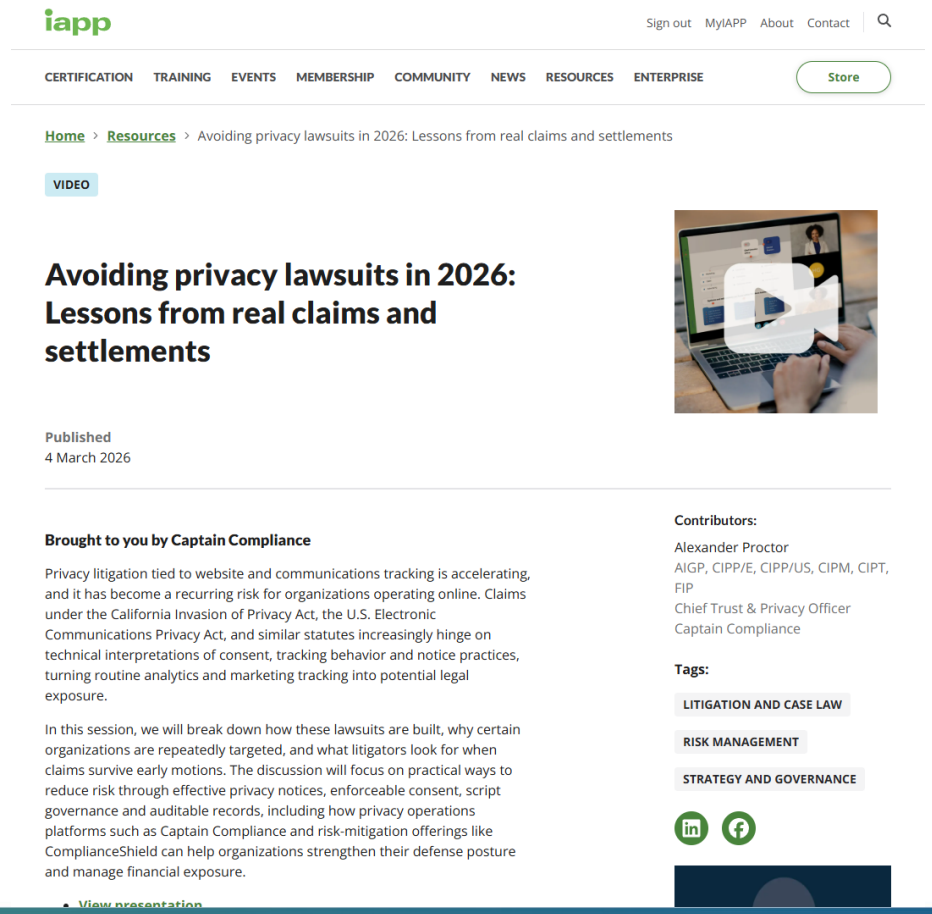
Resources Worth Bookmarking

Description	Web URL
CPPA Data Broker Registry	https://www.cppa.ca.gov/data_broker_registry
CalPrivacy's Data Broker Guide to DROP	https://www.privacy.ca.gov/drop-for-data-brokers
Delete Act Statute	https://cppa.ca.gov/regulations/pdf/data_broker_reg_delete_act_statute_eff_20260101.pdf
DROP Technical API Reference	https://privacy.ca.gov/drop-for-data-brokers/technical-specifications/api-operations/
IAPP U.S. State Privacy Legislation Tracker	https://iapp.org/resources/article/us-state-privacy-legislation-tracker
Captain Compliance Website	https://captaincompliance.com
Captain Compliance YouTube Channel	https://www.youtube.com/@captain-compliance
Complimentary Privacy Checkup with Alex	https://cal.com/alex-captaincompliance/checkup

Missed Our Last IAPP Webinar?

- The last Captain Compliance IAPP webinar, titled ***"Avoiding Privacy Lawsuits in 2026: Lessons from Real Claims and Settlements"*** aired on March 4, 2026, and is available on demand in the IAPP resource library (CPE eligible).
- Website privacy litigation has only accelerated since that session aired: CIPA and other wiretapping claims are being made in high volume, and the issues remain highly relevant.
- The webinar covers the web-tracking litigation landscape and addresses key topics such as opt-in vs. opt-out consent models, faulty CMPs, cookie blocking vs. script blocking, network traffic litigation risks, universal opt-out mechanisms, and more.
- The session included an offer for a **complimentary website tracking audit**, and this remains available to those who watch the webinar recording. Register now for a complimentary website tracking and consent mechanism effectiveness review.

  https://cal.com/alex-captaincompliance/checkup



Reference: https://iapp.org/resources/article/avoiding-privacy-lawsuits-in-2026-lessons-from-real-claims-and-settlements

Captain Compliance Platform

- **Free Cookie Scanner** analyzes any website and generates a categorized inventory of first-party and third-party cookies, while flagging higher-risk trackers.
- **Cookie Consent Module** delivers regionally-customizable banners and ensures that websites respect visitor tracking preferences in accordance with global privacy laws.
- **Cookie Transparency Page** automatically generates a clear, up-to-date web page describing the cookies and tracking technologies used on websites.
- **Dynamic Privacy Notice** turns a simple questionnaire into a comprehensive privacy disclosure, with dynamic, layered formatting that adjusts based on visitor location.
- **Data Subject Rights (DSR) Portal** provides a customizable and automatable workflow to intake, verify, and fulfill privacy requests from consumers.
- **Privacy Browser Extensions** allow insurance providers and similar parties to assess cookie consent functionality, including identifying banner misconfigurations.
- **ComplianceShield** extends beyond technical compliance by providing qualified customers with added legal risk mitigation and defense support in the event of web-tracking litigation.

Questions & Answers

Alex Proctor
AIGP, CIPP/E, CIPP/US, CIPM, CIPT, FIP
Chief Trust & Privacy Officer
Captain Compliance

www.captaincompliance.com

Web Conference
Participant Feedback Survey

Please take this quick (2 minute) survey to let us know how satisfied you were with this program and to provide us with suggestions for future improvement.

Click here: https://iappwf.questionpro.com/t/AbBPvZ9HjF

Thank you in advance!

For more information: www.iapp.org

Attention IAPP Certified Privacy Professionals:

This IAPP web conference may be applied toward the continuing privacy education (CPE) requirements of your AIGP, CIPP/US, CIPP/E, CIPP/A, CIPP/C, CIPT or CIPM credential worth 1.0 credit hour. IAPP-certified professionals who are the named participant of the registration prior to the live webinar will automatically receive credit. After the broadcast date, individuals may submit for credit by completing the continuing education application form here: submit for CPE credits.

Continuing Legal Education Credits:

The IAPP provides certificates of attendance to web conference attendees. Certificates must be self-submitted to the appropriate jurisdiction for continuing education credits. Please consult your specific governing body's rules and regulations to confirm if a web conference is an eligible format for attaining credits. Each IAPP web conference offers either 60 or 90 minutes of programming.

For questions on this or other IAPP Web Conferences or recordings please contact: livewebconteam@iapp.org